ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

Кваліфікаційна наукова
праця на правах рукопису

ТАРАСЮК Анатолій Васильович

УДК 336.7:340.5:347.7

ДИСЕРТАЦІЯ
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Спеціальність 12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право
08 – Право

Подається на здобуття наукового ступеня доктора юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ А. В. Тарасюк

Науковий консультант – Довгань Олександр Дмитрович, доктор юридичних наук, професор, заслужений діяч науки і техніки України.

Київ – 2021

АНОТАЦІЯ

Тарасюк А. В. **Теоретико-правові основи забезпечення кібербезпеки України**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право (081 – Право). – Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». – Київ, 2021.

Дисертація присвячена дослідженню проблеми формування теоретико-методологічних основ забезпечення кібернетичної безпеки України в сучасних умовах шляхом розвитку теоретичних засад інформаційного права та розроблення пропозицій з удосконалення інформаційного законодавства.

У дисертаційній роботі вирішена важлива наукова проблема – розроблення концептуальних правових та організаційних засад забезпечення кібернетичної безпеки України й практичних рекомендацій щодо вдосконалення механізмів її реалізації.

Запропоновано авторське трактування терміна «*культура кібербезпеки*» – це система переконань, уявлень та етичних норм щодо ведення інформаційної діяльності у кіберпросторі, знань, умінь і навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності в кіберпросторі.

«Глобальну культуру кібербезпеки» в роботі розглянуто як наднаціональну масову культуру кібербезпеки людини, суспільства, держави.

Водночас доведено, що основною метою формування глобальної культури кібербезпеки є досягнення такого стану соціальної взаємодії між суб'єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів кіберпростору.

Базовою в дослідженні кібербезпеки є категорія «безпека». В основу авторського підходу до сутності категорії «кібербезпека» покладено наукові

уявлення видатних учених сучасності, зокрема О. Довганя, В. Пилипчука, О. Баранова, І. Коржа, які поняття «кібербезпека» розглядають у соціальному розумінні «безпеки», що означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних і потенційних загроз або уникнути їх, що, з іншого боку, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їхній розвиток. Зазначений підхід у дисертації є базовим у дослідженні змісту кібербезпеки.

З’ясовано, що сучасний рівень розвитку інформаційної сфери зумовлює потребу виокремлення кібернетичної безпеки в самостійний вид безпеки, що дасть змогу, ураховуючи особливості відповідних систем і процесів управління, реалізувати правові, організаційні й технічні можливості захисних заходів. Це також передбачає підвищення вимог до захисту згаданих систем і процесів залежно від їхнього призначення, рівня, складу тощо. До того ж реалії сьогодення переконливо свідчать, що ця науково-правова категорія вийшла за межі інформаційного протиборства та військової безпеки і є елементом інформаційної сфери загалом.

Доведено, що кібернетична безпека – це також сукупність умов, які у фізичному, емоційно-психічному, духовно-освітньому, професійному, фінансовому, політичному й інших аспектах гарантовано забезпечують захищеність усіх компонентів інформаційних систем від якомога більшої кількості загроз і негативних впливів у кіберпросторі або ж від руйнівних наслідків у разі похибок, нещасних випадків, псування, аварій та іншої шкоди в цій сфері.

Аргументовано, що до предмета вивчення безпекової науки стосовно кіберсередовища належать: природні, соціально-економічні, соціально-політичні та техногенні процеси в контексті їхнього розвитку, взаємодії й утворення нових об’єктів і явищ, їхніх елементів із навколишнім середовищем

задля виявлення існуючих і потенційних небезпек, оцінювання відповідних ризиків та розробки адекватних методів і способів протидії, а також розробки належної нормативної бази для належної правової регламентації вимог, методик, механізмів, алгоритмів, застосування яких гарантує досягнення мети захищеності інтересів людини, суспільства й держави від наявних і можливих загроз.

На основі теоретичного аналізу співвідношення кібербезпеки й інформаційної безпеки розроблено логічну схему підпорядкованості різного роду безпек, зокрема кібербезпеку (Cybersecurite) визначено нами як складову інформаційної безпеки (Information Security). Кібербезпека формується в реляційних відносинах із безпекою мереж (Network Security), безпекою інтернету (Internet Security) і безпекою додатків (Application Security), а також здійснює підтримку безпеки інфраструктури критичної інформації у частині, що її стосується (Critical Information Infrastructure Protection); кіберзлочинність (Cybercrime) і безпечну діяльність у кіберпросторі (насамперед дітей і молоді в інтернеті – Cybersafety) відображено окремо. Кіберзлочинність впливає на інформаційну безпеку та, відповідно, кібернетичну безпеку. Безпечну діяльність у кіберпросторі, як певний орієнтир ідеальної поведінки, розміщено окремо.

На основі аналізу базових категорій, що наведені в Законі України «Про основні засади забезпечення кібербезпеки України», виявлено низку невідповідностей, а також відсутність розуміння базисних категорій кібербезпеки. На цій основі обґрунтовано пропозиції щодо визначення на законодавчому рівні таких понять:

– «*стан захищеності*», яке є системоутворювальним до категорії «безпека» та її еквівалентом. Запропоновано під цим терміном розуміти наявність параметрів, відповідно до яких об’єкти кібербезпеки перебувають під захистом. Основними параметрами визначено дотримання прав особи в кіберпросторі, реалізація національних інтересів в інформаційній сфері, здатність суб’єктів забезпечення кібербезпеки діяти і застосовувати засоби для

усунення або зниження рівня небезпеки для об’єктів кібербезпеки та кіберзахисту;

– «*кіберзлочин*» запропоновано у визначенні цього терміна словосполучення «міжнародними договорами» замінити словосполученням «міжнародним правом». Зазначений підхід забезпечить єдність термінологічного тлумачення на рівні національного та міжнародного законодавства;

– «*кіберзагроза*» обґрунтовано, що законодавче визначення цього терміна не співвідноситься за обсягом інформації, наведеної в терміні «кібербезпека», та не відповідає визначенню цього терміна. Адже кіберзагроза – це також злочинний акт, метою якого є пошкодження, викрадення цінних даних, доступ до несанкціонованих файлів або порушення цифрового життя загалом. Під кіберзагрозою слід також розуміти тактику, техніку та процедуру, що використовуються під час кібератаки.

На основі теоретичного аналізу правової природи відносин у сфері забезпечення кібернетичної безпеки людини комплексно досліджено всі її складові – суб’єкт (людина у глобальному інформаційному просторі, яка потребує належного правового забезпечення своєї безпеки при користуванні кібернетичним простором), об’єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов’язків усіх учасників зазначених суспільних відносин).

Удосконалено зміст поняття «кібернетична безпека людини», яке запропоновано розуміти як стан її захищеності, що визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.

Наголошено, що найуразливим суб’єктом інформаційних правовідносин є людина. Зумовлено це постійним виникненням нових викликів і загроз інформаційній безпеці особи, пов’язаних із недосконалістю інформаційно-телекомунікаційних технологій, інформаційно-психологічними впливами,

використанням інформації для досягнення геополітичних, терористичних та інших протиправних, руйнівних цілей. Отже, в умовах глобального інформаційного суспільства особистість у процесі задоволення своїх потреб найяскравіше виявляє свою соціальну складову і, ураховуючи нові безпекові виклики й загрози, змушена на основі культури інформаційної безпеки виробляти відповідні заходи протидії.

Визначено декілька основних критеріїв класифікації загроз кібербезпеці людини. Зокрема: мета, до якої прагне джерело загрози; джерело загрози кібербезпеці людини; розташування джерела загрози; характер впливу, природа виникнення.

Усебічне дослідження новітніх викликів і загроз кібербезпеці в умовах транскордонності у глобальному інформаційному суспільстві, а також небезпечних тенденцій у цій сфері дало змогу виокремити критерії їх можливої класифікації: джерело загрози (виклику), залежність від джерела загрози, розташування джерела загрози стосовно об’єкта, характер впливу. На цій основі з метою вдосконалення вітчизняної системи правового забезпечення кібернетичної безпеки людини запропоновано авторську класифікацію видів відповідних викликів і загроз. Зокрема, беручи до уваги значущість соціальних мереж, визначено джерела загроз в інтернеті, а саме: сайти, що становлять небезпеку для особистості (мають на меті вплив на свідомість індивіда, рекламовані задля отримання зиску й ін.); спам, тотальне розсилання реклами й іншої інформації без бажання користувача тощо.

Крім того, вивчення сучасних інформаційно-телекомунікаційних технологій дало змогу виявити специфічну групу загроз, пов’язаних із цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin та ін.), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie тощо).

Серед важливих теоретичних інновацій у роботі розроблено Концепцію кібернетичної безпеки людини та подано її обґрунтування. Визначено

структуру та зміст концепції, а також потребу долучення до її складу документів стратегічного планування України. Запропоновано структурно-змістовне наповнення зазначеної концепції, зокрема її головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення інформаційної безпеки людини. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави в цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість концепції.

Зазначено, що недосконалість вітчизняного інформаційного законодавства, неузгодженість системи міжнародної кібербезпеки, брак дійового інструментарію протидії викликам і загрозам в інформаційному (кібернетичному) просторі є основними чинниками, які, ураховуючи динаміку відповідних правопорушень, а також викликів і загроз, що негативно впливають на головного суб'єкта інформаційних відносин – людину, здійснюють значний вплив на характер цих відносин у суспільстві.

Теоретичний аналіз основних концепцій інформаційного суспільства дав змогу з'ясувати, що реальні загрози глобальному інформаційному суспільству на сучасному етапі сконцентровані в таких сферах: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо. На цій основі обґрунтовується висновок, що успішне розв'язання зазначених глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об'єднаних зусиль усього світового співтовариства.

Концептуальними засадами правового забезпечення кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів визначено: розвиток державно-приватного партнерства у сфері взаємодії державних органів із громадськими організаціями та громадянами з метою

забезпечення кібербезпеки України; інформаційно-просвітницьку, ідеологічну й освітню роботу із протидії радикальній ідеології та екстремізму; удосконалення нормативно-правового забезпечення протидії використанню інтернету в терористичних та екстремістських цілях, а також забезпечення національних інтересів суверенної України в інформаційній сфері; розвиток міжнародного чинника з метою утвердження України як повноправного учасника глобальних інформаційних процесів заради подальшої інтеграції в НАТО й поліпшення іміджу нашої держави серед міжнародних партнерів; створення, розвиток і забезпечення безпеки національних інформаційних ресурсів; практичну реалізацію на рівні законодавчого забезпечення національних інтересів України в кіберсфері.

З урахуванням міжнародного досвіду та на основі аналізу національної практики розроблено чотири основні складові національних інтересів України в кіберсфері: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму та патріотизму, наукового і культурного потенціалу країни; 2) інформаційне забезпечення державної політики, що пов’язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально значущих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв’язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних та інформаційних систем, як створюваних, так і тих, що функціонують на території України.

На основі аналізу основних підходів державної політики з реформування СБ України,доведено, що з метою підвищення ефективності організаційного забезпечення кіберзахисту об’єктів критичної інфраструктури та критичної інформаційної інфраструктури серед функціональних завдань СБ України необхідно передбачити такі заходи: здійснювати правове забезпечення діяльності національного координаційного центру кібербезпеки; вносити пропозиції щодо вдосконалення нормативно-правового забезпечення; оцінювати безпеку критичної інформаційної інфраструктури; координувати дії суб’єктів критичної інформаційної інфраструктури в напрямі обміну й надання інформації про комп’ютерні інциденти, щодо використання коштів, призначених для запобігання, виявлення та ліквідації наслідків комп’ютерних атак і реагування на комп’ютерні інциденти.

Ключові слова: *безпека, кібернетична безпека, інформаційне право, інформаційні правовідносини, загрози, інформаційна політика, кібербезпека, кіберзагрози, інформаційне законодавство, кіберпростір.*

SUMMARY

Tarasyuk A. V. Theoretical and legal bases of cyber security of Ukraine. – *Qualifying scientific work on the rights of the manuscript*.

The dissertation on competition of a scientific degree of the doctor of legal sciences on a specialty 12.00.07 – administrative law and process; finance law; information law (081 - Law). – State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine". – Kyiv, 2021.

The dissertation is devoted to research of a problem of formation of theoretical and methodological bases of maintenance of cyber security of Ukraine in modern conditions by development of theoretical bases of information law and formation of offers on perfection of the information legislation.

The dissertation solves a significant scientific problem - the development of conceptual legal and organizational principles of cyber security of Ukraine and practical recommendations for improving the mechanisms of its implementation.

The author's interpretation of the term "culture of cybersecurity" is offered. By this term we mean a system of beliefs, ideas and ethical standards for conducting information activities in cyberspace, knowledge, skills and abilities to ensure cybersecurity, as well as requirements for professional and psychological qualities of persons necessary for secure information activities in cyberspace.

"Global culture of cybersecurity", for its part, in the work is considered as a supranational mass culture of cybersecurity of man, society, state.

At the same time, it has been proven that the main goal of forming a global culture of cybersecurity is to achieve a state of social interaction between the subjects of information activities, when cybersecurity measures become a daily habit of every user of cyberspace services.

The basic category in cybersecurity research is the category of "security". The author's approach to the essence of the category "cybersecurity" is based on scientific ideas of prominent modern scientists, in particular O. Dovgan, V. Pylypchuk, O. Baranov, I. Korzh, who consider the concept of "cybersecurity" in the social sense

of "security", which means balanced the state of functioning of the social system (man, state, world community), anthropogenic, natural systems, etc., in which man due to knowledge of the environment and trends in its development is able to identify and minimize the negative impact of existing and potential threats or avoid them. , on the other hand, gives it the opportunity to maintain its value system and ensure their further development. This approach in the dissertation is taken as a basis in the study of the content of cybersecurity.

It was found that the current level of development of the information sphere necessitates the separation of cyber security into an independent type of security, which will allow, taking into account the peculiarities of relevant systems and management processes, to implement legal, organizational and technical capabilities of security measures. It also involves increasing the requirements for the protection of these systems and processes depending on their purpose, level, composition, and so on. In addition, the realities of today convincingly show that this scientific and legal category has gone beyond information confrontation and military security and is an element of the information sphere in general.

It is proved that cyber security is also a set of conditions that in physical, emotional, spiritual, educational, professional, financial, political and other aspects are guaranteed to ensure the protection of all components of information systems from as many threats and negative influences in cyberspace or from destructive consequences in case of errors, accidents, spoilage, accidents and other damage in this area.

It is argued that the subject of security science in relation to the cyber environment includes: natural, socio-economic, socio-political and man-made processes in the context of their development, interaction and formation of new objects and phenomena, and their elements with the environment to identify existing and potential hazards, assessment of relevant risks and development of adequate methods and methods of counteraction, as well as development of appropriate regulatory framework for proper legal regulation of requirements, methods, mechanisms, algorithms, the application of which guarantees the goal of protecting

human interests, society and the state from existing and potential threats.

Based on the theoretical analysis of the relationship between cybersecurity and information security, a logical scheme of subordination of various types of security has been developed, in particular, cybersecurity (Cybersecurite) has been defined by us as an integral part of information security (Information Security). Cybersecurity is formed in relational relations with network security (Network Security), Internet security (Security) and application security (Application Security), as well as supports the security of critical information infrastructure in its part (Critical Information Infrastructure Protection); cybercrime and safe activities in cyberspace (primarily children and young people on the Internet - Cybersafety) are reflected separately. Cybercrime has an impact on information security and, consequently, cybersecurity. Safe activity in cyberspace, as a guide to ideal behavior, is placed separately.

Based on the analysis of the basic categories given in the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine", a number of inconsistencies were identified, as well as a lack of understanding of the basic categories of cybersecurity. On this basis, the proposals to define the following concepts at the legislative level are substantiated:

– "security state", which is system-forming to the category of "security" and its equivalent. It is suggested that this term refers to the existence of parameters according to which cybersecurity objects are protected. The main parameters are the observance of individual rights in cyberspace, the realization of national interests in the information sphere, the ability of cybersecurity actors to act and apply means to eliminate or reduce the level of danger to cybersecurity and cybersecurity objects;

– it is proposed in the definition of the term "cybercrime" to replace the phrase "international treaties" with the phrase "international law". This approach will ensure the unity of terminological interpretation at the level of national and international law;

– it is substantiated that the legislative definition of the term “cyberthreat” does not correspond to the amount of information given in the term “cybersecurity”

and does not correspond to the definition of this term. After all, a cyber threat is also a criminal act aimed at damaging, stealing valuable data, accessing unauthorized files or disrupting digital life in general. Cyber threats should also be understood as tactics, techniques and procedures used during a cyber attack.

Based on the theoretical analysis of the legal nature of relations in the field of human cyber security, all its components are comprehensively studied - the subject (a person in the global information space who needs proper legal security in the use of cyberspace), object (state of protection from personal protection). internal and external threats during the use of cyberspace) and content (a set of rights and responsibilities of all participants in these social relations).

The content of the concept of "human cyber security" has been improved, which is proposed to be understood as a state of security, determined by a person's ability to resist internal and external negative information influences, as well as the ability of the information state and information society to ensure information security.

It is emphasized that the most vulnerable subject of information relations is a person. This is due to the constant emergence of new challenges and threats to information security, related to the imperfection of information and telecommunications technologies, information and psychological influences, the use of information to achieve geopolitical, terrorist and other illegal, destructive goals. Thus, in the global information society, the individual in the process of meeting their needs most clearly reveals its social component, and, given the new security challenges and threats, is forced to develop appropriate countermeasures based on the culture of information security.

Several main criteria for classifying human cybersecurity threats have been identified. In particular: the goal to which the source of threat seeks; source of threat to human cybersecurity; location of the source of threat; nature of influence, nature of origin.

A comprehensive study of the latest challenges and threats of cybersecurity in a cross-border environment in the global information society, as well as dangerous

trends in this area allowed to identify the criteria for their possible classification: source of threat (call), dependence on the source of threat, location of threat impact. On this basis, in order to improve the domestic system of legal support for cyber security, the author's classification of the types of relevant challenges and threats is proposed. In particular, given the importance of social networks, identified sources of threats on the Internet, namely: sites that pose a danger to the individual (aimed at influencing the consciousness of the individual, advertised for profit, etc.); spam, total mailing of advertising and other information without the user's desire, etc.

In addition, the study of modern information and telecommunications technologies has identified a specific group of threats related to the digital economy, financial and banking (including electronic money, cryptocurrencies - BitCoin, LitCoin, OneCoin, etc.), the confidentiality of personal data (Threats from state-of-the-art Real-TimeBidding online advertising (RTB), special cookies, etc.).

Among the important theoretical innovations in the work the Concept of cyber security of the person is developed and its substantiation is given. The structure and content of the concept are determined, as well as the need to include in its composition the documents of strategic planning of Ukraine. The structural and substantive content of this concept is proposed, in particular its main principles of formation, tasks, implementation mechanisms and the expected results of state policy in the field of information security. In addition, the goal of harmonization of information relations, increasing the responsibility of the state in this area, creating conditions for the formation of a favorable cyber environment as a strategic direction of the concept is substantiated.

It is noted that the imperfection of domestic information legislation, inconsistency of the international cybersecurity system, lack of effective tools to counter challenges and threats in the information (cyber) space remain the main factors that, given the dynamics of relevant offenses, as well as challenges and threats the subject of information relations - a person who has a significant influence on the nature of these relations in society.

Theoretical analysis of the basic concepts of the information society revealed

that the real threats to the global information society at the present stage are concentrated in the following areas: militarization of cyberspace, large-scale information wars, the spread of extremist and manipulative materials, destructive information and psychological influences on the individual and public consciousness, etc. On this basis, the conclusion is substantiated that the successful solution of these global socio-economic, political, security and other problems is possible only with the combined efforts of the entire world community.

Conceptual principles of legal support of cybersecurity of Ukraine at the present stage of development of global information processes define: development of public-private partnership in the field of interaction of state bodies with public organizations and citizens for the purpose of ensuring cybersecurity of Ukraine; informational, educational, ideological and educational work on counteracting radical ideology and extremism; improving the legal framework for combating the use of the Internet for terrorist and extremist purposes, as well as ensuring the national interests of sovereign Ukraine in the information sphere; development of the international factor in order to establish Ukraine as a full participant in global information processes for the sake of further integration into NATO and improving the image of our country among international partners; creation, development and security of national information resources; practical implementation at the level of legislative support of national interests of Ukraine in the cybersphere.

Taking into account international experience and based on the analysis of national practice, four main components of Ukraine's national interests in cyberspace have been developed: 1) observance of constitutional human and civil rights and freedoms in obtaining and using information, promoting spiritual renewal of the state traditions of humanism and patriotism, scientific and cultural potential of the country; 2) information support of state policy, related to bringing to the international community and the people of Ukraine truthful information about state national policy, the official position of the state on socially significant events of the state and international life, providing citizens with access to open national information resources; 3) application of the latest information technologies, creation

of the domestic information industry, including the industry of informatization, telecommunications and communication, meeting the needs of the domestic market with its products, as well as ensuring the accumulation, efficient use and preservation of national information resources; 4) protection of information resources from unauthorized access, ensuring the security of telecommunications and information systems, both created and those operating in Ukraine.

Based on the analysis of the main approaches of the state policy on reforming the Security Service of Ukraine, it is proved that in order to increase the effectiveness of organizational support of cyber protection of critical infrastructure and critical information infrastructure among the functional tasks of the Security Service of Ukraine it is necessary to make proposals for improving the regulatory framework; assess the security of critical information infrastructure; coordinate the actions of critical information infrastructure entities in the direction of exchange and provision of information on computer incidents, on the use of funds intended for the prevention, detection and elimination of the consequences of computer attacks and response to computer incidents.

Key words: *security, cyber security, information law, information legal relations, threats, information policy, cybersecurity, cyber threats, information legislation, cyberspace.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці в яких опубліковані основні наукові результати дисертації:

1. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи; Одеса : Фенікс, 2020. 404 с.

2. Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : моногр. Х. : Вид-во «ФІНН», 2011. 192 с.

3. Пилипчук В. Г., Брижко В. М., Доронін І. М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія; за заг. ред. акад. НАПрН України В. Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с., підр. 5.2.

4. Довгань О. Д., Тарасюк А. В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

5. Довгань О. Д., Тарасюк А. В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності *Інформація і право*. 2018. № 2 (25). С. 51–61.

6. Тарасюк А. В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. 4(31)/2019. С. 73–82.

7. Тарасюк А. В. Досвід забезпечення кібербезпеки у зарубіжних країнах. *Науковий вісник публічного та приватного права* : зб. наук. праць. 2019. № 4. С. 204–209.

8. Тарасюк А. В. Понятійно-категоріальний синтез правового забезпечення кібербезпеки України. *Порівняльно-аналітичне право*. №5. 2019. С. 296-298. URL : http://www.pap.in.ua/5_2019/77.pdf.

9. Тарасюк А. В. Стан правового забезпечення кібербезпеки в Україні. *Наукові записки ЛУБП*. Серія «Право». 2019. Вип. 23. С. 201–206.

10. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки Таврійського національного університету імені В.І. Вернадського.* Серія «Юридичні науки». 2020. Т. 31 (70), № 2. С. 119–124.

11. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. № 1. С. 133–136.

12. Довгань О. Д., Тарасюк А. В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*. 2020. № 2. С. 85–98.

13. Тарасюк А. В. Системний підхід у дослідженні правових основ кібербезпеки. *Прикарпатський юридичний вісник*. 2020. № 2. С. 108–111.

14. Тарасюк А. В. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254–258.

15. Тарасюк А. В. Забезпечення кібернетичної безпеки людини: міжнародно-правовий аспект. *Юридичний вісник*. 2020. № 3. С. 254–261.

16. Тарасюк А. В. Місце концепції «суспільства знань» у процесах забезпечення кібернетичної безпеки. *Юридичний науковий електронний журнал*. 2020. № 6. С. 156–169. URL : http://www.lsej.org.ua/6_2020/40.pdf.

17. Тарасюк А. В. Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях. *Вісник Запорізького національного університету.* Юридичні науки. 2020. № 4. Т. 1. С. 168–173.

18. Тарасюк А. В. Теоретико-правове підґрунтя інформаційної етики у системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52.

19. Довгань О. Д., Тарасюк М. В. Національні інтереси України в кібернетичній сфері. *Інформація і право*. 2021. № 1. С. 134-142

20. Тарасюк А. В. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights*. 2020. № 1. С. 167–172.

21. Тарасюк А. В. Актуальні питання правового забезпечення кібербезпеки України. *Recht der Osteuropäischen Staaten*. 4/2019. С. 164–168.

22. Тарасюк А. В. Пріоритети забезпечення кібербезпеки: досвід окремих країн. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. 4. С. 42–49. URL : https://doi.org/10.25313/2520-2308-2020-4-5818.

23. Тарасюк А. В. Окремі аспекти соціального чинника в забезпеченні кібербезпеки суспільства. *KELM (Knowledge, Education, Law, Management)*. 2020. № 3 (31). С. 206–211.

24. Тарасюк А. В. Місце та роль України у глобальних інформаційних процесах: питання кібербезпеки. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. XI (43). С. 46–52. URL : https://doi.org/10.25313/2520-2308-2020-11-6528.

25. Тарасюк А. В. Пріоритети національної політики України у сфері забезпечення міжнародної кібербезпеки. *Visegrad Journal on Human Rights*. 2021. № 1. С. 48-53.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

26. Тарасюк А. В. Актуальні питання протидії кіберзлочинності в сучасних умовах. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.-практ. Семінару. м. Харків, 26 жовт. 2018 р. 2018. С. 251–254.

27. Тарасюк А. В. Кібербезпека – один із важливих напрямків захисту держави. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.- практ. семінару, м. Харків, 23 трав. 2019 р. / редкол.: С.О. Гриненко (голов. ред.) та ін. Х. : Право, 2019. Вип. 10. С. 44–47.

28. Тарасюк А. В. Законодавчі підходи до кібернетичної безпеки України. *Актуальні проблеми правових наук в євроінтеграційному вимірі* зб. мат. Міжнародної наук.-практ. конф. м. Харків, 20–21 груд. 2019 р. 2020 р. С. 87–90.

29. Тарасюк А. В. Пріоритетні питання забезпечення кібербезпеки України. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку* : зб. мат. ІІІ Міжнародної наук.-практ. конф., м. Острог, 14 черв. 2019 р. / упорядн.: С. О. Дорогих, І. М. Доронін, О. Д. Довгань, О. В. Лебединська, В. Г. Пилипчук, О. Г. Радзієвська, М. С. Романов ; НУОА, НДІІП НАПрН України. К. : ТОВ «Вид. дім «АртЕк», 2019. С. 181–185.

30. Тарасюк А. В. Новації у сфері кібербезпеки великої Британії. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. Х Всеукраїнської наук.-практ. конф. м. Київ, 4 квіт. 2019 р. С. 217–218.

31. Тарасюк А. В. Окремі питання політики європейських країн щодо правового забезпечення кібербезпеки. *Теоретичні та практичні проблеми правового регулювання суспільних відносин* : зб. мат. Міжнародної наук.-практ. конф. м. Харків, 17–18 січ. 2020 р. С. 61–64.

32. Тарасюк А. В. Теоретико-правові конструкції правового забезпечення кібербезпеки України. *Реформування національного та міжнародного права: перспективи та пріоритети : зб. мат. Міжнародної наук.-практ. конф.* м. Одеса, 17–18 січ. 2020 р. С. 107–110.

33. Тарасюк А. В. Кіберпростір як об’єкт кібербезпеки держави. *Нові завдання та напрями розвитку юридичної науки у XXI столітті* : зб. мат. Міжнародної наук.-практ. конф. м. Одеса 21–22 лют. 2020 р. С. 115–118.

34. Тарасюк А. В. Окремі питання забезпечення кібербезпеки: досвід Європейського Союзу. *Міжнародне та національне законодавство: способи удосконалення* : зб. мат. Міжнародної наук.-практ. конф. м. Дніпро 3–4 квіт. 2020 р. С. 159–163.

35. Тарасюк А. В. Онтологічні засади поняття «кібербезпека». *Управління інформаційною безпекою* : зб. мат. Науково-практичної конф. НА СБУ. 15 травня 2020 р. К., С. 197-199

36. Тарасюк А. В. Окремі питання функціональних завдань суб’єктів забезпечення кібербезпеки. *Міжнародні та національні правові виміри*

забезпечення стабільності : зб. мат. Міжнародної наук.-практ. конф. м. Львів, 17–18 квіт. 2020 р. С. 72–76.

37. Тарасюк А. В. Окремі аспекти співпраці державного та приватного секторів безпеки у забезпеченні кібербезпеки. *Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні* : зб. мат. Міжнародної наук.-практ. конф. м. Запоріжжя, 24–25 квіт. 2020 р. С. 77–81.

38. Тарасюк А. В. Міжнародно-правові засади протидії кіберзагрозам *Розбудова правової держави в Україні: реалії та перспективи* : зб. мат. Міжнародної наук.-практ. конф. Одеса, 29 трав. 2020 р. С. 133–135.

39. Тарасюк А. В. Забезпечення кібербезпеки України як пріоритетне завдання цифрової дипломатії. *Кібербезпека в Україні: правові та організаційні питання» :* зб. мат. II Міжнародної наук.-практ. конф. м. Одеса, 26 листоп. 2020 р. С. 23–24.

40. Тарасюк А. В. Питання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : мат. наук.-практ. конф., м. Київ, 10 груд. 2020 р. / упоряд.: О. А. Баранов, В. М. Фурашев, С. О. Дорогих. К. : Фенікс, 2020. С. 241–246.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КБ	Кібернетична безпека
КПК	Кримінально-процесуальний кодекс
ІКТ	Інформаційно-комунікаційні технології
ІЗ	Інформаційна зброя
ІПВ	Інформаційно-психологічний вплив
РФ	Російська Федерація
ЄС	Європейський Союз
СБУ	Служба безпеки України
МО	Міністерство оборони
ЗМІ	Засоби масової інформації
НБ	Національна безпека
Інтернет-речей	IoT

ВСТУП

Актуальність теми дослідження. Сучасний етап розвитку світового співтовариства нерозривно пов’язаний з упровадженням цифрових технологій. Відповідно створюються умови для виникнення нових правовідносин.

Водночас сучасний етап стратегічної конкуренції і нові загрози вимагають удосконалення стратегії забезпечення кібербезпеки України, що має відповідати новим викликам, забезпечувати можливості процвітання Українського народу і бути фактором стримування для супротивників. Варто зауважити, що протягом 2020 року Службою безпеки України нейтралізовано понад 600 кіберінцидентів і кібератак на інформаційні ресурси органів влади й об’єкти критичної інфраструктури. Окрім цього, триває активна протидія кіберзагрозам з боку Росії. Відповідно, основоположне значення для втілення в життя нашої стратегії має забезпечення безпеки національного кіберпростору, що вимагає впровадження новітніх досягнень технічного прогресу, а також адміністративної ефективності держави і приватного сектора. Одного тільки технократичного підходу щодо кіберпростору недостатньо для розв’язання проблем, що виникають. Мають бути розроблені широкі інструменти ефективних заходів примусу, що дозволять запобігти можливій ескалації і забезпечать стримування структур, які здійснюють недружні дії. А з іншого боку, на постійній основі повинна тривати просвітницька робота. Метою якої має бути розвиток інформаційної культури людини, критичного мислення серед населення, екологія інформації та інформаційна гігієна.

Перспективним напрямом у вивченні проблем кібербезпеки України вважаємо якісно новий підхід, який би розглядав кібернетичну безпеку не тільки в конкретно прикладних аспектах, а і як внутрішній стан усієї соціальної системи. Діюча система кібербезпеки України має гарантувати рівноправну участь усіх суб’єктів інформаційної взаємодії в системі

глобальної безпеки й забезпечити захист їхніх основних прав і свобод. У зв'язку із застосуванням сучасних інформаційних технологій потрібна зміна підходу до правового регулювання суспільних відносин у процесі забезпечення кібербезпеки. Зважаючи на це, важливість досліджень теоретико-правових основ забезпечення кібербезпеки України лише зростає. Цим обумовлюється й авторська мотивація вибору зазначеного напряму наукового дослідження.

Актуальність теми дослідження визначається, насамперед, новизною самої проблеми кібербезпеки, особливо її правової, соціально-філософської та методологічної складових, акцентованих на забезпеченні безпеки людини, суспільства, держави, дослідженні її ціннісних уподобань. Ці питання особливо актуалізуються у наш час, коли слід активно протидіяти симбіозу бойових дій у кіберпросторі та інформаційним операціям, механізми якої активно застосовуються Росією у ході гібридної війни проти України. Зазначена проблематика певною мірою вже розроблялася вченими у правничій науці, де кожен із дослідників зробив свій внесок у загальну стратегію забезпечення кібербезпеки нашої країни. Це обумовлено значними трансформаціями, що відбуваються в сучасному світі в умовах розвитку інформаційно-комунікаційних технологій. При цьому держава і право в даних умовах не статичні, вони досить динамічні, постійно розвиваються і удосконалюються разом з розвитком суспільства. З плином часу з'являються нові суспільні відносини, які потребують правового врегулювання та наукового осмислення, особливо у контексті розвитку технологій штучного інтелекту. Зокрема це питання розробки асиметричних механізмів протидії розвідувально підривній діяльності у кіберпросторі та кібертероризму, протидії кіберзлочинності, посилення кіберзахисту критичної інфраструктури, забезпечення безпеки цифрових послуг, державно-приватного партнерства особливо в частині взаємодії учасників системи кібербезпеки, обміну інформацією про кіберзагрози на міжнародному та національному рівнях,

необхідність впровадження системи тренінгів та професійного навчання, підвищення рівня кіберкультури тощо.

Теоретичною базою дослідження стали пов'язані з проблематикою обраного наукового напряму праці в таких галузях і таких учених:

– *філософії:* А. Бергсон, Г. Гроцій, Р. Ієрінг, Н. Макіавеллі, Р. Оуен, Плутарх, Платон, Б. Рассел, Сенека, Сунь-цзи, А. Сен-Сімон;

– *інформаційного права*: І. Арістова, О. Баранов, К. Бєляков, В. Брижко, І. Бондар, С. Бондаренко, О. Довгань, С. Домбровська, О. Заярний, М. Згуровський, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, О. Костенко, В. Клочко, О. Логінов, А. Марущак, Є. Мануйлов, О. Морозов, А. Нашинець-Наумова, В. Остроухов, І. Панова, В. Пилипчук, В. Петрик, В. Політанський, М. Присяжнюк, Ю. Размєтаєва, В. Рубан, Ю. Руденко, Г. Сащук, Я. Собків, О. Тихомиров, Т. Ткачук, В. Фурашев, С. Феденько, Л. Харченко, О. Хілько, В. Шамрай, Р. Шаповал, В. Шатун, О. Ярема та ін.

– *інших галузей права*: вітчизняні вчені – В. Білоус, В. Горбулін, В. Григор'єв, В. Гулай, О. Дзьобань, Т. Карабін, А. Качинський, Я. Лазур, А. Легеза, Ю. Лісовська, І. Лях, Я. Малик, Й. Мастяниця, С. Мельник, Н. Нижник, Д. Прокоф'єва-Янчиленко, Г. Ситник, М. Савчин, О. Соснін, Л. Шиманський; зарубіжні вчені: С. Алексєєв, Дж. Барбер, Н. Вінер, В. Герхард, К. Геерс, Дж. Данн, К. Демпсі, Л. Козер, П. Корніш, А. Кемпф, Р. Оуен, В. Пілліттері, Б. Рассел, А. Робертс, Ф. Сталдер, М. Лібіскі, О. Лукашов, А. Левін, Х. Міллінгтон, М. Нільес, К. Шенон, К. Шилде, Р. Ярґер та ін.

На основі аналізу джерельної бази виявлено теоретичні та практичні проблеми – від браку достатніх теоретичних основ до відсутності системності й недостатньої ефективності відповідних практик забезпечення кібербезпеки України, необхідності правового врегулювання нових суспільних відносин, які виникають у досліджуваній сфері та адаптації національного законодавства до законодавства ЄС та НАТО.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Пріоритетних напрямів розвитку правової науки на 2016–2020 рр., затверджених постановою загальних зборів Національної академії правових наук України від 03.03.2016 р., Плану законодавчого забезпечення реформ в Україні, схваленого Постановою Верховної Ради України від 04.06.15 № 509-VIII, а також у межах планової науково-дослідної роботи Науково-дослідного інституту інформатики і права Національної академії правових наук України «Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні» (номер державної реєстрації 0116U007745).

Результати дослідження було розглянуто й обговорено в ході науково-практичного семінару в Науково-дослідному інституті інформатики і права НАПрН України, протокол № 2 від 25 лютого 2021 р.

Мета і завдання дослідження. *Мета* – сформувати теоретичну модель стратегії забезпечення кібернетичної безпеки України, запропонувати на цій основі теоретико-правові засади механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Окреслена дослідницька мета асоційована з розв'язанням вагомої *наукової проблеми* – формування теоретичної моделі стратегії забезпечення кібернетичної безпеки України та розробки теоретико-правових засад механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Досягнення поставленої мети передбачає розв'язання таких наукових *завдань*:

– дослідити генезис наукових поглядів забезпечення кібербезпеки України;

– на основі понятійно-категоріального синтезу з'ясувати змістовну сутність основних понять у національному законодавстві;

– з'ясувати особливості співвідношення кібербезпеки та інформаційної безпеки на сучасному етапі;

– дослідити методологічні засади правового забезпечення кібербезпеки України;

– дослідити стан правового регулювання кібербезпеки в Україні;

– охарактеризувати систему суб'єктів забезпечення кібербезпеки в Україні та дослідити практику правового регулювання їхньої діяльності;

– вивчити питання протидії кіберзагрозам на національному та глобальному рівнях, дослідити відповідний досвід законодавчого забезпечення зарубіжних країнах;

– на основі теоретико-правового аналізу дослідити загрози кібербезпеці людини під час використання кіберпростору та запропонувати правові механізми протидії їм;

– на основі порівняльно-правового дослідження дослідити особливості забезпечення кібербезпеки людини на міжнародному рівні;

– узагальнити теоретичні підходи до аналізу концепцій інформаційного суспільства;

– дати оцінку правовому чиннику у запобіганні кіберзагрозам сучасному українському суспільству;

– визначити теоретико-правове підґрунтя системи соціального регулювання в інформаційному суспільстві;

– виокремити концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів;

– запропонувати й обґрунтувати конкретні пріоритети розвитку правових основ державної політики України у сфері кібербезпеки;

– розробити напрями правового регулювання окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки.

Об'єктом дослідження є суспільні відносини у процесі забезпечення кібернетичної безпеки України.

Предмет дослідження – теоретико-правові основи забезпечення кібербезпеки України.

Методи дослідження. Як методологічна основа дослідження використані філософські (діалектичний), загальнотеоретичні, (гносеологічний, структурно-функціональний), спеціальні (порівняльно-правовий, індуктивний) та міжгалузеві методи наукового пізнання (історичний, аналітичний), застосування яких зумовлюється системним підходом.

За допомогою *філософських методів*, що стали онтологічною основою наукової праці, зокрема *діалектики*, досліджено кібернетичну безпеку України як важливу складову інформаційної в широкому розумінні та національної безпеки України, з'ясовано взаємозв'язки основних складових кібернетичної безпеки України, обґрунтовано взаємозалежність стану інформаційного законодавства та правового забезпечення кібербезпеки України (підрозд. 1.1–1.4). *Історичний метод* дав змогу дослідити генезис теорій і концепції забезпечення кібернетичної безпеки України (підрозд. 1.1). Використання *аналітичного методу* сприяло класифікації загроз кібернетичній безпеці України, розробці механізмів протидії їм (підрозд. 2.4, 2.5, 3.2, 4.2, 5.4), а також аналізу функціонування суб'єктів забезпечення кібернетичної безпеки України (підрозд. 2.3). *Порівняльно-правовий метод* покладено в основу дослідження міжнародного досвіду забезпечення кібернетичної безпеки (підрозд. 2.5, 4.3.1, 5.2). *Формально-юридичний метод* застосовувався при тлумаченні норм права для з'ясування їхньої суті, змісту та вираженої в них волі законодавця (підрозд. 2.1, 3.1). *Структурно-функціональний аналіз* дав можливість визначити відповідність нормативно-правових актів, з якими асоційована сучасна система правового забезпечення кібернетичної безпеки України реальним суспільним відносинам у цій сфері та міжнародним стандартам (підрозд. 5.2, 5.3). Використання *індуктивного методу*, *методів правового моделювання та прогнозування* дало змогу підтвердити висновок про необхідність удосконалення правового забезпечення кібернетичної безпеки України (підрозд. 5.3, 5.4).

Наукова новизна одержаних результатів. Дисертаційна робота є одним з перших у вітчизняній правничій науці комплексним дослідженням теоретико-правових основ забезпечення кібернетичної безпеки людини, суспільства, держави. Основними науковими добутками нашої праці стали:

вперше:

– *розроблено* структуру та зміст Концепції кібернетичної безпеки людини. Визначено її головні правові принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері правового регулювання кібернетичної безпеки людини;

– *обґрунтовано* існування комплексного міжгалузевого інституту інформаційного законодавства, яким є інститут забезпечення кібербезпеки. *Охарактеризовано* такі його властивості: 1) сформований і розвивається на базі матеріальних та процесуальних норм інформаційного, конституційного, цивільного, адміністративного, кримінального, процесуального, фінансового й інших галузей законодавства; 2) як самостійний інститут формується на основі нечисленної сукупності юридичних норм, що регулюють специфічне коло суспільних відносин стосовно забезпечення безпекових інтересів людини, суспільства, держави в інформаційній сфері; 3) як складова підгалузі правового регулювання інформаційної безпеки в системі інформаційного законодавства взаємопов’язаний з іншими інститутами цієї підгалузі – охороною комерційної та державної таємниці, захисту персональних даних і низка інших; 4) в основі змісту лежать норми зазначених вище галузей права, що об’єднані спрямованістю на забезпечення безпекових інтересів людини, суспільства, держави в кіберпросторі;

– *розроблено* концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів;

– *запропоновано* логічну схему співвідношення кібернетичної та інформаційної безпеки. Обґрунтовано, що кібербезпека формується в реляційних відносинах з безпекою мереж, безпекою інтернету і безпекою

додатків, а також здійснює підтримку безпеки критичної інформаційної інфраструктури в частині, що її стосується;

– *виокремлено* та *систематизовано* складові національних інтересів України в кіберпросторі: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновлення держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни; 2) інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України;

– *розроблено* нові механізми співпраці між приватним сектором та державними органами у процесі забезпечення кібербезпеки України. Виокремлено такі пріоритетні напрями: розвиток кіберрозвідки, аудит кібербезпеки, взаємний обмін інформацією щодо кіберзагроз, заміна нормативних документів в галузі технічного захисту інформації на ефективніший та сучасніший базовий стандарт і запровадження галузевих стандартів кібернетичної безпеки, створення галузевих центрів з реагування на кібернетичні інциденти (Security Operations Center (SOC)) та центрів інформаційного обміну про кібернетичні атаки (Information Systems Audit and Control Association (ISACA)), створення на базі національних навчальних

закладів тренінгових центрів для налагодження ефективного діалогу у рамках державно-приватного партнерства з протидії кіберзагрозам.

удосконалено:

– базові поняття дослідження: «кібернетична безпека України», «забезпечення кібернетичної безпеки України», «кібератака», «кіберпростір», «кіберзлочин», «стан захищеності», «кіберзагроза», «інформаційна інфраструктура України», «критична інформаційна інфраструктура» що дозволить упорядкувати понятійно-категоріальний апарат інформаційного права;

– тлумачення терміна «*культура кібербезпеки*», під яким розуміється система переконань, уявлень та етичних норм щодо ведення інформаційної діяльності в кіберпросторі, знань, умінь і навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності у кіберпросторі;

– підхід до системно-функціонального аналізу суб'єктів забезпечення кібернетичної безпеки України, у частині розвитку державно-приватного партнерства, розширення функціональних повноважень Національного координаційного центру кібербезпеки, удосконалення функціональних завдань Служби безпеки України;

– критерії класифікації кіберзагроз державі, зокрема: загрози існуванню нації, за деструктивним впливом на основні сегменти національного кіберпростору, за посяганням на національні цінності кібербезпеки (життєво важливі інтереси людини і громадянина, суспільства та держави);

– теоретичний підхід у рамках якого кіберпростір може розглядатися одночасно як об'єкт правового захисту і як джерело загроз. На цій основі у пріоритеті рівнів кібербезпеки (безпека людини, суспільства й держави, в основу якого покладені конституційні принципи захисту життєво важливих інтересів зазначених суб'єктів) стосовно кібербезпеки запропоновано надати пріоритет інтересам держави, оскільки від цього безпосередньо залежатиме й реалізація інтересів особи й суспільства. Забезпечення

кібербезпеки держави є передумовою особистісної та громадської кібернетичної безпеки

– критерії класифікації загроз кібербезпеці людини, у частині їх впливу на національну свідомість; за посяганням на національні цінності; за природою виникнення;

– роль правового чинника, як єдиного регулятора процесів та відносин у сфері роботи глобальної мережі Інтернет, розвитку Інтернету-речей (IoT), інтелектуалізації робототехніки, використання можливостей кіберсистем, мікрочіпів, нанотехнологій, їх упровадження в інформаційні процеси управління, взаємодії людини і влади, у повсякденній життєдіяльності «цифрової людини»;

– систему забезпечення кібербезпеки людини, суспільства, держави в контексті доповнення до її структури соціальної та морально-етичної складових;

– пріоритетні напрями розвитку правових основ державної політики у процесі забезпечення кібернетичної безпеки з урахуванням досвіду європейських країн і сучасної обстановки в нашій державі.

дістали подальшого розвитку:

– теоретичні засади утвердження інформаційного права як самостійної галузі права та розширення меж його правового впливу, у частині удосконалення законодавства про забезпечення кібернетичної безпеки України;

– теоретичні положення щодо розвитку інформаційно-правових досліджень правового регулювання кібернетичної безпеки України;

– теоретичні підходи до змісту, динаміки розвитку сучасних загроз кібернетичній безпеці України та механізмів протидії їм;

– узагальнення зарубіжного досвіду забезпечення кібернетичної безпеки, що створює правову базу побудови системи кібернетичної безпеки в Україні, здійснення гармонізації національного законодавства з міжнародними стандартами та європейським законодавством.

Практичне значення одержаних результатів. Висновки і пропозиції були впроваджені та можуть бути використані:

– *у правотворчій діяльності* – при підготовці змін і доповнень до законодавчих та відомчих нормативно-правових актів, що стосуються питань забезпечення кібернетичної безпеки України;

– *у правоохоронній діяльності* – при удосконаленні практичних засад забезпечення кібернетичної безпеки України *(акт впровадження від 05.03.2021р. Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України*);

– *у правозастосовній практиці* – під час реалізації завдань аналітичної діяльності, прогнозування й моніторингу кіберзагроз в Україні *(акт впровадження від 13.01.2021р. № 12 Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю РНБО України)*;

– *у науково-дослідній діяльності* – як основа для подальших теоретичних і практичних розробок системи забезпечення кібербезпеки, а також опрацювання проблемних питань інформаційного права. Окремі положення дослідження враховано в науково-дослідній роботі Науково-дослідного інституту інформатики і права НАПрН України *(акт впровадження від 16.12.2020р.)*;

– *у навчальному процесі* – під час розробки й оновлення навчально-методичного забезпечення навчальних дисциплін «Кібербезпека», «Інформаційне право», «ІТ-право».

Особистий внесок здобувача. Дисертаційна робота є самостійною науковою працею. Викладені в дисертації наукові положення, висновки і рекомендації, що винесені на захист, отримані дисертантом самостійно. Для обґрунтування деяких висновків використано праці інших учених, на які зроблено посилання. Із праць, опублікованих у співавторстві, використано ідеї та положення, що одержані особисто здобувачем. Особистий внесок автора в наукові праці, виконані у співавторстві, становить: «Глобальна культура

кібербезпеки в системі запобігання кіберзлочинності в Україні» (60 %), «Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності» (60 %), «Протидія загрозам кібербезпеці держави на глобальному рівні» (60 %); «Національні інтереси України в кібернетичній сфері» (70 %).

Апробація результатів дослідження. Результати досліджень, викладені в дисертації, були представлені у вигляді доповідей і виступів на таких наукових заходах, як:

– *міжнародні науково-практичні конференції*: «Досудове розслідування: актуальні проблеми та шляхи їх вирішення» (м. Харків, 26.10.2018); «Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення» (м. Харків, 23.05.2019); «Актуальні проблеми правових наук в євроінтеграційному вимірі» (Харків, 20–21.12.2019); «Теоретичні та практичні проблеми правового регулювання суспільних відносин (м. Харків, 17–18.01.2020); «Реформування національного та міжнародного права: перспективи та пріоритети» (м. Одеса, 17–18.01.2020); «Нові завдання та напрями розвитку юридичної науки у XXI столітті» (м. Одеса, 21–22.02.2020); «Міжнародне та національне законодавство: способи удосконалення» (м. Дніпро, 3–4.04.2020); «Міжнародні та національні правові виміри забезпечення стабільності» (м. Львів, 17–18.04.2020); «Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні» (м. Запоріжжя, 24–25.04.2020); «Розбудова правової держави в Україні: реалії та перспективи» (м. Одеса, 29.05.2020); «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 26.11.2020);

– *всеукраїнські науково-практичні конференції*: «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку» (м. Острог, 14.05.2019); «Актуальні проблеми управління інформаційною безпекою держави» (м. Київ, 30.03.2018); «Актуальні проблеми управління інформаційною безпекою держави» (м. Київ, 4.04.2019); «Захист прав, свобод

і безпеки людини в інформаційній сфері в сучасних умовах» (м. Київ, 21.05.2020); «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» (м. Київ, 10.12.2020).

Публікації. Основні положення та висновки дисертації викладено в 40 наукових працях, зокрема в 2 індивідуальних монографіях, у розділі в 1 колективній монографії, у 22 статтях, що опубліковані у фахових виданнях України, наукових періодичних виданнях інших держав і наукових періодичних вітчизняних виданнях, що внесені до міжнародних наукометричних баз даних (6 із яких – у наукових періодичних виданнях інших держав), у 15 тезах доповідей на конференціях.

Структура та обсяг дисертації зумовлена метою й завданнями дослідження та складається зі вступу, п’яти розділів, що містять 19 підрозділів, висновків до кожного розділу та загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 461 сторінка, з яких основного тексту – 381 сторінка. Список використаних джерел розміщено на 41 сторінці (407 найменувань), додатки – на 8 сторінках.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

1.1 Ґенеза наукових поглядів забезпечення кібербезпеки України

Значення для людства впровадження Інтернету та вільного доступу до нього важко переоцінити. Він не лише сприяв значному підвищенню ефективності діяльності у науковій, економічній та інших продуктивних сферах, але й зумовив виникнення унікальних можливостей для обміну інформацією, ідеями, культурами врешті-решт поміж роз'єднаними простором чи іншими обставинами людьми, групами, народами. Тому не буде перебільшенням твердження, що Інтернет спричинив глобальну революцію – наукову, комунікативну, бізнесову тощо.

Водночас інтернет- (чи кібер-) простір має безліч зв'язків та з'єднань, а це зумовлює наявність серйозних ризиків, оскільки охоплення, можливості та функції, які постійно зростають і розширюються, збільшують потенції не лише законослухняних, а й зловмисних користувачів. У такому разі зловмиснику, аби отримати певний зиск, варто лише віднайти найуразливішу ланку в мережі опонента та здійснити на неї «рейдерську» кібератаку. При цьому дрібні, локальні, здавалося б, проблеми, здатні значно збільшуватися, стрімко поширюватися, створюючи системні загрози та ризики.

Сьогодні вже не треба нікого переконувати, що вразливість у кіберпросторі є цілком реальною та небезпечною й поширюється досить швидко. Цілями кібератак стають суб'єкти державного управління, об'єкти особливо важливої інфраструктури, різноманітні комунікації, військові, розвідувальні структури, особливо їхні керівні й контрольні органи,

торговельно-економічні, фінансові та логістичні операції, системи попередження й ліквідації надзвичайних ситуацій тощо, які значною мірою залежать від функціонування ІТ-мереж. «Кібервикрадення» – від корпоративної та особистої інформації й коштів, інтелектуальної власності аж до державних таємниць – набули глобальних масштабів, впливаючи практично на всі сфери людської життєдіяльності.

Походження, наміри, потенції, масштаби діяльності, ресурсна база суб'єктів, які використовують Інтернет із метою завдання фізичної шкоди й порушення чи пошкодження цифрової інфраструктури, найрізноманітніші. Такими суб'єктами можуть виступати як держави в особі своїх урядів, розвідувальних, військових та інших структур, так і недержавні утворення – злочинні, зокрема терористичні, угруповання, які зазвичай чітко зорганізовані й оперують значними коштами, окремі хакери чи «звичайні» злочинці, невдоволені працівники чи інші особи, котрі мають доступ до конфіденційної інформації.

Крім того, кіберпростір надає широкі можливості для ведення асиметричних, так званих «гібридних», воєн. Нападників приваблюють вельми невисокі матеріальні витрати для проведення кібератак на об'єкти важливої інфраструктури противника й доволі низький рівень технічної підготовки, потрібний для цього. Напередодні збройного нападу Росії на Грузію у 2008 році агресор провів низку кібератак, паралізувавши роботу багатьох грузинських урядових, військових, комунікаційних та інших структур [1]. Подібні приклади можемо простежити у всіх випадках збройних конфліктів за останні декілька десятиліть, а особливо з початком воєнної агресії Росії в Криму та східних теренах нашої країни.

Воєнні зазіхання охопили не лише земний, водний, повітряний і космічний простори, а й чи не єдину раніше вільну від цього сферу – кіберпростір [2, с. 6], який складається з усієї множини світових комп'ютерних мереж і всього, що вони з'єднують та контролюють, чим управляють за допомогою різноманітних інтерфейсів. І це не лише власне глобальна відкрита

мережа Інтернет, а й безліч інших електронних каналів, які відділені від Інтернету (принаймні, на це сподіваються їхні володільці, окремі з цих приватних мереж, зовні схожі на Інтернет, ізольовані від нього, хоча б теоретично). Ще однією складовою кіберпростору є транснаціональні мережі, в яких, приміром, циркулює інформація про фінансові потоки потоках, різноманітні біржові та кредитні операції тощо. За допомогою, зокрема, технологій радіочастотної ідентифікації (РЧІ) [3] налагоджені такі системи отримання й контролю даних, які дають змогу «міжмашинного спілкування», що отримало назву «Інтернет речей». Скажімо, пульти управління, «ведуть перемови» з технологічними лініями, електрогенераторами, промисловим, будівельним, побутовим чи іншим устаткуванням.

Такі мережі є об'єктами зацікавленості кібернетичних зловмисників, котрі можуть, зламавши їхній захист, встановити над ними власний контроль, порушити функціонування або взагалі їх знищити. Більше того, з допомогою такого контролю можна впливати на поведінку людей, їхні світогляд та світосприйняття. Такий контроль може призвести також і до заволодіння всією інформацією або ж до впровадження команд системам управління банківськими операціями, промисловими підприємствами, енергетикою, транспортом, військовими об'єктами тощо, які спричинять техногенні катастрофи, загибель людей, руйнування та інші наслідки. Знищення ж мереж, інформації, що в них циркулює може призвести до руйнації найважливіших систем життєдіяльності людської спільноти – фінансових, енергетичних, постачання їжі та продукції, залізничного й авіатранспорту, зв'язку та ін. Якщо контроль за цими системами не буде швидко відновлений, це за лічені дні може викликати серйозні фінансово-економічні й соціально-гуманітарні проблеми. Зазначимо, що це не абстрактні міркування, оскільки подібне, у більших чи менших масштабах, уже траплялося – чи то в експериментальному вигляді, чи як наслідок помилкових дій або злочинних кібератак, чи то в результаті справжньої кібернетичної війни.

Інформація, розміщена в електронних мережах керування об'єктами

названих вище та інших життєво важливих сфер, може бути атакованою з віддалених місць і використаною зі злочинною метою. Така можливість об'єктивно зумовлена самою природою кіберпростору, а також неминучими похибками у всесвітній комп'ютерній мережі, вадами відповідного обладнання та програмного забезпечення, прагненням охопити он лайн операціями усе більшу кількість важливих систем, брак чи відсутність надійних засобів і способів захисту.

Тому загрози, що виникають у кіберпросторі, такі ж численні й різноманітні, як і сам цей простір. Їм притаманні масштабність, взаємозв'язок, швидкість поширення, складність розуміння загроз і реагування на них. При цьому від кібератак, які здійснюються не лише з географічно віддалених місць, а й із-за меж фізичного простору – у цифровому кібернетичному просторі, не існує ідеального захисту. Постійне вдосконалення інтернет-технологій зумовлює відповідне зростання небезпечності, швидкості й руйнівної потужності кібератак, проводити які стає все простіше й дешевше, тоді як захист від них потребує все більших зусиль і витрат. Сьогодні маємо чимало прикладів, коли один комп'ютерний злодій викрадає більше грошей, ніж великі банди грабіжників банків.

Ситуація ще більше ускладнюється тим, що сама природа Інтернету суперечить традиційним уявленням про те, що і суверенні країни, і бойові дії прив'язані до географії та фізичного місцезнаходження. Компанія може мати головний офіс в одній країні, а мережі й сервери — в іншій. Якщо кібератаку спрямовано проти цих мереж і серверів, хто має реагувати: країна, де розташовано головний офіс, чи країна, де розміщено мережі й сервери? Якщо не реагуватиме жодна із цих двох країн, а натомість корпорація захищатиметься сама, організувавши власний кібернаступ, то хто ще буде втягнений у цю ситуацію? Якщо немає міжнародних норм і договорів, що дають визначення і встановлюють межі кіберконфліктів, то кібервійна може відбуватися між двома країнами, а може між країною і компанією.

Протягом сотень років пограбування банку передбачало, що в

приміщення вдираються озброєні люди, набивають міхи грошима й зникають у невідомому напрямку. Відповідальність за те, щоб знайти, затримати та покарати крадіїв, було покладено на правоохоронців. Нині перед правоохоронними органами та спеціальними службами постало питання: як уряду трактувати кібератаки, що спустошують рахунки розташованого на їхній території комерційного банку, — як напад на їхню державу, як пограбування чи як щось зовсім інше? Відповідно необхідним є розроблення критеріїв трактування подібних інцидентів, із метою їх чіткої класифікації на предмет загроз безпеці людині, суспільству, державі з подальшою їх правовою оцінкою.

Це ж стосується й можливостей терористів, коли лишень один комп'ютер може спричинити більш тяжкі катаклізми, ніж цілий арсенал традиційної зброї. На жаль, така тенденція швидко посилюється, вагомих аргументів до її стримування поки що немає, і сучасна кіберзлочинність набуває характеру глобальної цифрової епідемії.

Зважаючи на безпекові виклики, пов'язані із забезпеченням кібернетичної безпеки, абсолютно слушною вбачається теза, що «конструкція Інтернету впливає на соціальні відносини, які виникають навколо глобальної мережі, і сприяє формуванню кіберкультури – специфічної форми культури інформаційного суспільства» [4, с. 23]. Отже, створена людським розумом і працею віртуальна реальність, глобальна всесвітня мережа Інтернет стають моделлю буття соціуму, чинником соціальної дійсності, який усе більше впливає як на свідомість окремого індивіда, так і на групову, масову, загальносуспільну свідомість. Усе зростаючими темпами відбувається загальна «віртуалізація» індивідуального й суспільного життя, про що, зокрема, свідчить поширення таких явищ, як віртуальні гроші, інтернет-торгівля, віртуальне навчання, електронне урядування тощо. Тобто феномен віртуальної реальності давно вийшов за межі комп'ютерної техніки й інформаційно-телекомунікаційних мереж, у кіберпросторі закладені й уже реалізуються величезні комунікативні, медійні, пізнавальні, управлінські та

інші потенції, широкі можливості керування фінансовими потоками, реалізації демократичних процедур тощо.

Отже, пріоритетними стають такі нові категорії, як кіберкультура. Як відомо, існує достатня кількість визначень поняття «культура», які розглядаються у філософії, культурології, педагогіці, психології, соціології, економіці й інших галузях знань, жодне з яких поки що не стало загальноприйнятим. Спільну основу цих визначень можна виділити те, що культура людини утверджується як комплекс якостей, які людина виробила в собі власними зусиллями, і вона є проявом людської самосвідомості.

У межах цього дослідження слід звернути увагу на поняття інформаційної культури, а також співвідношення між поняттями інформаційної культури та культури кібербезпеки.

Аналіз підходів до сутності інформаційної культури [5, с. 169], які сформувалися в різних галузях знань, свідчить, що розуміння цього поняття є неоднозначним. Спільною рисою, зокрема, є визнання детермінаційних зв’язків між рівнем інформаційної культури і розвитком певної сфери професійної активності особистості. Відмінності полягають у широкому та вузькому охопленні ознак інформаційної культури, від навичок володіння окремими інформаційними технологіями (комп’ютерної грамотності) до опанування знань та навичок майже у всіх сферах людської діяльності. З погляду на визначення корпоративної культури становить інтерес таке визначення інформаційної культури у вузькому розумінні [6, с. 38]: інформаційна культура в управлінській діяльності включає культуру правил організації подання, сприймання та використання інформації, культуру правил суспільних відносин із використанням мережі Інтернет та культуру суспільних правовідносин із застосуванням нових комп’ютеризованих інформаційних технологій.

Тому з погляду на предмет дослідження зосередимо увагу на вузькому розумінні поняття інформаційної культури, обмежуючись сутністю корпоративної культури безпеки у кіберпросторі – цифровою грамотністю та

культурою безпекового поводження у кіберпросторі.

Ототожнення культури кібербезпеки як складової інформаційної культури у вузькому розумінні уявляється обґрунтованим, оскільки безпековий аспект є важливою частиною інформаційних відносин, що передбачають використання сучасних ІТ-технологій мережі Інтернет [7, 8].

Поняття культури кібербезпеки (у розумінні захисту інформації) почало поширюватись у світі після прийняття у 2003 році Резолюції Генеральної Асамблеї ООН «Створення глобальної культури кібербезпеки». У звіті Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) 2017 року «Культура кібербезпеки організації» запропоновано таке визначення культури кібербезпеки [9]: знання, переконання, уявлення, норми і цінності людей по відношенню до кібербезпеки та використання інформаційних технологій. Формування культури кібербезпеки в організації спрямоване на зміну мислення співробітників, сприйняття ризику та спільної відповідальності за забезпечення кібербезпеки організації, сприйняття заходів із забезпечення особистої кібербезпеки як побутової звички.

Складовими культури кібербербезпеки, визначеними у Резолюції Генеральної Асамблеї ООН, є:

- обізнаність – учасники повинні бути інформовані про ризики та необхідність забезпечення кібербезпеки, а також про свої можливості у підвищенні стану захищеності;
- відповідальність – учасники відповідають за безпеку інформаційних систем та мереж згідно зі своєю роллю у системі кібербезпеки;
- реагування – учасники повинні вживати своєчасних і спільних заходів щодо попередження інцидентів, які стосуються кібербезпеки, їх виявлення та реагування на них;
- переоцінка – учасники повинні піддавати оцінюванню стан забезпечення кібербезпеки та вносити належні зміни в політику, практику, заходи і процедури забезпечення кібербезпеки, враховуючи при цьому появу нових і зміну колишніх загроз і чинників уразливості;

– етика – учасники повинні враховувати законні інтереси інших і визнавати, що їхні дії або бездіяльність можуть зашкодити іншим.

Можна виокремити рівень корпоративної культури кібербезпеки та глобальний рівень кібербезпеки. У першому випадку йдеться про компетентність та корпоративні цінності, пов’язані із забезпеченням особистої та корпоративної безпеки в кіберпросторі у відповідності до визначеної політики кібербезпеки окремої особистості чи установи.

Наприклад, політика кібербезпеки установи повинна бути орієнтована передусім на попередження загроз витоку електронної інформації щодо результатів досліджень до їх офіційного опублікування та/або оформлення авторських прав, попередження випадків неправомірного звинувачення у порушенні авторських і суміжних прав та негативного впливу на іміджеві позиції співтовариства.

Реалізація політики кібербезпеки повинна передбачати заходи захисту корпоративної та особистої кібернетичної інфраструктури співробітників установи від загроз несанкціонованого доступу до електронної інформації, її модифікації та знищення, передбачати можливість доведення авторства, цілісності та дати виготовлення електронної інформації, урегулювання питань щодо безпечного використання технологій мережі Інтернет. Політика кібербезпеки установи повинна передбачати заходи корпоративної взаємодії та реагування на інциденти порушення безпеки інформації й інформаційно-психологічної безпеки в межах діяльності установи.

Особиста кібербезпека співробітника установи є основним спрямуванням заходів формування корпоративної культури кібербезпеки, орієнтованим на засвоєння необхідних умінь та навичок захисту, що стосуються як технічних, так і психологічних аспектів, так званої соціальної інженерії і можливостей інформаційно-психологічного впливу. Відповідно, основними складовими формування корпоративної культури кібербезпеки можна визначити навчання та мотивування співробітників установи, етичний контроль зокрема.

Основними принципами формування корпоративної культури кібербезпеки установи можна вважати своєчасність, зрілість та доступність заходів із формування у співробітників корпоративних етичних норм безпекового поводження в кіберпросторі.

Методи формування корпоративної культури кібербезпеки установи доцільно розглядати в межах сфери компетенції підрозділу управління персоналом, оскільки потрібно враховувати особистість кожного співробітника, пропонувати індивідуальні мотиватори для сприйняття, усвідомлення та опанування технологій кіберзахисту.

Узагальнюючи результати проведеного дослідження, маємо всі підстави для твердження, що в сучасних умовах розвитку та впровадження ІТ-технологій в Україні заходи формування культури кібербезпеки є доволі ефективним механізмом протидії кіберзлочинності. І, звісно, йдеться про системні заходи забезпечення кібербезпеки в розрізі небезпек життєво важливим інтересам особистості у кіберпросторі, з позицій захисту інформації та інформаційно-психологічного захисту (захисту від інформації) відповідно. Детальніше розглянемо ці питання в наступних розділах роботи.

Глобальна культура кібербезпеки – це шлях вирішення проблеми підвищення рівня кіберзахисту особи та суспільства з використанням соціальних заходів на міжнародному й національному рівнях. Актуальність цієї проблеми обумовлена наявними та прогнозованими тенденціями збільшення кількості кримінальних правопорушень у кіберпросторі у зв’язку зі значним поширенням технологій електронної економіки та урядування, безпрецедентними масштабами комунікації в кіберпросторі спільнот національного та міжнародного виміру.

Історично термін «культура кібербезпеки» був використаний саме у глобальному розумінні в Резолюції Генеральної Асамблеї «Створення глобальної культури кібербезпеки» (Creation of a global culture of cybersecurity) у 2002, 2003 та 2009 роках, хоча в цих документах не запропоновано його визначення. Зазначені документи були визначені як рекомендації для

розроблення національних стратегій кібербезпеки, що визначають сутність національних систем кібербезпеки та заходи з поширення передових практик кіберзахисту.

Досліджуючи дефініцію «глобальна культура кібербезпеки», доцільно звернути увагу на концепти масової та глобальної культури. Спираючись на поняття кібербезпеки і кіберпростору, під «масовістю» розумітимемо обсяг носіїв культури, фактично, широкі верстви населення – масового користувача. Під «глобальністю» розуміємо не інтеграцію національних культур, а феномен наднаціональної професійної культури. Тобто глобальну культуру кібербезпеки можна розглядати як наднаціональну масову культуру кібербезпеки, що охоплює категорії «культура кібербезпеки», «інформаційна культура», «професійна культура», «культура» тощо.

Очевидно, що дослідження проблеми формування глобальної культури кібербезпеки має міждисциплінарний характер та потребує розгляду з позицій філософії, культурології та соціології.

Термін «культура» походить від латинських слів: «colo», що означає «обробіток»; «colore» – «обробляти, вирощувати», а пізніше – «поклонятися та вшановувати богів та предків»; «cultura», що означає «обробіток, виховання, освіта» – систему надбіологічних програм людської діяльності, поведінки, спілкування, які історично еволюціонують. У сучасному розумінні культура – це складний суспільний феномен життєдіяльності людини, що стосується побуту, дозвілля, способу життя як окремої особи, так й усього суспільства [10, с. 477].

У філософії культура (матеріальна і духовна категорія) розглядається у всесторонньому історичному розумінні як:

– процес розвитку людських сил і здібностей; показник міри людського в людині;

– характеристика розвитку людини як людської істоти;

– процес освоєння природи, який одержує своє зовнішнє вираження у всьому багатстві та різноманітті створюваної людьми дійсності, у всій сукупності результатів людської праці і думки.

При цьому, на думку більшості сучасних філософів, у структурі феномена культури можна виділити два класи елементів. Перший характеризує культуру як систему еталонів суспільної поведінки людей, другий – як систему, що здійснює соціальний контроль над цінностями та ідеями. Вочевидь, у контексті запобігання кіберзлочинності доцільно розглядати матеріальну культуру в розумінні системи еталонів суспільної поведінки людей.

На цей час у культурології виділяють передусім такі аспекти культури як неприродного штучного явища:

– генетичні – культура є продуктом суспільства з позиції її виникнення;

– гносеологічні – культура є сукупністю досягнутих у процесі освоєння світу матеріальних і духовних цінностей;

– гуманістичні – культура є розвитком самої людини, її духовних, творчих здібностей;

– психологічні – культура є процесом адаптації до життєвого середовища, навчання та формування звичаїв;

– історичні – культура є процесом соціального наслідування та формування традицій;

– структурні – культура є організованими повторювальними реакціями суспільства звичаями та традиціями;

– правові – культура є системою, що регулює соціальні відносини в суспільстві, орієнтує людину у світі;

– соціологічні – культура є обмеженнями в діяльності конкретного соціального суб’єкта, а також станом і розвитком тієї чи іншої діяльності.

Загалом у соціології культура вважається життєвим устроєм суспільства (мова, звичаї, символи і об’єкти матеріальної культури) та результат

соціальної взаємодії:

– щодо створення, засвоєння, збереження та розповсюдження предметів, ідей, ціннісних уявлень, які забезпечують взаєморозуміння людей у різних соціальних ситуаціях;

– соціальних суб'єктів із життєвим середовищем, який забезпечує формування досвіду, розвиток форм та способів діяльності.

Соціологія культури – це спеціальна соціологічна теорія, яка вивчає закономірності функціонування культури в суспільстві через призму трьох основних складових: ставлення людей до природи; ставлення до інших людей; ставлення людини до самої себе (самопізнання, самовиховання, самовдосконалення, саморозвиток).

До того ж, загальновідомо, що правова культура – це система правових цінностей, що відповідають рівню досягнутого суспільством правового процесу і відбивають у правовій формі стан свободи особи та інші соціальні цінності. Культура управління являє собою культурологічний підхід до змісту, видів, функцій та методів управління, стосується процесу управління, спирається на мораль, етику, естетику й особливості професійної діяльності. Інформаційна культура у вузькому розумінні ототожнюється з поняттям цифрової грамотності (компетентності – знання, вміння і навички, особистісні якості суб'єктів інформаційної діяльності), яка необхідна для ефективної інформаційної діяльності.

Кіберкультура передбачає також [11, с. 177] «високий рівень загальної культури міжособистісного спілкування; готовність толерантно сприймати іншу точку зору; вміння аргументовано вести дискусії, готовність визнати себе переможеним у цій дискусії; готовність не тільки отримувати нові знання, а й ділитися своїми; знання норм і правил, що регламентують використання інтелектуальної власності і готовність користуватися ними тощо».

Виходячи із мети та завдань нашого дослідження, зосередимо увагу на таких аспектах професійної культури:

етичних нормах інформаційної діяльності, компетентності;

змісті, видах та методах професійного переконання суспільства щодо необхідності виконання етичних норм і технічних регламентів безпеки, формування професійної зрілості широких верств населення з питань кібербезпеки.

Крім того, звернемо також увагу на визначення культури кібербезпеки у звіті 2017 року Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) «Культура кібербезпеки організації» [12]: знання, переконання, уявлення, норми і цінності людей по відношенню до кібербезпеки та використання інформаційних технологій.

Отже, спираючись на отримані результати дослідження щодо запобігання кіберзлочинності та сутності професійної культури, під «*культурою кібербезпеки*» будемо розуміти систему переконань, уявлень та етичних норм щодо ведення інформаційної діяльності в кіберпросторі, знань, вмінь та навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності у кіберпросторі.

«Глобальною культурою кібербезпеки» будемо вважати наднаціональну масову культуру кібербезпеки суспільства, організацій та особистості.

Основною *метою формування глобальної культури кібербезпеки* є досягнення такого стану соціальної взаємодії між суб'єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів кіберпростору.

Далі зазначимо, що в Резолюції Генеральної Асамблеї ООН [13] було запропоновано дев'ять взаємопов'язаних принципів глобальної культури кібербезпеки:

1) обізнаність (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що вони можуть здійснити для підвищення безпеки);

2) відповідальність (учасники відповідають за безпеку мереж відповідно до своєї ролі);

3) реагування (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявленню та реагування, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне й ефективне співробітництво з попередження, виявлення та реагування на такі інциденти);

4) етика (врахування законних інтересів інших);

5) демократія (безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації);

6) відкритість та гласність;

7) оцінка ризиків (учасники повинні здійснювати періодичне оцінювання ризиків з метою виявлення загроз і факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації, яка захищається);

8) проєктування та впровадження засобів забезпечення безпеки;

9) переоцінка (належні та своєчасні заходи з внесення змін у політику, практику забезпечення безпеки з урахуванням нових та зміни існуючих загроз).

Світова практика формування глобальної культури кібербезпеки та реалізації зазначених принципів базується на рекомендаціях міжнародних організацій та національних ініціативах. Реалізується вона, насамперед, шляхом: інформування (формуванням обізнаності) широких верств населення, фахівців державних і приватних установ щодо існуючих загроз, заходів попередження їх реалізації, виявлення та реагування; формування та підтримки ринку засобів і послуг кіберзахисту, проведення відповідного навчання. Національні стратегії кібербезпеки передбачають механізми взаємодії та відповідальності в межах приватно-державного партнерства при реалізації заходів формування глобальної культури кібербезпеки.

Заходи формування обізнаності громадян із питань забезпечення

кібербезпеки відбуваються шляхом інформування співробітників організацій та установ різних форм власності: у засобах масової інформації; на веб-ресурсах державних і приватних структур; на конференціях, семінарах та тренінгах; при реалізації освітніх програм у середніх і вищих навчальних закладах. Формування та підтримка ринку засобів і послуг із забезпечення кібербезпеки передбачає: заходи нормативно-правового регулювання сфери технічного й криптографічного захисту інформації; створення громадських організацій для надання правової і технічної допомоги громадянам для забезпечення їхньої кібербезпеки; розбудову національної системи оповіщення про кібератаки та кіберінциденти; започаткування механізмів страхування ризиків та інших інструментів управління кібербезпекою.

У сучасних умовах державна політика з питань формування глобальної культури кібербезпеки повинна бути спрямована на ефективну координацію діяльності правоохоронних органів, державних і бізнес-структур, інститутів громадянського суспільства, мати за мету подолання цифрової нерівності та забезпечення доступності правових і технічних механізмів захисту особи в кіберпросторі.

Оскільки Інтернет, кіберпростір стали невід'ємною частиною практично всіх сфер життєдіяльності соціуму включно з виконанням державно-управлінських функцій, виникає потреба розроблення та впровадження у цій сфері суспільних відносин, зокрема й у галузі забезпечення безпеки в кіберпросторі (забезпечення кібербезпеки), чіткої державної політики. Політика Української держави у сфері забезпечення кібербезпеки являє собою систему науково обґрунтованих положень, принципів і поглядів, які визначають шляхи, засоби, форми й методи діяльності державних інституцій та громадянського суспільства із запобігання негативним тенденціям у кібернетичному просторі (завдання шкоди технічним засобам, матеріальному, соціально-політичному, духовному благополуччю особи, суспільства й держави), їх припинення, знешкодження та усунення негативних наслідків у разі реалізації.

З’ясувавши важливість кіберпростору для життєдіяльності будь-якої країни, розглянемо інший аспект кібербезпеки, який стосується власне кібернетичної складової, тобто загальних закономірностей процесів управління й циркулювання інформації в різноманітних системах. Базуючись на принципах теорії управління складними системами, дослідники цілком слушно до змісту поняття «кібернетична безпека» відносять і систему державного управління. Вони вважають, що в разі небезпеки «ураження» державних структур певною системною хворобою жоден природний інтелект окремих сумлінних і розумних управлінців, жоден штучний інтелект ЕОМ не в змозі здолати вади системи, і найнебезпечніше це в безпековій сфері, а передувсім у військовій та оборонній, де вади системи особливо дошкульні і для держави, і для суспільства, і для окремих громадян [14, с. 137].

Основою та запорукою здатності державних органів своєчасно приймати й ефективно втілювати управлінські рішення є інформація, її достовірність, оперативне транслювання об’єктам управління й добре налаштований зворотний зв’язок. Тому забезпечення кібербезпеки в її традиційному розумінні як несанкціонованого доступу до інформаційних ресурсів у цьому разі замало. Потрібне також запобігання можливим загрозам функціонуванню державному й суспільному інформаційно-управлінському інструментарію. Отже, під кібербезпекою слід також розуміти стан захищеності інформаційно-управлінської системи держави й суспільства, її стійкості до несприятливих внутрішніх та зовнішніх чинників, спроможності виробляти, приймати і втілювати в життя ефективні управлінські рішення.

Наведені вище міркування дають підставу для висновку, що кібернетична безпека є унікальним, універсальним явищем, продуктом світової цивілізації, розвиток якого потребує глибокого наукового осягнення, належного нормативно-правового врегулювання та створення відповідних структур, котрі мають забезпечувати національну безпеку України у глобальному кібернетичному просторі.

Як уже зазначалося, інформатизація не лише створює широкі

можливості для людини, суспільства й держави, а й висуває перед ними нові виклики, ставить усе складніші й невідкладніші завдання, одним із головних з яких є нормативно-правове регулювання інформаційних відносин. Негативні наслідки відставання від їхнього розвитку регуляторних правових механізмів можуть бути вельми серйозними, приклади чого були наведені вище. Тому потрібні постійний моніторинг та аналіз усіх процесів і явищ, які відбуваються в суспільному житті й державному будівництві, щоби своєчасно реагувати на них удосконаленням, актуалізацією відповідної правової бази.

Останнім часом у науковій літературі, засобах масової інформації та й у повсякденному житті «кібернетична» термінологія (кіберпростір, кіберзлочинність, кібертероризм, кібервійна тощо) застосовується дедалі частіше і стає загальновживаною. Водночас у нормативно-правових документах ці та інші подібні терміни визначені недостатньо й уживаються досить рідко.

Спробуємо з'ясувати, чи означає поширення вказаної термінології новий виток еволюції інформаційних відносин, чи це лише модна «фішка» для привертання уваги. Чи мають вони стосунок до сучасних проблем інформаційної та безпекової сфер та до власне науки кібернетики.

Кібернетика (від гр. kybernetike – мистецтво керування) – наука про загальні закони отримання, зберігання, передання й перероблення інформації. Головним об'єктом її дослідження є кібернетичні системи, які розглядаються абстрактно, незалежно від їхньої матеріальної сутності. Кожна з таких систем складається із множини взаємозв'язаних об'єктів – елементів системи, які здатні сприймати, запам'ятовувати, переробляти інформацію та обмінюватися нею. Кібернетика розроблює загальні принципи створення систем керування та систем для автоматизації розумової праці. Основними технічними засобами для вирішення завдань кібернетики є ЕОМ, тому її виникнення як самостійної науки пов'язане зі створенням у 40-х роках XX століття таких машин, а її теоретичний і практичний розвиток – з прогресом електронно-обчислювальної техніки [15, с. 571].

Отже, кібернетична наука, як бачимо, насамперед ґрунтувалася на понятті «управління», яке в широкому розумінні означає функцію організованих систем різної природи (біологічних, соціальних, технічних), яка забезпечує їх упорядкування, реалізацію програми та мети функціонування цих систем, приведення їх у відповідність до закономірностей навколишньої об'єктивної дійсності. Однак, деякі дослідники поняття управління використовують тільки стосовно живих систем і штучних систем управління – комп'ютерів і т.п.

Те, що значення і роль кібернетики в епоху становлення й розвитку інформаційного суспільства, проникнення інформаційних технологій в усі сфери життєдіяльності людства зростає, цілком природно. Якщо буквально кількадесят років тому на комп'ютерних технологіях розумілися лишень вузькі фахівці й письменники-фантасти, то сьогодні вони проникли в усі сфери життя, управлінські системи всіх рівнів, доступні практично кожному мешканцю навіть найбіднішої країни.

Не дивно, що інформаційна й управлінська проблематика, природа та співвідношення цих понять стали предметом дослідження багатьох учених. І попри широке розмаїття поглядів на ці питання, усі фахівці зазначають нерозривність управління та інформації, неможливість першого без другого.

У найзагальнішому вигляді система управління являє собою два пов'язаних прямими й зворотними зв'язками блоки: система, що управляє, та об'єкт управління. Керівний вплив передається системою управління каналами прямого зв'язку об'єктові управління, а від останнього каналами зворотного зв'язку транслюється інформація про його стан. Іншими словами, управління – це впорядкований обмін інформацією між елементами системи з метою підтримання їх у певному стані.

Проте, не варто забувати, що для кожного виду управління потрібна інформація, але не будь-яка, а певної спрямованості й відповідно структурована. Це, передусім, дані про об'єкт управління й надання їм форми, прийнятної для передання каналами зв'язку, після чого ця інформація

транслюється в керівну систему, скажімо, у комп'ютер чи безпосередньо людині. Базуючись на закладених в неї алгоритмах, система управління обробляє отриману інформацію, продукує керівні команди й транслює їх виконавчим структурам, що покликані змінювати стан об'єкта управління, здійснюючи на нього відповідний влив. Потім каналами зворотного зв'язку дані щодо стану об'єкта управління, дій виконавчих структур ретранслюються керівній системі, котра враховує цю інформацію під час вироблення наступних управлінських рішень.

Як бачимо, сутність елементів системи управління ідентична природі складових інформаційної сфери, до якої належать власне інформація, відповідна інфраструктура, суб'єкти інформаційних відносин та система засобів їх регулювання. Тому є всі підстави вважати управлінську інформацію, інфраструктуру та суб'єктів різновидом аналогічних структур інформаційних відносин.

У цьому контексті варто зіставити алгоритм здійснення управління й систему регулювання інформаційних відносин, природа та призначення котрих, як ми з'ясували вище, аналогічні й становлять підґрунтя формування управлінських впливів. Проте система регулювання інформаційних відносин складається із сукупності правил опрацювання інформації й вироблення рішень, управлінської інформації, яка зумовлює прийняття відповідних рішень, суб'єктів управління (компетентні у сфері інформаційних відносин державні органи та їхні службові особи), а також належну інфраструктуру. Тоді як алгоритм управління – це комплекс згаданих вище правил. Тобто інформаційні відносини є об'єктом управління системи їхнього регулювання, котра є різновидом кібернетичної системи, а кібернетична сфера є складовою сфери інформаційної. Ця кіберсфера має свої специфічні інформацію, суб'єктів, інфраструктуру та необхідні для провадження управління правила.

Водночас унаочнюються не лише нерозривні взаємозв'язки інформаційної та кібернетичної сфер, а й специфіка їхніх складників, що дає змогу виокремити загрози стосовно них, а також ураховувати ці особливості,

вирішуючи безпекові питання щодо управління. Отже, забезпечення інформаційної безпеки спрямоване на досягнення такого стану захищеності інформаційної сфери, коли вона убезпечується від здійснення існуючих загроз. А діяльність із забезпечення кібернетичної безпеки спрямована на унеможливлення порушень процесів управління завдяки створенню відповідного стану їх захищеності.

Ще однією відмінністю є особливості об’єктів розглядуваних видів діяльності. Так, на зміст забезпечення інформаційної безпеки практично не впливає специфіка об’єкта чи системи, у межах якої воно реалізується. Себто, і щодо держави в цілому, і щодо, скажімо, окремої організації чи установи ця діяльність полягає у забезпеченні безпеки інформації, відповідної інфраструктури, суб’єктів інформаційних відносин і системи регулювання останніх.

Що ж стосується кібербезпеки, то характер діяльності з її забезпечення значно більше залежить від специфіки певних процесів управління та кіберсистем, а вимоги, які висуваються до деяких видів управління, можуть істотно різнитися. Приміром, державному управлінню мають бути притаманні відкритість і доступність даних у контексті інформування громадян про діяльність владних інституцій і органів.

Натомість, надійна утаємниченість має бути забезпечена стосовно, скажімо, керування збройними силами держави. Мало того, активізація застосування у військовій сфері інформаційних технологій значно розширила перелік традиційних вимог до системи управління, основні з яких: ефективність, сталість, безупинність, оперативність, латентність. У сучасних реаліях висувається ціла низка принципово нових і надзвичайно важливих вимог, з-поміж яких: пристосованість до мінливих умов, способів і методів застосування війська; підтримання під час воєнних дій єдиного інформаційного простору; еволюційність розвитку; технологічна незалежність; спроможність до створення, акумулювання й нарощування потенціалу; здатність до оптимізації оперативного й допоміжного складу.

Як бачимо, залежно від призначення конкретної системи управління, вимог до неї, особливостей об’єкта управління, зовнішніх умов, стану і складу управлінських сил і засобів, від установленого порядку управління та інших чинників зміст забезпечення кібербезпеки може істотно різнитися.

1.2 Понятійно-категоріальний синтез забезпечення кібербезпеки України в науці інформаційного права

Реалії сьогодення свідчать про те, що в сучасному світі кібервійна, що проявляэться через атаки окремих хакерів, терористичних і злочинних угруповань, держав тощо, набула цілком конкретних обрисів. Конфлікти в віртуальному світі іноді мають асиметричний характер, тобто слабкіші в аспекті матеріальної сили гравці можуть використовувати кібервійну, щоб протистояти сильнішому супротивникові. При цьому кібервійна між країнами та коаліціями може бути завершена до початку застосування традиційної зброї і навіть без ведення бойових дій.

Вона швидкоплинна та несподівана, ведеться в реальному часі, і є малоресурсною. З метою ефективного відбиття кіберзагроз і забезпечення можливості проведення симетричної відповіді на виклики або завдання упереджувального удару, нагальною вимогою часу стає перегляд принципів забезпечення кібербезпеки як у мирний, так і воєнний час. Своєчасне планування та реалізація заходів забезпечення кібербезпеки й інформаційного протиборства на глобальному та регіональному рівнях стає одним із пріоритетних напрямів забезпечення національної безпеки кожної країни. Відтак набуває непересічної актуальності питання правового забезпечення кібербезпеки, а також питання розроблення й становлення понятійно-категоріального апарату забезпечення кібербезпеки.

Поняття кібербезпеки є вкрай багатогранним, тому складно формалізується, адже існує дуже багато різних уявлень і поглядів. У наш час у глобальному медіапросторі, публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн разом із доктринальною інституціалізацією кібербезпеки активно відбувається становлення її понятійно-категоріального апарату, який характеризують, зокрема, такі поняття, як «кібервійна», «кібератака», «кіберзброя», «кіберконфлікт», «кіберзагрози», «кібертероризм», «інформаційне протиборство», «інформаційний вплив», «інформаційна зброя» тощо.

Як зазначає А. Капто, поняття «кібервійна» означає вищий ступінь кіберконфлікту між державами, під час якого кібератаки, що проводяться проти кіберструктур противника, є складовими воєнної операції. Кібервійні передують спочатку «кібератаки», що передбачають застосування кіберзброї, а потім «кіберконфлікт», який становить напружену ситуацію, до якого залучено дві або кілька країн або політичних груп, коли ворожі кібератаки провокують дії у відповідь. Поняття «кіберзагрози» має низку значень залежно від того, у контексті якого феномена воно розглядається – кіберзлочинність, кібертероризм або використання інформаційних технологій у військово-політичних цілях (що власне і становить кібервійна). Окремий випадок застосування кіберзброї необов'язково призводить до кібервійни, іменується «кіберінцидентом». Серед кіберзловмисників науковець пропонує розрізняти: «кібертерористів» (кіберзлочинці, що спеціалізуються на зламі комп'ютерних систем, які навчили організовувати окремі кібератаки на глобальні мережі); «хакерів» (зловмисників, які проникають у державні та приватні інформаційні банки і які домагаються визнання своїх технологічних можливостей), серед яких розрізняють «кракерів», які керуються кримінальними інтересами, і політично мотивованих «хактивістів». На думку А. Капто, під «кібербезпекою» розуміють властивість кіберпростору, кіберсистем тощо протистояти умисним і неумисним загрозам, а також реагувати на них і відновлюватися в разі реалізації цих загроз, яка включає також розвиток

наступальних можливостей» [16].

Також можна навести такі визначення кібербезпеки:

- «стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [17, с. 60];
- «стан захищеності державних електронних інформаційних ресурсів у кіберпросторі від ризику стороннього впливу, виявлення та запобігання різних зовнішніх втручань через інформаційні системи, а також загрози національним та особистим інтересам» [18, с. 575];
- «стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі, в якому є можливим безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорон, захист інформації, а у вузькому сенсі – стан індивіда, суспільства та держави, де відсутня будь-яка небезпека» [19, с. 176-177];
- «один із видів національної безпеки держави, що являє собою стан захищеності від внутрішніх та зовнішніх загроз віртуальної реальності в кіберпросторі» [20, с. 42];
- «стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації» [21, с. 168];
- «сукупність спеціальних суб'єктів забезпечення кібернетичної безпеки, засобів та методів, що ними використовуються, а також комплекс відповідних взаємопов'язаних правових, організаційних та технічних заходів, що ними здійснюються» [22, с. 317];
- «сукупність узгоджених за завданнями елементів, які комплектуються та розгортаються за єдиним замислом і планом у кібернетичному просторі з

метою забезпечення кібернетичної безпеки інформаційних, телекомуніка-ційних та інформаційно-телекомунікаційних систем» [23];

- «стан захищеності кіберпростору держави в цілому чи окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним або національним інтересам» [24, с. 15];

- «основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки» [25, с. 53];

- «стан захищеності кіберпростору, що передбачає функціонування безпечного Інтернету, соціальних мереж, інформаційно-телекомунікаційних систем, вжиття з боку держави превентивних заходів щодо недопущення, блокування кібератак та актів кібертероризму» [26, с. 15-16];

– «стан захищеності життєво важливих інтересів людини і громадянина, юридичних осіб, суспільства та держави в кіберпросторі, який забезпечується комплексним ужиттям заходів кіберзахисту, заходів правоохоронного, військового, розвідувального, контррозвідувального, оперативно-розшукового, а також політичного, інформаційного, організаційно-правового, технологічного, соціального, освітянського характеру та передбачає організацію дієвого кіберзахисту з метою недопущення кібератак, настання кіберінцидентів, боротьби з кіберзлочинністю та кібертероризмом» [27, с. 29].

Як слушно зазначає Р. Лук’янчук, до 2014 року кібербезпека не визнавалася самостійною складовою національної безпеки, а вважалася винятково складовою інформаційної безпеки. Гібридна війна, розпочата проти України, зумовила перегляд системи державного управління кібербезпекою, у зв’язку з чим було внесено корективи до основних засад державної політики забезпечення національної безпеки [27]. Зокрема, у Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015

року № 287 [28] як самостійний напрям було визначено забезпечення кібербезпеки. Воєнна Доктрина України, затверджена Указом Президента України від 24 вересня 2015 р. [29], визначає, що основними завданнями воєнної політики України з урахуванням характеру актуальних загроз національній безпеці є, зокрема, поглиблення кооперації та співробітництва з НАТО та ЄС у контексті боротьби з кіберзлочинністю.

Слід зазначити, що термін «кібербезпека» є похідним від родового терміна «безпека», отже «кібербезпека» становить частину більш загального поняття «безпека», що вирізняється специфічними особливостями, й одночасно має виступати результатом синтезу поняття «безпека» та прикметника «кібернетична» (скорочено – «кібер»).

Базовою категорією в дослідженні кібербезпеки виступає категорія «безпека». У своєму дослідженні ми будемо керуватися поняттям «безпека», яке визначив український дослідник І. Корж. Вчений вважає, що в соціальному розумінні «безпека» означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних та потенційних загроз або уникнути їх, що, своєю чергою, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їх розвиток [30]. Такий підхід нами взятий як базовий у дослідження змісту кібербезпеки.

Створена ще в 1967 році Асоціація аудиту і контролю інформаційних систем (ISACA) у виданому 2014 року глосарії визначає *кібербезпеку* як «захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, котрі взаємодіють в мережах» [31]. А в аналітичному виданні «Трансформація кібербезпеки» детальніше тлумачить це поняття: «…Кібербезпека охоплює все, що захищає організації та фізичних осіб від умисних атак, порушень, інцидентів та їх наслідків. На практиці кібербезпека

стосується насамперед тих типів атак, порушень та інцидентів, які є цільовими, високотехнологічними та складними у виявленні чи управлінні. …Кібербезпека зосереджується на так званих складних спрямованих постійних загрозах (APT), кібервійнах та їхньому впливі на організації та людей» [32].

Передусім, з урахуванням наведеного вище, важливим видається визначення співвідношення кібербезпеки, інформаційної та національної безпеки.

У Законі України «Про національну безпеку України» визначено, що національна безпека України – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. У ч. 4 ст. 3 вказаного Закону зазначається, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо. Відповідно до ст. 19 того ж Закону завдання щодо контррозвідувального захисту державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об’єктів критичної інфраструктури покладається на Службу безпеки України. Це дає підстави вважати, що кібербезпека є самостійною складовою національної безпеки України, так само, як і інформаційна безпека. Закон України «Про національну безпеку України» передбачає також необхідність розробки стратегії кібербезпеки України – «документу довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [33].

Практика вживання понять «інформаційна безпека» і «кібербезпека» в правовій сфері свідчить про їхні суттєві відмінності, у результаті чого стає

очевидною потреба в пропозиціях, спрямованих на забезпечення єдності правового регулювання, що досягається через увпорядкування понятійно-категоріального апарату.

У сучасному світі інформаційна безпека становить органічне поєднання безпеки інформації та безпеки «від інформації» (за структурного підходу), а також постійний процес діяльності компетентних органів, спрямований на попередження, протидію загрозам в інформаційній сфері, а також застосування активних заходів інформаційного впливу та сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час [34] (за діяльнісного підходу). Натомість кібербезпеки, не зважаючи на свою інформаційну природу, є феноменом цифрового світу, який має більш виражений технологічний характер, що передбачає, зокрема, використання декількох протоколів безпеки. Тому згадані сфери інформаційної дійсності ніяк не можуть бути визначені поняттями з однаковим обсягом.

Як зазначають М. Безкоровайний та О. Татузов, «кібербезпека так само, як і кіберпростір може описуватися тріадою її складових: інформаційні ресурси, комп'ютерна та мережева архітектура (інфраструктура) і способи взаємодії користувачів» [35, с. 25]. Тож поняття «кібербезпека», як уже зазначалося вище, також має базуватися на понятті «кіберпростір», котрий доречно визначити як простір, в якому здійснюється функціонування і взаємодія кіберсистем (під кіберсистемою розуміється сукупність пов'язаних один з одним елементів, здатних сприймати, зберігати, переробляти інформацію, а також обмінюватися інформацією [36, с. 75] у цифровому форматі).

Кіберпростір є самостійною складовою інформаційного простору, що утворюється сукупністю автоматизованих інформаційних систем, комунікаційних каналів Інтернету та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечують їхнє функціонування, та цифрових інформаційних ресурсів. Функціонування в кіберпросторі передбачає також соціальну активність його суб’єктів (окремих осіб, їхніх

спільнот, країн тощо). Кіберпростір - це складне середовище, яка не існує в жодній фізичній формі, що виникає в результаті взаємодії людей, програмного забезпечення, інтернет-сервісів за допомогою технологічних пристроїв і мережевих зв'язків.

Кіберпростір формує будь-яка діяльність у мережевій, цифровій формі, а також інформаційний зміст і дії, що здійснюються за допомогою цифрових мереж [37]. Основний зміст кіберпростору полягає в діяльності користувачів цифрових інформаційних ресурсів та інформаційно-комунікаційної інфраструктури. Так само, як і кіберпростір, кібербезпека може описуватися тріадою складових:

1) інформаційні ресурси;
2) комп'ютерна та мережева архітектура (інфраструктура);
3) способи взаємодії користувачів.

Управління суб'єктами кіберпростору відіграє визначальну роль у виникненні, існуванні та підтримці основних властивостей цього середовища. Зазначені властивості, а саме численність елементів, що становлять кіберпростір, велика кількість взаємозв'язків між ними, можливість застосування спеціальних технік управління діями цих елементів, і визначають розвиток актуальних кіберзагроз [38]. У цьому контексті слід згадати, що власне прикметник «кібернетичний»/«кібернетична» є похідним від терміна «кібернетика», що становить науку про управління, отримання, передачу та перетворення інформації в кібернетичних системах. Вихідним поняттям кібернетики є управління, що являє собою результат виконання цілеспрямованої впорядкованої послідовності перетворень інформації в кібернетичній системі (об'єкті кіберпростору).

Можна виокремити низку глобальних безпекових викликів, пов'язаних із кіберпростором, а саме:

– сьогодні найбільшу небезпеку національній безпеці всіх країн у соціально-економічній, політичній, військовій та інших сферах несуть кіберзагрози, масштаби котрих, утім, дуже часто недооцінюються через

складність і слабке розуміння самого предмета, що заважає спрогнозувати наслідки реалізації загроз і розробити ефективні стратегії та засоби запобігання і протидії;

– багатоаспектна проблема забезпечення кібербезпеки стосується практично всіх сфер життєдіяльності суспільства, тому скласти вичерпний перелік конкретних загроз і виробити відповідні безпекові заходи практично неможливо;

– можливості кібернетичного простору, змога маніпулювання, зловживань, отримання переваг у ньому стають усе привабливішими для організованої злочинності;

– сьогоднішній кіберпростір, боротьба за домінування в ньому та здатність протистояти кіберзагрозам стали чи не найважливішими ареною та змістом агресії, воєнних дій. Отже, докорінно змінюватиметься не лише структура, а й сама природа збройних сил країн, коли головним складником військової могутності держави стане кібернетична потужність;

– глобальний характер проблем кіберпростору зумовлює потребу вироблення загальної стратегії запобігання, виявлення та протидії загрозам у масштабах усього безпекового сектору, реформування останнього й управління ним;

– кібернетичну безпеку неможливо забезпечити в одній окремій країні. Вирішення цієї проблеми потребує небувалої кооперації, інтеграції й акумуляції зусиль державних і приватних суб’єктів у загальносвітовому масштабі.

При цьому, якщо інформаційний простір - це природне і штучно створене середовище, в якому зокрема здійснюється обіг інформаційних проєкцій матеріальних об’єктів, то кіберпростір - це «техносвіт», який штучно створений і штучно розвивається. Також слід зауважити, що в кіберпросторі можуть реалізовуватись як загрози інформаційній безпеці, так і загрози іншим складовим національної безпеки – економічній, фінансовій, воєнній тощо. Підтвердження цієї тези можемо побачити у визначенні кібербезпеки,

закріпленому в Законі України «Про основні засади забезпечення кібербезпеки України», де встановлюється, що *кібербезпека* – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Власне кіберпростір у вказаному Законі визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [39].

Однак, визначений законодавцем підхід до змісту кібербезпеки, з предмета свого безпосереднього правового впливу опускає досить важливу складову, яка проявляється в результаті дії загроз кібербезпеці – це запобігання шкоди. Таке опущення, на нашу думку, не дає змоги повною мірою визначити мету правового регулювання.

Окреслений нами підхід правового регулювання кібербезпеки відображений у низці правових актів багатьох країн, зокрема, Національна стратегія кібербезпеки Нідерландів передбачає, що «кібербезпека – це сукупність зусиль щодо запобігання шкоди, що може бути заподіяна внаслідок збоїв у роботі ІКТ або неправильного їх використання, а також з відновлення ІКТ після реалізації цих загроз» [40]. У Стратегії кібербезпеки Канади передбачено, що рівень кібербезпеки визначається рівнем шкоди, що може бути завданий від кібератаки [41].

Незважаючи на те, що більшість визначень безпеки, зокрема й законодавчих, тлумачать це поняття через «захищеність», необхідно зауважити, що захищеність об'єкта - це його захист від зовнішніх джерел небезпеки, тоді як безпечність об'єкта - це передусім його внутрішня

властивість не бути джерелом небезпеки для навколишнього середовища. Відповідно, в англомовних наукових джерелах розрізняють «Cyber safety object» і «Cyber security object». Відтак, на нашу думку, поняття «кібербезпека» має включати як аспект «кіберзахищеності», так і аспект «кібербезпечності». Крім того, у визначенні кібербезпеки основний наголос і цільова установка повинні робитися на збереження сприятливого стану кіберпростору, а не на кількість чи якість загроз, яким необхідно протидіяти.

Дослідження поняття й сутності кібернетичної безпеки, аналіз наявних у цій сфері загроз дає змогу зробити певні висновки, а також запропонувати визначення деяких термінів.

Так, убачається необхідним розрізняти термінологічні словосполучення, похідні від термінів «інформація» й «кібернетика». Перші (інформаційна безпека, інформаційні загрози, інформаційна війна тощо) мають більш загальний зміст, і їх слід застосовувати до інформаційної сфери в цілому. Такі ж поняття, як кібернетичний простір, кібернетична злочинність, кібернетична війна і т.п., стосуються тих явищ, котрі пов’язані з управлінням, відповідними процесами й системами. На концептуальному рівні, у широкому розумінні, базові категорії цього дослідження можемо визначити таким чином:

Кібербезпека – це такий стан захищеності управління, який унеможливлює його порушення.

Забезпечення кібербезпеки – це діяльність із досягнення такого стану захищеності управління, який унеможливлює його порушення.

Кіберзагрози – це такі явища, дії, чинники та умови, котрі становлять для управлінських інформації, інфраструктури, суб’єктів і порядку небезпеку, яка полягає в можливості порушення властивостей одного чи декількох із зазначених складників, що може призвести до порушення управління.

Кібератака – це дії з метою порушення управління.

Окремо слід зазначити, що сучасний рівень розвитку інформаційної сфери зумовлює потребу виокремлення кібернетичної безпеки в самостійний вид безпеки, що дасть змогу, ураховуючи особливості відповідних систем і

процесів управління, реалізувати правові, організаційні й технічні можливості захисних заходів. Це також передбачає підвищення вимог до захисту вказаних систем і процесів залежно від їхнього призначення, рівня, складу тощо.

У сучасних умовах надзвичайно важливо правильно сформулювати поняття кібербезпеки та в цілому синтезувати понятійно-категоріальний апарат її правового забезпечення, оскільки від цього залежить, наскільки точно будуть визначені головні цілі роботи спецслужб і напрями використання засобів захисту кіберпростору від актуальних загроз національній безпеці та її складовим. Кібербезпека має на меті передусім забезпечення нормального функціонування кіберпростору, ефекетивно захищаючи його від виникаючих загроз. Отже, визначати кібербезпеку доцільно не лише як «стан захищеності», але й доцільно враховувати її діяльнісний аспект. Крім того, поняття кібербезпеки має включати як аспект «кіберзахищеності», так і аспект «кібербезпечності». За результатами проведеного дослідження може бути запропоноване таке визначення кібербезпеки – *це безпечність об'єктів кіберпростору й захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, у процесі чого забезпечено розвиток інформаційного суспільства, розвиток кіберкультури людини, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз безпеці України у кіберпросторі, а також постійний процес попередження й протидії відповідним загрозам*.

У цьому визначенні реалізується *визначальна мета державної політики в кіберпросторі*: забезпечення стану захищеності основних прав і свобод громадян на життя, здоров'я, фізичну й духовну недоторканність, доступ до інформації, законних інтересів людини, суспільства й держави в кібернетичному просторі від внутрішніх і зовнішніх загроз, що полягає в дотриманні загальновизнаних і встановлених міжнародною спільнотою обмежень на поширення завідомо недостовірної та шкідливої інформації, збереженні інформаційних ресурсів, їхньої цілісності, конфіденційності й недоступності для стороннього втручання, а також захисту інформаційно-

телекомунікаційних мереж і відповідного обладнання, котрі забезпечують розміщення, накопичення, обіг і використання інформації.

1.3 Співвідношення кібербезпеки та інформаційної безпеки

Сьогодення постає перед Україною з новими викликами та надскладними завданнями. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини та верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки і оборони в умовах обмежених ресурсів. Цілком погоджуємося з думкою М. Присяжнюка, що «запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави» [42, с. 45-46], що неможливо без чіткого усвідомлення сутності останньої. Цікавим є і той факт, що самі російські дослідники відзначають, що інформаційна безпека від другої половини XX сторіччя стає одним із найважливіших елементів національної безпеки.

Стаття 17 Конституції України визначає, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [43], що свідчить про набуття категорією

«інформаційна безпека» в нормативно-правовому аспекті конституційного статусу [44, с. 30].

Зауважимо, що система інформаційної безпеки, особливо на рівні її вихідних компонентів, може бути структурована за різними критеріями. Щодо кібернетичної безпеки, то Законом України «Про основні засади забезпечення кібербезпеки України» [39] вона визначена як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізуються законні інтереси суб'єктів інформаційних процесів. Тож «кібернетичний вимір» властивий усім складовим інформаційної безпеки. Варто зауважити, що кібербезпека нами розглядається як складова інформаційної безпеки (див. рис. 1).

Саме прийняття Закону України «Про основні засади забезпечення кібербезпеки України» означає для України закріплення на законодавчому рівні понятійного апарату з приставкою «кібер» і початок регулювання цифрової економіки в цілому.

Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої указом президента у 2016 році. Метою стратегії було створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства та держави. При цьому основний масив положень стратегії стосується сфери національної оборони і не зачіпає бізнес. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання та ратифікація Україною Конвенції про кібербезпеку. Країни – члени Ради Європи та деякі інші, які підписали конвенцію, взяли на себе зобов'язання вжити загальних та індивідуально-країнових заходів для запобігання злочинам у цифровій сфері.

Основним досягненням Закону «Про основні засади забезпечення кібербезпеки України» є імплементація в правове поле визначень, що стосуються кібербезпеки, кібератак і кіберзахисту.

Не вдаючись до детального аналізу цього Закону, можна визначити низку принципово важливих, на нашу думку дискусійних аспектів, які в перспективі слід буде доопрацьовувати та вдосконалювати:

– чи поширюється дія Закону на приватні мережі суб'єктів господарювання, адже такі мережі, усе ж таки, підключені до мережі Інтернет;

– неузгодженість та відсутність конкретизації повноважень суб'єктів національної системи кібербезпеки;

– декларативний зміст деяких положень, що потребує прийняття цілої низки конкретизуючих підзаконних нормативно-правових актів.

Крім практичної площини та зважаючи на відсутність єдності поглядів науковців щодо місця кібербезпеки в системі інформаційної безпеки, запропонуємо авторське розуміння її основних складових, а також її співвідношення з інформаційною безпекою держави.

На рис. 1 простежується загальна логічна схема підпорядкованості різного роду безпек, зокрема:

Рисунок 1 .Співвідношення інформаційної та кібернетичної безпеки

СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

кіберзлочинність

стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, у т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів

безпечна діяльність у кіберпросторі

ІНФОРМАЦІЙНА БЕЗПЕКА

захищеність життєво важливих інтересів держави

КІБЕРНЕТИЧНА БЕЗПЕКА

захищеність життєво важливих інтересів суспільства

захищеність життєво важливих інтересів людини та громадянина

безпека додатків (Application Security)

безпека мереж (Network Security)

Інтернет-безпека (Internet Security)

захист критичної інформаційної інфраструктури (національної свідомості) та критично важливих об'єктів інфраструктури

основні об'єкти руйнівної дії кіберзагроз

- життєво важливі національні інтреси України у кіберпросторі
- стан кібербезпеки держави
- кіберзахист об'єктів держави
- інтелект людини та масова свідомість

– кібербезпека (Cybersecurite). Визначається нами як складова інформаційної безпеки (Information Security);

– кібербезпека знаходиться в реляційних відносинах із безпекою мереж (Network Security), безпекою Інтернету (Internet Security) і безпекою додатків (Application Security), а також здійснює підтримку безпеки інфраструктури критичної інформації в частині, що її стосується (Critical Information Infrastructure Protection);

– як не дивно, кіберзлочинність (Cybercrime) і безпечна поведінка в кіберпросторі (передусім все дітей та молоді в Інтернеті – Cybersafety) відображено окремо. Кіберзлочиність впливає на інформаційну безпеку та, відповідно, кібернетичну безпеку. Безпечна діяльність у кіберпросторі, будучи певним орієнтиром ідеальної поведінки, знаходиться окремо.

У поняття «кібербезпека» входить широкий спектр практичних прийомів, інструментів і концепцій, тісно пов’язаних із технологіями інформаційної та операційної безпеки. Відмітна риса кібербезпеки полягає в тому, що вона включає в себе використання інформаційних технологій у наступальних цілях для атак противника. По суті, кібербезпека повинна включати не тільки заходи оборони та контрзахисту, а й наступу. Що стосується сучасного стану кібербезпеки України – пріоритетним її напрямом мають стати заходи активної оборони.

Термін «cybersecurity» слід використовувати для позначення практичних методів забезпечення безпеки, що поєднують у собі заходи наступального й оборонного характеру, які включають в себе сукупність або системи інформаційних та (або) операційних технологій або які ґрунтуються на них. Це всього лише одне визначення й одна рекомендація, але, зрозуміло, вони не єдині, на які спираються фахівці. Спостерігається, що деякі спеціалісти починають використовувати цей термін, або не надаючи технології для атак противника, або надаючи технології, які непридатні для таких атак.

У більшості підходів до тлумачення категорії «кібербезпека» немає такого елемента, як «наступальний характер». Проте такий підхід може мати

виняткового формальний характер, пов’язаний із необхідністю не розголошувати секретну інформацію.

Т. Ткачук відмічає, що *«кібернетичний*, або *спеціальний програмно-математичний вплив* реалізується з використанням засобів знищення, перекручення або розкрадання інформаційних масивів. Після подолання систем захисту противника з його інформаційних масивів отримується інформація, володіння якою вважається необхідним; доступ до них для законних користувачів при цьому обмежується чи взагалі унеможливлюється. У рамках кібервпливу вдаються також до дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп’ютерних систем тощо» [2, с. 132-133].

У Європейській Конвенції з кібернетичних злочинів наведено таке визначення цього поняття: «*кіберзлочини – це правопорушення, спрямовані проти конфіденційності, цілісності та доступності комп’ютерних систем, мереж і даних, а також їх неправомірне використання»* [45]. Віртуальний характер кіберзлочинів, а також засоби, за допомогою яких вони здійснюються, дають змогу зловмисникам швидко знищити сліди. Це значно ускладнює з’ясування обставин і пошук винуватців, тож постає нагальна потреба в розробленні нових методів розслідування кіберзлочинів і відповідних законодавчих норм, що регламентують сферу інформаційної безпеки.

«Інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття, - зазначається в Окінавській Хартії глобального інформаційного суспільства. Їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки» [46]. Відповідно міжнародне законодавство останнім часом почало приділяти значну увагу кіберзагрозам та протидії їм.

Серед основних загроз національним кіберпросторам стратегії більшості

країн визначають:

– *«кібершпигунство та воєнні дії, які здійснюються за підтримки або з відома держави*. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигунства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією» [41]. Так, однією з найрезонансніших кібератак за останній час стали дії КНДР проти компанії «Sony Pictures Entertainment», внаслідок яких зловмисники заволоділи конфіденційними даними, зокрема й інформацією про комерційні операції компанії [47];

– *«використання Інтернету у терористичних цілях»*. Терористичні угрупування використовують Інтернет із метою пропаганди, збирання коштів і вербування прихильників [41];

– *«кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом»*. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе ПЗ.

Відповідно, національні законодавства країн, як правило, регулюють питання:

– захисту персональних даних (Естонія, Іспанія, Канада, Швеція, Нідерланди, Фінляндія);

– захисту електронної комерції та безпеки електронних транзакцій та платіжних інструментів (Естонія, Італія, Канада, Польща, США);

– захисту дітей (США);

– захисту важливих об'єктів інфраструктури та інформаційних систем (Франція) [48, с. 244].

По-різному й трактують поняття «кібербезпека» в зарубіжних країнах:

– сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору (*Політика захисту кіберпростору Республіки Польщі*);

– бажаний стан безпеки інформаційних технологій, за якого ризики для

кіберпростору скорочені до прийнятного мінімуму (*Стратегія кібербезпеки Німеччини*);

– заходи з попередження шкоди від збоїв у роботі ІКТ та її усунення (*Національна стратегія кібербезпеки Королівства Нідерландів*);

– бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (*Стратегія безпеки та оборони інформаційних систем Франції*) [50, с. 143].

Щодо вітчизняного правового регулювання окреслених питань, то на законодавчому рівні проблему системи інформаційної безпеки досі комплексно не вирішено. Навіть Доктрина інформаційної безпеки України [51], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже - вже треба було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Відтак, як зазначають провідні вітчизняні науковці «сьогодні вкотре слід порушувати питання щодо розробки нормативного акта (закону), яким визначатиметься єдиний понятєво-категорійний апарат, державна політика забезпечення інформаційної безпеки, об’єкти інформаційної безпеки та суб’єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур з іншими органами та відомствами, віднесеними законодавством до суб’єктів забезпечення національної безпеки України, тощо» [52, с. 37].

«Усе це зайвий раз доводить нагальну потребу розробки та прийняття Закону України «Про інформаційну безпеку України» як базового

нормативно-правового акта, що регулюватиме відповідні питання» [53, с. 89]. «Такий закон як фундамент для побудови ефективної стратегії інформаційної безпеки має містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи її забезпечення, механізм її функціонування, повноваження і схему взаємодії суб'єктів забезпечення інформаційної безпеки тощо» [54, с. 21].

Це зумовлюється і досить динамічним розвитком інформаційного суспільства. У цьому ракурсі ми поділяємо думку В. Брижка, що в наш час життєдіяльність світової цивілізації все більше спрямовується інформаційною сферою, яка завдяки інформаційно-технологічним змінам, що почалися наприкінці XX століття, об'єктивно зумовила появу нового типу суспільства – інформаційного суспільства [55, с. 20]. Досить цікавою в ракурсі цього дослідження є думка В. Фурашева про те, що інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об'єктів і процесів, спрямованих на задоволення інформаційних потреб усіх живих істот на Землі [56, с. 45].

Підсумовуючи, зазначимо, що проведена диференціація інформаційної та кібернетичної безпеки не є чисто умоглядною. Її необхідність, на концептуальному рівні, зумовлена переходом людства на стадію інформаційного суспільства – нової соціально-економічної формації. І якщо донедавна питаннями забезпечення кібербезпеки переймалися й опікувалися здебільшого військові в межах інформаційного та радіоелектронного протиборства, то нині подібні проблеми стосуються і держави загалом, і суспільства, і кожної окремої особи.

Причин такого стану справ чимало. Основними з них убачаються такі:

– вторгнення інформаційних технологій в усі сфери життєдіяльності, розбудова на їхній базі державних, військових та інших управлінських систем;

– розвиток державних програм, спрямованих на формування інформаційного суспільства (електронне урядування тощо);

– недосконалість міжнародної та національної правових засад відповідальності за правопорушення в інформаційній сфері;

– брак міжнародно-правової заборони застосування інформаційної зброї, проведення інформаційних операцій та війн;

– недостатня участь міжнародних інститутів у сфері забезпечення інформаційної безпеки світової спільноти;

– стрімкий розвиток інформаційних технологій військового призначення, зокрема засобів ураження не лише військових, а й цивільних управлінських систем;

– створення та застосування спеціальних сил і засобів ураження критично важливої інформаційної інфраструктури, зокрема й шкідливого програмного забезпечення, яке уражає автоматизовані системи управління промисловими, енергетичними, транспортними й іншими об’єктами критично важливої інфраструктури країни;

– створення деякими державами доктрин ведення агресивних і підривних дій в інформаційному просторі й утілення цих стратегій проти окремих країн чи інших об’єктів;

– виникнення таких форм протесту громадян проти державної політики чи дій (бездіяльності) владних органів, які супроводжуються посяганнями на інформаційну інфраструктуру, тощо.

Вважаємо за доцільне детальніше розглянути деякі із наведених чинників з урахуванням потреби виокремити із сукупності безпекових різновидів безпеку кібернетичну. Так, одним із новітніх викликів в інформаційній сфері є виникнення одноособових і групових хакерських утворень, котрі, керуючись власними принципами та правилами, виступають у соціальних мережах Інтернету і традиційних ЗМІ із критикою соціально-політичних негараздів і пов’язаних із цим державних чиновників, олігархів, закликають до протестів тощо. На відміну від хакерів «звичайних», «хактивісти» [57] оголошують себе борцями за справедливість, не приховуючи своєї діяльності. Це свідчить про те, що певна частина хакерської спільноти,

виявивши небайдужість до соціально-економічних процесів у країні, прагне вплинути на них за допомогою своїх специфічних засобів, намагаючись провести кібератаки на інформаційні ресурси урядових, військових, бізнесових та інших структур, зорганізувати масові протестні акції. Діяльність таких утворень, їхня часто нігілістична ідеологія, безапеляційно негативне ставлення до всіх державних органів і службовців убачається серйозною загрозою для державного управління, зокрема й для керування збройними силами та їхньої інфраструктури. Останніми роками чимало фахівців з інформаційної безпеки вважають хактивізм чи не провідною негативною тенденцією. Повною мірою це стосується й України з огляду на транскордонний характер цього явища.

Оскільки хактевісти створюють і вдосконалюють шкідливе програмне забезпечення, котре розробляється задля ураження автоматизованих систем управління, потрібні нові підходи до забезпечення безпеки об’єктів критичної інфраструктури, зокрема й військово-промислового комплексу, приділяючи серйозну увагу безпеці систем управління, запобіганню реалізації можливих загроз, виявленню й усуненню «слабких» щодо можливих атак місць.

Ключовим поняттям у термінологічному словосполученні «інформаційна безпека даних» є «інформаційна безпека». Це – стан захищеності особи й інших суб’єктів (установ, організацій, спільнот, держави й ін.) та їхніх законних інтересів від будь-яких негативних загроз і впливів в інформаційному просторі. Складові інформаційної безпеки відповідають головним властивостям інформації – конфіденційність (доступ до інформації відповідно до визначених на це прав), цілісність (гарантування від несанкціонованих змін), доступність (відкритість для будь-яких суб’єктів відповідно з наданим доступом).

Відмінність інформаційної безпеки від кібернетичної, таким чином, полягає в тому, що перша спрямована на комплексний захист інформаційних ресурсів у будь-якій із можливих форм їх існування, тоді як кібербезпека опікується захистом виняткова цифрових форм даних.

Важливим чинником, який зумовлює потребу категоріального виокремлення кібербезпеки, є також розроблення деякими державами доктрин ведення спеціальних операцій в інформаційному просторі й утілення цих стратегій проти окремих країн чи інших об’єктів за допомогою спеціалізованих органів і структур. Сьогодні так звані центри кібернетичного захисту (чи з іншою назвою, але подібними функціями) функціонують у Австралії, Великій Британії, США, ФРН, Китаї, Ізраїлі, Ірані, РФ та інших країнах. Основні завдання цих структур (захист, спільно зі спецслужбами та правоохоронними органами, органів державного управління й об’єктів критичної інфраструктури), їхня підпорядкованість здебільшого військовим відомствам, та й навіть самі їхні назви свідчать, що головна їх мета в усіх країнах – забезпечення безпеки державного, зокрема військового, управління.

Слід зазначити, що останніми роками суттєво змінилося ставлення до місця та ролі інформаційного протиборства, яке нині вважається цілком самостійним і вельми ефективним інструментом боротьби з противником, а не допоміжним, супутнім бойовим діям засобом. І в цій своїй новій іпостасі інформаційне протиборство набуває значно ширшого змісту, далеко виходячи за межі традиційних воєнних дій. Воно здатне швидко вивести з ладу головні сили й засоби ворожої країни, не завдаючи при цьому невідновної фізичної шкоди її господарству, критичній інфраструктурі й території, за допомогою не заборонених міжнародно-правовими нормами потужних засобів, котрі, крім того, украй важко виявити й нелегко знешкодити.

Отже, подальший розвиток системи забезпечення безпеки інформаційної сфери України, вбачається надзвичайно важливим, особливо в умовах безпрецедентної інформаційної війни, що її розгорнула проти нашої країни Російська Федерація. Задля виконання цього життєво важливого завдання потрібні узгоджені спільні зусилля всіх без винятку державних інституцій, Збройних Сил, спеціальних служб, правоохоронних органів, наукових установ, громадських організацій, приватних структур, засобів масової інформації й окремих громадян.

Слід також акцентувати увагу на проблемі істотних розбіжностей між сучасними інформаційними відносинами та їхнім нормативно-правовим регулюванням, яке неналежним, на наш погляд, чином враховує рівень небезпечності нових негативних чинників у сфері інформаційної безпеки. Причому це стосується як вітчизняного законодавства, так і міжнародного права.

1.4 Методологічні засади забезпечення кібербезпеки України

Становлення й еволюція світового інформаційного суспільства, динаміка та характер розвитку глобального кіберпростору зумовили виникнення новітніх викликів і загроз, спрямованих насамперед на людину як найуразливішу ланку інформаційних відносин у кіберпросторі. Відтак актуалізувалася проблема формування й удосконалення системи міжнародної кібернетичної безпеки, під якою розуміємо такий стан глобального кібернетичного простору, який гарантує дотримання законних прав людини, а також суспільства й держави під час його використання.

Тому нагальність теоретико-правового дослідження загроз кібербезпеці України в контексті правового забезпечення її інформаційної безпеки та розвитку засадничих положень цієї складової інформаційного права не викликає сумнівів.

Вже сьогодні ми маємо всі симптоми й індикатори загроз, так як нам доведеться мати справу з новою біозброєю, зламаною ДНК і крадіжками генетичної та біометричної інформації. Ми живемо в експоненційні часи, коли інформація подвоюється кожні два роки, коли ми є технологічно незахищеними, так як усіма критичними системами та інфраструктурами керують комп’ютери. Цікавою є думка керівника відділу інновацій NASA Омара Хатамле про експоненційний розвиток технологій. Він зазначає, що

дивлячись на обчислювальну потужність, яка буде доступна десь до 2030 року, то до того часу вона буде еквівалентна одному людському мозку [58]. І справа не тільки в ІТ-проблемах, які пронизують усе життя сучасної людини, яка також стикається із соціальними, особистими, фінансовими проблемами, проблемами охорони здоров'я, виробництва та суспільної безпеки, транспорту й енергетики, конфіденційності і прав людини [59, с. 125].

Інформаційна сфера, зокрема й кібернетична безпека, стали визначальним чинником життєдіяльності сучасної світової спільноти та фактично кожної окремої особистості. Це зумовило, крім звичних розробок технічних аспектів проблематики, сплеск філософських, соціологічних, культурологічних, політологічних, економічних, психологічних та інших гуманітарних досліджень. Убачається, що в умовах транскордонного глобалізованого інформаційного суспільства наука інформаційного права мусить звернути особливу увагу на формування уявлень про специфіку та значення реалізації інтересів людини, суспільства, держави у цій сфері.

Наразі дискусійним є твердження Фурашева В. М., Петряєва С. Ю., Поперечнюка В. М., що наявність та циклювання інформації, як об'єктивної субстанції, не залежить від волі людини, живої істоти, штучної системи, адже інформація є цілком незалежним та самостійним утворенням. Звісно, людина може певним чином впливати на обіг інформації, її структуру, види тощо. Особливо це стосується тієї інформації, що циркулює у суспільстві, та тієї, що була створена людиною (спільністю людей) [60, с. 11]. Такий підхід може бути предметом уваги філософії чи, в окремих випадках, метафізики права. Зауважимо, що такий підхід зрештою можливий, але в суспільстві, де висока інформаційна культура та розвинені принципи інформаційної гігієни. В українському суспільстві нашого часу контроль та глибоке усвідомлення інформаційних процесів повинні бути в основі створення інформації. Такий стан має передувати просвітницькій діяльності, навчанню критичного мислення та навичкам створення фільтрів при роботі з інформацією. Проте ми цілком погоджуємось із авторами, що інформацію слід розглядати як рівну

величину термінам «енергія» і «матерія» [60, с. 13].

Отже, актуальність наукової розробки питань протидії деструктивним інформаційно-психологічним впливам у кіберпросторі визначається насамперед потребою забезпечення кібернетичної безпеки. У цій праці автор має на меті, в межах розбудови науки інформаційного права здійснити спробу комплексного наукового дослідження вказаної проблематики.

Убачається доцільним, розпочинаючи аналіз змісту поняття «кібернетична безпека», розглянути підходи до його визначення представників різних наукових галузей – правничої, філософії, соціології, політології, психології, технічних та інших наук. Беручи до уваги безліч поглядів на питання, спробуємо виокремити найхарактерніші позиції з огляду предмета нашого наукового дослідження.

Загальнофілософський підхід визначає кібернетичну безпеку як єдність трьох складників: задоволення інформаційних потреб особи; забезпечення безпеки інформації; забезпечення захисту суб'єктів інформаційних відносин. Відповідно до цього підходу, кібербезпекою є такий стан інформаційного середовища, який дає змогу об'єктові, котрий у ньому перебуває, зберігати здатність і мати змогу приймати й утілювати рішення відповідно до спрямованої на прогресивний розвиток мети.

Як бачимо, у цьому разі кібернетична безпека може забезпечуватися комплексом технічних, організаційних та правових заходів, спрямованих як на забезпечення стану кіберсередовища, безпечного для об'єкта, його захисту від шкідливих впливів, так і на розвиток здатності об'єкта уникати таких впливів, зокрема й завдяки знанням про їхню наявність, вироблення своєрідного інформаційного імунітету. Отже, задля забезпечення кібербезпеки держава має створити такі умови функціонування інформаційної інфраструктури та суб'єктів інформаційних відносин, насамперед – людини, за яких кожна окрема особа, групи людей, владні інститути можуть приймати й утілювати обґрунтовані, спрямовані на прогрес усього суспільства управлінські рішення.

З погляду соціально-політичних реалій пошук засобів протидії

численним викликам і загрозам у сфері кібернетичної безпеки потребує передусім об'єднаних зусиль бізнесових структур, політичних інституцій, правоохоронних та інших органів влади, галузевих аналітичних та експертних спільнот. Кібернетична безпекова політика має відповідати актуальним викликам, тобто спиратися на пріоритети розвитку громадянського суспільства, взаємовигідної співпраці. При цьому, звісно, держава має стати ефективним менеджером і координатором указаних процесів. Убачається, що для вироблення й утілення в життя науково обґрунтованої, системної безпекової політики в інформаційній сфері в теперішній час наявні всі передумови.

Багатоаспектним є *технічний* підхід до проблематики кібернетичної безпеки, значною мірою навіть базовий. Це, зокрема, забезпечення безпеки сайтів, а саме: атестація, ліцензування й сертифікація об'єктів інформатизації; захист серверів; застосування криптографічних методик і засобів захисту даних у мережах; ідентифікація й аутентифікація користувачів тощо.

Соціологічний підхід щодо кібернетичної безпеки спостерігаємо в розвитку соціології інформатики – одного із сучасних напрямів науки про суспільство.

Аксіологічний підхід – є філософським вченням про природу цінностей, їхню роль у реальному житті та про структуру ціннісного світу, тобто про взаємозалежність різних цінностей, їхні зв'язки із соціальними, культурними чинниками та структурою людської особистості. Базовою категорією аксіології є цінність – особистісне, соціальне й культурне значення певних явищ дійсності. Головне завдання аксіології, її основна ідея – визначення місця цінності в загальній тканині буття, її співвідношення з явищами дійсності, виявлення ролі, яку відіграють певні цінності в людському житті.

При цьому об'єктивність наукового знання й ціннісні судження не повинні суперечити одне одному, оскільки пізнання людини й соціуму неможливе без урахування суб'єктної й суб'єктивної природи людських взаємин, особистісних і суспільних цінностей, пріоритетів та ідеалів, намірів і

прагнень.

Для вироблення нової ціннісної моделі при формуванні інформаційної картини світу потрібна трансформація уявлень про сутність нинішнього інформаційного етапу розвитку людства та роль особистості в цей період. І усвідомлена ця картина світу має бути не лише об'єктивно, виходячи із характеристик і властивостей новітніх інформаційних технологій, а й з позицій їхньої особистісної та суспільної цінності, тобто відповідності вказаних технологій соціальній природі людини, їхньої корисності чи шкідливості, безпечності, здатності задовольняти інтереси людини.

Людська спільнота на сучасному – інформаційному етапі свого розвитку – це складне багаторівневе соціальне утворення, система, складена з багатьох компонентів, задіяних в інформаційних комунікаціях. Не забуваючи про техніко-логічні характеристики вказаних комунікацій, зазначимо, що під час аналізу інформаційної взаємодії та інформаційного обміну слід неодмінно зважати, що це – взаємини людини й соціальних елементів системи (суспільних структур), котрі виражають інтереси окремих осіб, груп людей, а також великих спільнот. Головним, що вирізняє зазначене високоорганізоване соціальне утворення в інформаційну епоху, є його цілковите підпорядкування засадам результативної інформаційної комунікації.

Провідна ідея, покладена в основу аксіологічного підходу до вивчення інформаційної картини світу, вбачається цілком очевидною. Проте, на нашу думку, її складники потребують наукового осягнення. Саме це і стане наповненням схеми міждисциплінарного аналізу як методологічної бази цього дослідження проблематики інформаційної безпеки людини.

Однією із таких складових є усвідомлення цінності множинно-варіативного способу щодо шляхів розвитку інформаційного суспільства, а також оціночних суджень у множині системних підходів до обґрунтування такої точки зору.

Інформація, поняття якої наприкінці 1920-х років запровадив у науковий обіг американський дослідник Р. Хартлі як кількісний показник «відомостей,

що поширюються технічними каналами зв'язку» [61], є безумовною цінністю інформаційного світу. Проте, сакральний зміст поняття «інформація» не розкрито до цього часу. Відома та загальноприйнята теорія Клода Шеннона [62], з урахуванням сучасного технологічного прогресу та перенасичення інформацією, характеризується формальним, чи навіть абстрактним трактуванням інформаційних взаємозв'язків. Основу такого твердження складає гіпотеза про те, що в теорії К. Шеннона сама цінність інформації для споживача не береться до уваги. Підтвердженням цього є й те, що сам дослідник назвав свою теорію «математична теорія зв'язку», відповідно до якої повідомлення – певні кодові пересилання передавача, а не сам зміст повідомлення. Сьогодні людство активно впроваджує концепції «екології інформації» та «інформаційної гігієни». Цей етап інформаційного розвитку людства продукує розвиток фази змістовного аналізу інформації, а не просто відповідного набору кодових значень. З упевненістю можна констатувати, що людство перейшло в епоху, основною характеристикою якої є цінність інформації, яка енергетично збагачує та дає можливість реалізувати мету. Все інше буде на кшталт інформаційного шуму та марних (пустих) даних.

У теперішній час термін «інформація» і в науці, й у широкому вжитку може набувати найрізноманітніших значень. За влучним висловом Т. Стоуньєра, інформаційне суспільство все ще не дійшло єдиної думки про те, що таке інформація [63]. Утім, не викликає сумнівів міждисциплінарний характер цього поняття, яке застосовується практично в усіх галузях сучасних природничих і соціальних, технічних і гуманітарних, теоретичних і прикладних наук.

З-поміж множини підходів до розуміння інформації в контексті її цінності для інформаційного суспільства можна виокремити три провідних. Це, по-перше, так званий антропно-комунікативний підхід, тобто тлумачення інформації у сфері спілкування як засобу загальнонаукового усвідомлення міжлюдських соціальних зв'язків і відносин. Другий, функціональний, підхід визначає інформацію як пов'язану з упорядкуванням взаємодій властивість

самоорганізуючих систем. Нарешті, атрибутивний підхід розглядає інформацію як показник такої властивості всіх матеріальних систем, як гетерогенність розподілу матерії та енергії.

Як бачимо, за таких підходів до тлумачення інформації вже із самого її поняття випливає можливість порушень інформаційної (кібернетичної) безпеки, тобто інформаційних ризиків. Інформація, яка охоплює всі сфери життєдіяльності суспільства, створює умови інформаційної нерівності, коли розподіляється відповідно до соціально-статусних, ресурсних та матеріальних чинників. А така нерівність значною мірою зумовлює виникнення інформаційних ризиків, порушення інформаційної безпеки. Це, зокрема, стосується негативних впливів окремих інформаційних ресурсів маніпулятивного характеру, вторгнення в особистісний інформаційний простір, кібернетичної злочинності й інших порушень інформаційних прав людини.

Отже, *кібернетична безпека людини, суспільства й держави в усіх її аспектах є найважливішою світовою цінністю інформаційної епохи*.

Наведені вище міркування стосовно інформаційної картини світу, застосування міждисциплінарної методології як підґрунтя вивчення проблем кібернетичної безпеки втрачає сенс без з'ясування «локації» людини в цьому «живописі». Осягнення місця особи у глобальному інформаційному просторі сучасного суспільства пов'язане зі з'ясуванням сутності здатної до критичного мислення людини інформаційної епохи, яка включена у глобальні інформаційні комунікації, у філософському та соціальному сенсі.

Важливість такого осягнення важко переоцінити, позаяк це дає змогу виявити нові системні відносини, котрі виникають в інформаційну епоху у двоєдності людина – суспільство, відповідні нові властивості як людини, так і соціуму.

Що ж стосується *правових* аспектів кібернетичної безпеки, то на сьогодні мусимо констатувати відсутність у юриспруденції єдиного підходу до визначення цього поняття. Детальніше це питання буде розглянуто в

наступних параграфах дослідження.

Специфіка предмета – кібернетичної безпеки – у межах науки інформаційного права висуває перед дослідниками низку гносеологічних завдань стосовно методів і прийомів пізнання, оптимальних способів систематизації набутих знань, засадничих принципів правового забезпечення в цій галузі, її понятійно-категоріального апарату, закономірностей розвитку тощо. Вважаємо, що в умовах глобального інформаційного суспільства ці та інші методологічні проблеми у сфері правового забезпечення інформаційної безпеки потребують першочергового розв'язання.

Отже, вихідним предметом цього дослідження визначено правове забезпечення кібернетичної безпеки особи в умовах глобального інформаційного суспільства. Специфіка цього предмета, яка, природно, впливає на характер, перебіг і результати дослідження, полягає передусім у значущості суб'єкта інформаційних відносин – особистості, її місця та ролі в розвитку цих відносин. Розкрити умови генезису особи в глобальному інформаційному суспільстві, її унікальність, – ці та інші завдання зумовили особистісно орієнтований та аксіологічний підходи цього дослідження, в межах якого «особа» і «глобальне інформаційне суспільство» є провідними елементами, котрі визначають важливість проблематики правового забезпечення кібернетичної безпеки особи, а також такі соціально-правові категорії як інформаційна гігієна, екологія інформації тощо.

У цьому дослідженні провідною гіпотезою є залежність, взаємна зумовленість, кореляція, ефективність розвитку суспільства в умовах інформатизації й глобалізації та рівня забезпечення кібернетичної безпеки головного споживача всіх набутків сучасних інформаційно-телекомунікаційних технологій – людини, особистості. Факторний аналіз, який є основним методом цього дослідження, базується на вивченні чинників, що у глобальному інформаційному суспільстві впливають на результативність реалізації особою своїх інтересів, становлять для неї небезпеку. Тому, метою цього дослідження є визначення корелятів потенцій особи в глобалізованому

інформаційному суспільстві та пов’язаних з багатоманітністю видів і форм загроз інформаційній безпеці стримувальних чинників.

Указаною вище основною гіпотезою зумовлені також ті методи, інструменти й прийоми – філософські, загальнонаукові та спеціальні, які застосовуються під час цього дослідження. Скажімо, на загальнофілософському методі, котрий дає змогу визначити закономірності розвитку сучасного інформаційного суспільства, ґрунтується ідея діалектичного розвитку останнього. З-поміж загальнонаукових і спеціальних методів наукового пошуку основними є формально-логічний, системного аналізу, соціологічний, порівняльно-правовий, історичний, прогностичний та ін.

Так, із метою узагальнення висновків проведеного дослідження за допомогою аналізу інформаційного законодавства, його систематизації, з’ясування змісту основних понять застосовується інструментарій формально-логічного, або юридичного методу. Дослідженню правового забезпечення кібернетичної безпеки України за допомогою виявлення тенденцій, порівняльного аналізу підходів до вказаної проблематики в законодавствах іноземних країн та в міжнародно-правових документах сприяє застосування порівняльно-правового методу. Завдяки використанню історичної (історично-правової) методики досягається мета здобуття й узагальнення даних щодо сутності й закономірностей розвитку інформаційного права, його інститутів у контексті інформаційно-безпекової проблематики. За допомогою засобів системного аналізу здійснюється, зокрема, оцінювання підходів до забезпечення інформаційної безпеки особи, які усталилися у вітчизняній юриспруденції, їх кореляція з актуальними суспільними відносинами. Водночас виявити й оцінити чинники, котрі впливають на правову поведінку особи, дає змогу соціологічний метод. А прогностичний метод дає можливість за допомогою моделювання окреслити перспективи, передбачити ймовірні шляхи розвитку галузевого законодавства у сфері інформаційної безпеки особи, її правового забезпечення.

До методологічної бази дослідження належать також принципи, покладені в основу забезпечення кібернетичної безпеки в умовах глобалізованого інформаційного суспільства. У межах досліджуваної проблематики ці принципи отримують свій логічний розвиток на підставі вивчення змісту засадничих принципів галузевого законодавства.

Статут ООН наголошує на безумовній цінності прав людини та її особистості: «Ми, народи об'єднаних націй, сповнені рішучості відновити ствердження віри в основні права людини, у гідність і цінність людської особистості…» (преамбула). А сприяння «…загальній повазі й дотриманню прав людини й основних свобод для усіх, без розрізнення раси, статі, мови й релігії…» (ст. 55) цей установчий документ ООН визначив головні завдання забезпечення безпеки людини, у тому числі й кібернетичної.

Низку засадничих положень містить також ухвалена Генасамблеєю ООН у 1948 році Загальна декларація прав людини. Цей важливий міжнародно-правовий акт проголошує насамперед про право кожної людини на життя, свободу й особисту недоторканність; на недоторканність житла, таємницю листування; неприпустимість безпідставного втручання в її особисте й сімейне життя, посягань на її честь і репутацію; на свободу думки, совісті, переконань, інформації; на можливість вільного пошуку й отримання інформації, а також її поширення незалежно від державних кордонів і в будь-який спосіб (ст. 3, 12, 19).

Римська Конвенція про захист прав людини і основних свобод (1950) також містить положення, які стосуються правового забезпечення інформаційної безпеки особи. Зокрема Конвенція закріплює право кожного на свободу й особисту недоторканність (ст. 5), на повагу до приватного й сімейного життя людини, недоторканність її житла й особистої кореспонденції (ст. 8). Крім того, у зв'язку з реалізацією цього права забороняється втручання органів чи представників публічної влади, «окрім випадків, коли таке втручання передбачене законом і потрібне в демократичному суспільстві в інтересах національної безпеки та громадського порядку, економічного

добробуту країни, з метою запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі або захисту прав і свобод інших осіб».

Конвенція також проголошує право людини вільно висловлювати свою думку, передбачаючи при цьому аналогічні попереднім обмеження й формальності, пов'язані, приміром, із відверненням злочинів, охороною життя і здоров'я, завданням шкоди іншим людям, захистом їх прав і репутації, забезпеченням авторитету й неупередженості судочинства, запобіганням оприлюдненню конфіденційної інформації та ін. (ст. 10).

Основоположні принципи, задекларовані наведеними вище документами, були розвинуті й деталізовані в інших міжнародно-правових актах. Це, зокрема, ухвалені у грудні 1966 року міжнародні пакти «Про громадянські й політичні права» та «Про економічні, соціальні й культурні права», які прийняті з метою «здійснення ідеалів свободи людської особистості, вільної від страху і злиднів» і наголошують на важливості такого атрибуту людської особистості, як гідність.

Оскільки інформаційне законодавство проходить у теперішній час етапи свого становлення як самостійної галузі національного права, воно ще не має, на наш погляд, потужної методологічної бази, достатньо розроблених засад інформаційно-правової теорії. Наявні сьогодні в цій сфері нормативні акти не утворюють повноцінну систему інформаційного законодавства, яка б адекватно регулювала правові відносини в інформаційній сфері.

Що стосується методології, то одним із найважливіших питань убачається проблема сутності правових норм, яка визначається відповідними правовими принципами, тобто тими втіленими у праві вихідними, «первісними» нормативно-керівними засадами, які зумовлюють його формування, його підґрунтя, закономірності суспільного життя, відображені в ньому. На жаль, та система принципів, яка простежується в чинному вітчизняному інформаційному законодавстві, свідчить про відсутність цілісного, дієвого механізму правового регулювання суспільних відносин в інформаційній сфері.

Значення загальновизнаних міжнародно-правових принципів беззаперечне, як і актуальність питання про основоположні, фундаментальні принципи правового забезпечення кібернетичної безпеки. Водночас слід відзначити першорядність питання про спосіб формування загальних правових уявлень, які зумовлюють зміст правового регулювання не лише кібернетичної безпеки, а й усіх соціальних відносин, а також механізми розроблення конкретних правочинів, котрі стають регуляторами у глобальному, загальнолюдському масштабі. Відтак, варто приділити пильну увагу питанню детальної регламентації принципів як фундаментальних ідей, передумов, сукупність котрих визначає оптимальний спосіб, ідеальну модель регулювання певної сфери суспільних відносин.

Так, для втілення в життя принципу недоторканності особистісної приватності, неприпустимості без згоди людини збирати, зберігати й поширювати інформацію про її особисте життя необхідним, зокрема, убачається законодавче впровадження постійного моніторингу стану захищеності особи від внутрішніх і зовнішніх загроз в інформаційній сфері, зокрема й у кібернетичному просторі.

Для вироблення у вітчизняному праві тих принципів, які сформують міцний фундамент регулювання суспільних відносин в умовах їх інформатизації та глобалізації, має посприяти доволі солідний іноземний досвід. Так, вихідними принципами у Стратегії ідентифікації США (National Strategy for Trusted Identities in Cyberspace) [64] є: добровільність будь-якої зацікавленої особи щодо використання її персональних (облікових) даних для отримання «ідентифікаційної посвідки»; посилення безпекових заходів щодо персональних (облікових) даних із метою захисту інформації користувачів мережі Інтернет; сумісність персональних (облікових) даних, котрі використовуються для ідентифікації; економічна продуктивність, простота користування, а також доступність для постачальників і користувачів інтернет-ресурсів. Крім зазначених, Стратегія передбачає запровадження так званих Fair Information Practice Principles (FIPP) – низки спеціальних

принципів доброчесного використання інформації.

Проведене вивчення базисних положень, себто принципів регулювання суспільних відносин в інформаційній сфері, у галузі комп'ютерних технологій, захисту інформації та кібербезпеки, а також генеральної мети й головних напрямів правового забезпечення захисту інформації й кібернетичної безпеки, котрі втілені в чинних і проєктних документах стратегічного планування, дає змогу дійти певних проміжних висновків.

Насамперед, як уявляється, зазначені принципи правового забезпечення кібернетичної безпеки особи належить закріпити як базисні під час визначення національних інтересів і стратегічних пріоритетів у Стратегії національної безпеки України, Доктрині інформаційної безпеки та інших документах стратегічного планування, а не лише в законодавстві. На нашу думку, при виробленні державної політики у сфері забезпечення кібернетичної безпеки провідними принципами мають стати такі:

– визнання людини головним суб'єктом і найуразливішим учасником інформаційних відносин;

– відповідальності держави у сфері інформаційних відносин;

– відповідності організаційно-правових заходів, що вживаються державою, реальним та потенційним викликам і загрозам;

– державного контролю за забезпеченням інформаційної (кібернетичної) безпеки особи, а також шляхом застосування суспільних інструментів захисту інформаційних прав і свобод.

Про безперечний міжгалузевий характер інституту забезпечення кібернетичної безпеки особи переконливо засвідчить аналіз його специфічних рис. Це стосується передусім різноманітності матеріальних, духовних, соціальних, політичних, культурних та інших інтересів особистості. І одним із найважливіших людських запитів є рівноправ'я в інформаційній сфері, безпосередні комунікації з органами державної влади й місцевого самоврядування у процесі, скажімо, надання останніми послуг за допомогою комп'ютерних мереж, розвитку електронного документообігу, механізмів та

інструментів електронної демократії. Це також втілення права особи на захист шляхом формування системи електронного судочинства, отримання нею різних переваг завдяки правовому забезпеченню безпеки в інформаційній сфері, вдосконаленню фінансово-кредитної інфраструктури у глобальному кібернетичному просторі тощо.

Крім того, про міжгалузевий характер розглядуваного інституту свідчить регулювання ним цілого комплексу правовідносин, механізм реалізації яких заснований на нормах інформаційного, конституційного, цивільного, адміністративного, кримінального, процесуального, трудового, фінансового, банківського, податкового й інших галузей права.

Отже, у цьому дослідженні забезпечення кібернетичної безпеки розглядається як самостійний комплексний міжгалузевий інститут інформаційного права. Про комплексність зазначеного інституту свідчать, зокрема, такі його властивості:

1) правовий інститут забезпечення кібернетичної безпеки сформований і розвивається на базі матеріальних і процесуальних норм інформаційного, конституційного, цивільного, адміністративного, кримінального, процесуального (цивільного процесуального, кримінального процесуального та ін.), трудового, фінансового, банківського, податкового та інших галузей права, хоча й суміжних, але не однорідних. Загалом же формування в системі інформаційного права як галузі вітчизняного права міжгалузевих правових інститутів зумовлене його міжгалузевим характером;

2) правове забезпечення кібернетичної безпеки в системі галузі інформаційного права можна розглядати як самостійне, базове правове утворення, позаяк воно сьогодні надзвичайно актуальне й широко представлене в нормах чинного законодавства;

3) правове забезпечення кібернетичної безпеки як самостійний інститут формується на основі порівняно нечисленної сукупності юридичних норм, котрі регулюють специфічне коло суспільних відносин стосовно забезпечення безпекових інтересів людини, суспільства, держави в інформаційній сфері;

4) інститут правового забезпечення кібернетичної безпеки як складова підгалузі правового забезпечення інформаційної безпеки в системі інформаційного права взаємопов'язаний з іншими інститутами цієї підгалузі – захисту комерційних та державних секретів, охорони державної таємниці, захисту персональних даних та іншими;

5) основу змісту інституту правового забезпечення кібернетичної безпеки становлять норми зазначених вище неоднорідних правових галузей, які об'єднані спрямованістю на забезпечення безпекових інтересів людини, суспільства, держави в кіберпросторі.

Комплексна, міжгалузева природа розглядуваного вище правового феномена базується на певній сукупності пов'язаних між собою різногалузевих норм, пріоритет з-поміж яких належить нормам інформаційного права як сполучній ланці й системоутворювальній складовій.

Отже, задля розвитку й удосконалення галузі інформаційного права вбачається абсолютно доцільним визнати інститут правового забезпечення кібернетичної безпеки самостійним.

Висновки до розділу 1

Серед пріоритетних напрямів наукових досліджень, які розглядалися в цьому розділі, були: дослідження генезису правового забезпечення кібербезпеки людини, суспільства, держави, проведення понятійно-категоріального синтезу правового забезпечення кібербезпеки України; вивчення теоретико-правових основ визначення об'єкта правового забезпечення кібербезпеки України; виявлення основних констант співвідношення кібербезпеки та інформаційної безпеки. За результатами проведеного дослідження можемо зробити такі висновки:

1. У процесі вивчення та аналізу основних теоретичних підходів до

правового забезпечення кібербезпеки людини, суспільства, держави виокремлено рівень корпоративної та глобальної культури кібербезпеки. У першому випадку мова йде про це компетентність та корпоративні цінності, пов’язані із забезпеченням особистої та корпоративної безпеки в кіберпросторі у відповідності до визначеноїполітики кібербезпеки окремої особистості чи установи. Особиста кібербезпека співробітника установи є основним спрямуванням заходів формування корпоративної культури кібербезпеки, орієнтованим на засвоєння необхідних умінь та навичок захисту, що стосуються як технічних, так і психологічних аспектів, так званої соціальної інженерії і можливостей інформаційно-психологічного впливу.

Доведено, що формування глобальної культури кібербезпеки є дієвим механізмом запобігання кіберзлочинності, який спрямовано на попередження, виявлення й усунення причин та умов, які сприяють вчиненню кіберзлочинів. Мова йде про системні заходи забезпечення життєво важливих інтересів осіб у кіберпросторі з позицій захисту інформації та інформаційно-психологічного захисту. Глобальну культуру кібербезпеки визначено як шлях вирішення проблеми підвищення рівня кіберзахисту особи і суспільства з використанням соціальних заходів на міжнародному і національному рівнях.

2. Доведено, що кібернетична безпека є унікальним, універсальним явищем, продуктом світової цивілізації, розвиток якого потребує глибокого наукового осягнення, належного нормативно-правового врегулювання та створення відповідних структур, котрі мають забезпечувати національну безпеку України у глобальному кібернетичному просторі.

При цьому з’ясовано низку правових прогалин, зокрема, визначений законодавцем підхід до змісту кібербезпеки з предмета свого безпосереднього правового впливу упускає досить важливу складову, яка проявляється у результаті дії загроз кібербезпеці – це запобігання шкоді. Таке упущення, на нашу думку, не дає змоги повною мірою визначити мету правового регулювання.

3. Доведено, що на сучасні безпекові виклики і вітчизняне, іміжнародне

право питання кібербезпеки реагують явно недостатньо, що створює сприятливі умови для хакерських, екстремістських, терористичних суб'єктів для впливу на органи державної влади й досягнення інших злочинних цілей.

У цьому контексті варто зазначити недостатню реалізацію потенціалу правового захисту державного управління й систем керування об'єктами критично важливої інфраструктури. Ураховуючи їхню значущість, ці системи значно краще, ніж звичайні об'єкти, захищені фізично. Проте їх нормативно-правовий захист (особливо в сенсі юридичної відповідальності) практично не відрізняється.

4. Запропоновано, що предмет вивчення безпекової науки стосовно кіберсередовища включає: природні, соціально-економічні, соціально-політичні та техногенні процеси в контексті їхнього розвитку, взаємодії та утворення нових об'єктів і явищ, їхніх елементів із навколишнім середовищем задля виявлення існуючих та потенційних небезпек, оцінювання відповідних ризиків та розроблення адекватних методів і способів протидії, а також розроблення належної нормативної бази для належної правової регламентації вимог, методик, механізмів, алгоритмів, застосування яких гарантує досягнення мети захищеності інтересів людини, суспільства й держави від наявних та можливих загроз.

Науково доведено, що з метою кіберзахисту всіх суб'єктів – від окремої особи до суспільства й держави в цілому – слід сформувати комплексну систему (доктрину, політику) їхньої безпеки, підґрунтям якої має стати кібербезпека. Себто створення захисту інформаційних систем від негативних впливів належить розпочинати саме з кібербезпеки як основи захищеності відповідних даних.

5. Доведено, що кібербезпека є самостійним видом безпеки з тісними взаємозв'язками з національною та інформаційною безпекою. Кібербезпека виникла як складова інформаційної безпеки, а нині – це еволюція інформаційної безпеки, оскільки від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації.

Запропонована така логічна схема еволюції кібербезпеки як окремого виду безпеки: кібербезпека визначається як складова частина інформаційної безпеки; кібербезпека знаходиться в реляційних відносинах із безпекою мереж (Network Security), безпекою Інтернету (Internet Security) і безпекою додатків (Application Security), а також здійснює підтримку безпеки інфраструктури критичної інформації в частині, що її стосується (Critical Information Infrastructure Protection).

6. У дослідженні кібернетичної безпеки України основними методологічними підходами стали загально філософський, соціологічний, технічний, аксіологічний та правовий підходи. На основі даного методологічного інструментарію визначено, що провідною гіпотезою є залежність, взаємна зумовленість, кореляція ефективності розвитку людини, суспільства, держави в умовах інформатизації й глобалізації. Факторний аналіз, який є основним методом цього дослідження, базується на вивченні чинників, що у глобальному інформаційному суспільстві впливають на результативність реалізації особою своїх інтересів, становлять для неї небезпеку. Вихідним предметом цього дослідження визначено правове забезпечення кібернетичної безпеки в умовах глобального інформаційного суспільства.

7. У розділі наголошується, що з метою узагальнення висновків проведеного дослідження за результатами аналізу інформаційного законодавства, його систематизації, з’ясування змісту основних понять застосовується інструментарій формально-логічного, або юридичного методу. Дослідженню правового забезпечення кібернетичної безпеки України за допомогою виявлення тенденцій, порівняльного аналізу підходів до вказаної проблематики в законодавствах іноземних країн та в міжнародно-правових документах сприяє застосування порівняльно-правового методу. Завдяки використанню історичної (історично-правової) методики досягається мета здобуття й узагальнення даних щодо сутності й закономірностей розвитку інформаційного права, його інститутів у контексті інформаційно-безпекової

проблематики. За допомогою засобів системного аналізу здійснюється, зокрема, оцінювання підходів до забезпечення інформаційної безпеки особи, які усталилися у вітчизняній юриспруденції, їх кореляція з актуальними суспільними відносинами. Водночас виявити й оцінити чинники, котрі впливають на правову поведінку особи, дає змогу соціологічний метод. Прогностичний метод дає можливість за допомогою моделювання окреслити перспективи, передбачити ймовірні шляхи розвитку галузевого законодавства у сфері кібербезпеки України, її правового забезпечення.

Отже, у цьому дослідженні забезпечення кібернетичної безпеки розглядається як самостійний комплексний міжгалузевий інститут інформаційного права.

Основні результати дослідження, проведеного в цьому розділі викладено також у працях автора [65-71].

РОЗДІЛ ІІ

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

2.1 Стан правового регулювання кібербезпеки в Україні

Цивілізаційний розвиток у XXI столітті, заснований на розробці та впровадженні в практику передових наукових розробок, дав змогу значно прискорити життєво важливі процеси, що протікають у багатьох сферах суспільного життя. З впровадженням в ці процеси комп'ютерних технологій, новітніх засобів і способів доставки інформації людство фактично опинилося в новій реальності. Зокрема, одним із фундаментальних наслідків світової інформатизації стало виникнення і стрімкий розвиток та розширення в обсягах принципово нового середовища соціальної активності – кіберпростору. За своїми технічними характеристиками і призначенням кіберпростір є транснаціональною сферою інфраструктур інформаційних технологій і взаємозалежних мереж. Він включає в себе Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори в критичних галузях. Глобально взаємопов'язаний і взаємозалежний, кіберпростір лежить в основі сучасного суспільства і забезпечує важливу підтримку світової економіки, цивільної інфраструктури, громадського порядку та національної безпеки. Відповідно, особливої важливості у світі та в національних державах набувають питання кібербезпеки та її правового забезпечення.

Актуальність дослідження правових основ забезпечення кібербезпеки визначається і тим, що прагнення України до вступу в Європейський Союз і НАТО ставить завданням наближення нормативно-правового регулювання заходів безпеки до рівня вимог Європейського Союзу та стандартів НАТО [72,

с. 2002].

Згідно з визначенням Міжнародного союзу електрозв'язку кібербезпека становить набір засобів, стратегії і принципів забезпечення безпеки, гарантії безпеки, підходів до управління ризиками, дії і практичний досвід, страхування і технологій, які можуть бути використані для захисту кіберсередовища, ресурсів організації і користувача. Кібербезпека, як правильно зазначає, О. Баранов, включає заходи захисту і дії, що дозволяють здійснити захист кіберпростору як у цивільній, так і у військовій сфері від загроз, які пов'язані з його взаємозалежними мережами і інформаційною інфраструктурою або можуть завдати їм шкоди [73, с. 61]. Стандарт ICO/IEC 27032 визначає кібербезпеку через категорію безпеки кіберпростору – збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. При цьому кіберпростором вважається середовище, що виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [74].

Основним багатостороннім міжнародним документом з інформаційної безпеки є Конвенція про кіберзлочинність (Будапештська конвенція), прийнята Радою Європи в 2001 році. Ця Конвенція містить класифікацію комп'ютерних злочинів, а також рекомендації органам законодавчої і виконавчої влади держав щодо боротьби з цими злочинами [75]. Також важливою віхою у забезпеченні кібербезпеки на міжнародному рівні є Директива про безпеку мереж та інформаційних систем (The Directive on security of network and information systems (NIS Directive), схвалена Європарламентом у 2016 році [76].

Водночас, з огляду на зростаючу роль кіберпростору та кібербезпеки, більшість країн розробляє власні стратегії кібербезпеки та відповідне національне законодавство. Зокрема, наразі 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 інших країн затвердили національні стратегії кібербезпеки [77].

У національних стратегіях кібербезпеки переважно здійснюється:

– визначаються цілі та заходи, спрямовані на розвиток обігу електронної інформації, а також забезпечення її конфіденційності, доступності та цілісності в кіберпросторі;

– розглядається забезпечення інформаційної безпеки та кібербезпеки як необхідна умова нормального функціонування й розвитку суспільства;

– наголошується на тому, що інформаційні системи повинні бути здатні протистояти загрозам у кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації;

– визначаються цілі і способи розвитку державних можливостей і необхідної законодавчої бази для участі в міжнародній боротьбі з кіберзлочинністю.

В Україні кібербезпека розглядається як складова національної безпеки. Стратегія кібербезпеки України була затверджена Указом Президента України від 15 березня 2016 року [78]. Ця Стратегія базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV [79], законодавства України щодо забезпечення національної безпеки, законодавства з питань засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та іншої захищуваної інформації, а також спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [80].

Стратегія кібербезпеки України належить до документів довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики у сфері кібербезпеки. На підставі Стратегії

кібербезпеки розробляються державні програми та нормативно-правові акти, що стосуються забезпечення кібербезпеки України [81, с. 130-132].

Реалізація положень Стратегії передбачається щорічними планами, які формуються Державною службою спеціального зв'язку України та захисту інформації й затверджуються Розпорядженнями Кабінету Міністрів України.

Як зазначає Н. Ткачук, аналіз стану виконання на загальнодержавному рівні планів реалізації Стратегії кібербезпеки України свідчить про те, що вказані документи мають переважно декларативний характер, а більшість заходів, передбачених ними, досі не виконано або виконано частково та/або із простроченням установлених термінів. Наразі розпочато процес розробки проєкту Стратегії кібербезпеки України на 2021 – 2025 роки, щодо якої також існує ризик декларативного виконання внаслідок формального підходу до стратегічного планування у сфері кібербезпеки [81]. На нашу думку, однією з причин такого стану речей є недостатня розвиненість правового забезпечення як кібербезпеки в Україні так й інформаційної безпеки загалом. Як вірно з цього приводу зазначають О. Довгань та Т. Ткачук «прийняття базового Закону України «Про інформаційну безпеку України» вбачається необхідним задля консолідації, вдосконалення відповідного законодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, лакун та інших вад» [82, с. 98]. Водночас, як слушно зауважує І. Доронін, і це є актуальним і сьогодні, у питанні розробки нормативно-правових актів немає системного підходу та належного теоретичного підґрунтя [83, с. 110].

Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий 5 жовтня 2017 року [39], заклав загальні засади побудови національної системи кібербезпеки, а також визначив основні завдання та компетенцію суб'єктів забезпечення кібербезпеки, до яких належать Національний координаційний центр кібербезпеки, Міністерство оборони, Генеральний штаб Збройних Сил, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Національна поліція,

Національний банк, розвідувальні органи України тощо. Законом також передбачено створення умов для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації, та/або є власниками (розпорядниками) об’єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об’єднань і громадян [84]. До основних досягнень зазначеного Закону також належить впровадження до правового поля визначень, що стосуються кібербезпеки, кібератак і кіберзахисту тощо. Відтак Закон України «Про основні засади забезпечення кібербезпеки України» є одним з перших та дуже важливих кроків держави у сфері регулювання кіберпростору. Також вводиться поняття «критична інформаційна структура», об’єкти якої будуть зобов’язані проходити обов'язковий аудит з кібербезпеки й відповідати інфраструктурним вимогам Кабінету Міністрів України [85].

Окрім зазначеного Закону законодавчу база з питань кібербезпеки і протидії кіберзлочинності в Україні наразі становлять:

– Закон України «Про національну безпеку України» від 21 червня 2018 року [33];

– Кримінальний кодекс України від 5 квітня 2001 року [86];

– Закон України «Про Службу безпеки України» від 25 березня 1992 року [87];

– Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 року [88];

– Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» від 30 червня 1993 року [89];

– Закон України «Про Державну службу спеціального зв’язку та захисту інформації України» від 23 лютого 2006 року [90];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року [91];

– Закон України «Про інформацію» від 2 жовтня 1992 року [92];

– Закон України «Про телекомунікації» від 18 листопада 2003 року [93];

– Закон України «Про державну таємницю» від 21 січня 1994 року [94];

– Закон України «Про захист персональних даних» від 1 червня 2010 року [95];

– Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року [96].

До актів вторинного законодавства з питань кібербезпеки і протидії кіберзлочинності в Україні можуть бути віднесені:

– Указ Президента України № 96 від 15 березня 2016 року Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" (яка вже згадувалася вище);

– Указ Президента України № 505/98 від 22 травня 1998 року «Про затвердження Положення про порядок здійснення криптографічного захисту інформації в Україні» [97];

– Указ Президента України № 1229/99 від 27 вересня 1999 року «Про затвердження Положення про технічний захист інформації в Україні» [98];

– Указ Президента України № 242/2016 від 7 червня 2016 року «Про затвердження Положення про Національний координаційний центр кібербезпеки» [99];

– Указ Президента України № 8/2017 від 16 січня 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» [100];

– Указ Президента України № 32/2017 від 13 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [101];

– Указ Президента України № 254/2017 від 30 серпня 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32» [102];

– Постанова Кабінету Міністрів України № 1519 від 11 жовтня 2002 року «Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям» [103];

– Постанова Кабінету Міністрів України № 303 від 14 травня 2015 року «Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку» [104];

– Постанова Кабінету Міністрів України № 563 від 23 серпня 2016 року «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [105];

– Розпорядження Кабінету Міністрів України № 1009 від 06 грудня 2017 року «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» [106];

– Постанова Кабінету Міністрів України № 518 від 19 червня 2019 року «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [107] та деякі інші.

Слід зазначити, що активно ведеться законопроєктна робота. Зокрема, у Верховній Раді України 8-го скликання були зареєстровані такі законопроєкти:

– проєкт Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо розмежування підслідності злочинів, вчинених у сфері використання електронно - обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і

мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури» (реєстр. № 8304);

– проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за злочини, вчинені у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, державних інформаційних ресурсів і об'єктів критичної інформаційної інфраструктури, та відповідальності за пошкодження телекомунікаційних мереж» (реєстр. № 8304-1);

– проєкт Закону України «Про внесення змін до Кримінального кодексу України (щодо посилення відповідальності за кібертероризм та кіберзлочини)» (реєстр. №2328а);

– проєкт Закону України «Про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм» (реєстр. № 439а);

– проєкт Закону України «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» (реєстр. № 2133а);

– проєкт Закону України «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю» (реєстр. № 2133а-1);

– проєкт Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері» (реєстр. № 6688);

– проєкт Закону «Про критичну інфраструктуру та її захист, розроблений Міністерством економічного розвитку і торгівлі» (реєстр. № 10328) [108, с. 25-26].

При цьому у Верховній Раді України 9-го скликання зареєстрований проєкт Закону про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (щодо підтвердження

відповідності інформаційної системи вимогам із захисту інформації) (реєстр. № 2043 [109]. Крім того, був перереєстрований згаданий вище проект Закону «Про критичну інфраструктуру та її захист, розроблений Міністерством економічного розвитку і торгівлі». Також триває робота над розробкою нових редакцій Законів України «Про Службу безпеки України» та «Про оперативно-розшукову діяльність».

Наразі опрацьовуються, зокрема, такі проєкти актів вторинного законодавства, розроблені Державною службою спецзв'язку і захисту інформації:

– проєкт постанови Кабінету Міністрів України «Про затвердження вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та порядку проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»;

– проєкт постанови Кабінету Міністрів України «Про затвердження Порядку формування переліку об'єктів критичної інформаційної інфраструктури, внесення об'єктів критичної інформаційної інфраструктури до державного реєстру об'єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування»;

– проєкт постанови Кабінету Міністрів України «Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, критеріїв та порядку віднесення об'єктів до об'єктів критичної інфраструктури» [108, с. 26-27].

Відзначаючи позитивну динаміку розвитку законодавства у сфері забезпечення кібербезпеки, слід зауважити, що є необхідність привести національне законодавство у відповідність до міжнародних стандартів. Зокрема, у законодавстві України не наведені визначення таких термінів як "користувач послуг", "дані про рух інформації" та "електронні докази" і не врегульовано такі категорії як "термінове збереження комп'ютерних даних, які зберігаються", "термінове збереження та часткове розкриття даних про рух інформації", що заважає ефективному виконанню положень Будапештської

конвенції та обмежує можливості взаємодопомоги з іншими країнами у сфері попередження кіберзлочинності та протидії кіберзлочинам.

Крім того, експерти визначають такі проблемні моменти правового забезпечення кібербезпеки в Україні [108, с. 29]:

– непослідовність у термінології, адже Закон України “Про основні засади забезпечення кібербезпеки України” впроваджує низку нових термінів, які не узгоджуються з термінами, які раніше використовувались у законодавстві;

– відсутність закону про критичну інфраструктуру, внаслідок чого наразі відсутня єдина національна система захисту критичної інфраструктури, а регуляторні правила щодо її захисту - недостатні та непослідовні;

– немає правил щодо проведення аудитів інформаційної безпеки об’єктів критичної інфраструктури, які мають ґрунтуватись на міжнародних стандартах, включаючи стандарти Європейського Союзу і НАТО, і розроблятися з обов’язковим залученням представників основних національних суб’єктів сфери кібербезпеки, наукових установ, незалежних аудиторів, експертів з кібербезпеки тощо;

– дублювання підвідомчості (до основних органів, відповідальних за контроль кібербезпеки в Україні, належать Міністерство оборони України, Державна служба спецзв’язку та захисту інформації, Служба безпеки України, Національна поліція України, Національний банк України та розвідувальні органи). Існує правова невизначеність щодо повноважень, завдань та обов’язків державних агенцій, відповідальних за захист критичної інфраструктури. Наприклад, хоча Закон України “Про основні засади забезпечення кібербезпеки України” передбачає повноваження Служби безпеки України щодо кіберінцидентів, це не відображено належним чином в інших нормативно-правових актах. Правоохоронні повноваження, на кшталт тих, про які йдеться в Будапештській конвенції, не є чітко визначеними в українському кримінально-процесуальному законодавстві, і це негативно

впливає на співробітництво між надавачами правоохоронних послуг, на права конфіденційності, а іноді й на верховенство права;

– немає вимог щодо безпеки та інформування для операторів об’єктів критичної інфраструктури та провайдерів цифрових послуг. Директива NIS [110] вимагає, щоб країни встановили вимоги щодо безпеки та інформування для операторів суттєвих послуг і для провайдерів цифрових послуг. Закон України «Про основні засади забезпечення кібербезпеки України» вимагає від операторів об’єктів критичної інфраструктури інформувати CERT-UA про кіберінциденти, однак, оскільки законопроєкт про критичну інфраструктуру перебуває на розгляді, ця норма залишається декларативною. Постановою Кабінету Міністрів України № 518 від 19 червня 2019 року [107] визначено, що власник та/або керівник об’єкта критичної інфраструктури зобов’язані організувати невідкладне інформування CERT-UA (у разі наявності - галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління Служби безпеки України (Ситуаційний центр забезпечення кібербезпеки Служби безпеки України) або відповідного підрозділу регіонального органу Служби безпеки України про кіберінциденти та кібератаки, які стосуються його об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Однак, процедура й терміни такого інформування не встановлені. Крім того, чітко не визначено, чи належать провайдери цифрових послуг до категорії об’єктів критичної інфраструктури;

– не проводиться довгострокове стратегічне планування з чітко визначеними проміжними результатами, часовими рамками та відповідальністю за їх досягнення;

– бюджетні обмеження здатності держави платити конкурентоспроможні зарплати для залучення та утримання високопрофесійних фахівців із питань кібербезпеки [108, с. 35].

Також, виходячи з аналізу базових категорій, які наводяться в Законі України «Про основні засади забезпечення кібербезпеки України», вважаємо за доцільне на законодавчому рівні визначити таке:

– поняття «стан захищеності»;
– поняття «цифрове комунікативне середовище»;
– критерії забезпечення кібербезпеки.

Визначення терміна «кібербезпека» базується на дефініції терміна «*кіберпростір*», який у Законі «Про основні засади забезпечення кібербезпеки України» визначено як *«середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних».*

Запропоноване визначення беззаперечно виключає з поля дії автономні автоматизовані системи управління (наприклад, об'єктів атомної енергетики), які, саме з огляду на вимоги безпеки, є автономними.

Надане визначення терміна «кіберпростір» суб'єктно обмежує «простір» лише інформаційними (автоматизованими), телекомунікаційними та інформаційно-телекомунікаційними системами, тобто автоматизованими системами.

Крім того, у Законі не надано визначення терміна «середовище», що призводить до невизначеності у тлумаченні терміна «кіберпростір».

Кіберпростір – це специфічне інформаційне середовище, якому притаманні особливі просторово-часові властивості транскордонності, екстериторіальності, децентралізованості, багатоканальності, розгалуженості, імітаційності, гіпертекстовості, віртуальності; яке виникло й функціонує за допомогою комп'ютерів та інших електронних пристроїв (супутників, телевізійних пристроїв, засобів стільникового зв'язку, ігрових приставок і т.п.) на базі інформаційно-телекомунікаційних мереж, насамперед Інтернет, а тому має, зазвичай, параметри глобального інформаційного обсягу й виконує

функції комунікації, розміщення й використання інформації, надання інформаційних та інших соціально значущих послуг, взаємодії державних інституцій, громадянського суспільства й окремої особи; яке є імітаційним чинником впливу на індивідуальну, групову та масову свідомість, економічну, соціально-політичну, духовну (культурну, ідеологічну, наукову, освітню, релігійну) та інші сфери життєдіяльності суспільства.

Варто також зазначити, що широко вживані в науковому та професійному вжитку терміни «захист інформації», «захист інформаційних технологій» і «захист кіберпростору» дещо різняться за змістом. Не заглиблюючись у деталі, можна сказати, що захист інформації являє собою сукупність методів і засобів, які забезпечують цілісність, конфіденційність і доступність інформації в разі впливу на неї загроз природного або штучного характеру. Натомість безпека інформаційних технологій передбачає ще й захист технічної частини та забезпечення працездатності, зокрема під час кібератак. Захист же кіберпростору – це безпека комунікаційних систем, об’єктів критичної інформаційної інфраструктури, комунікацій та систем керування [111, с. 24].

На законодавчому рівні необхідність захисту кібернетичного простору вперше передбачено воєнною доктриною США «Concept Force XXI» (1996) [112]. З усвідомленням глобального характеру кібербезпеки зросла роль міжнародних інститутів у розв’язанні цієї проблематики. Приміром, Міжнародний союз електрозв’язку (ITU) сформулював таке визначення кібернетичної безпеки в контексті діяльності цієї організації: сукупність безпекових принципів, стратегій і засобів забезпечення, гарантії безпеки, основні засади управління ризиками, діяльність, підготовка кадрів, практичний досвід, страхування, механізми й технології захисту кібернетичного простору, ресурсів союзу та користувачів. Загальними завданнями забезпечення кібербезпеки було визначено гарантування цілісності, доступності та конфіденційності інформації [113-114].

Донедавна кібернетичну безпеку США американські військові фахівці

тлумачили у вказаній вище традиційній тріаді: конфіденційність – доступність – цілісність: система заходів, спрямованих на захист комп'ютерів, електронних даних і мереж їх передання від несанкціонованого доступу та інших спроб маніпулювання (викрадення), блокування, умисного чи випадкового псування, трансформації, спотворення, руйнування та знищення інформації [115]. А у словнику військової й дотичної термінології, виданому оборонним відомством США у 2019 році, безпека кіберпростору, себто кібербезпека – це вжиті в захищеному кіберпросторі заходи щодо запобігання несанкціонованому доступу, експлуатації або пошкодженню комп'ютерів, електронних систем зв'язку та інших інформаційних технологій, у тому числі інформаційних технологічних платформ, а також наявної в них інформації, для забезпечення її доступності, цілісності, автентичності, конфіденційності й достовірності [116]. Як бачимо, буквально за лічені роки базовий термінологічний апарат Міністерства оборони США у галузі кібербезпеки істотно оновився, що свідчить про вміння американських фахівців швидко реагувати на зміни та актуальні виклики у цій сфері. На жаль, вітчизняний законодавець подібною гнучкістю не відзначається: система цих заходів до сьогодні визначена як «технічний захист інформації» (ТЗІ) [117].

Дискусійні аспекти законодавчого визначення базових категорій можуть бути певними причинами деформацій самої мети та предмета правового регулювання, а також неправильного визначення комплексу заходів щодо правового забезпечення кібербезпеки.

Так, вважаємо доцільним у визначенні терміна «*кіберзлочин*» словосполучення «міжнародними договорами» замінити на словосполучення «міжнародним правом». Такий підхід забезпечить єдність термінологічного тлумачення на рівні національного та міжнародного законодавства.

Сьогодні поняття кіберзлочину охоплює цілу низку правопорушень, зокрема: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж тощо (так зване «хакерство»); фальшування й шахрайство за допомогою

комп’ютера, наприклад, фішинг (незаконний спосіб отримання персональної інформації – паролів, номерів банківських рахунків чи кредитних карт тощо шляхом розсилання від імені банку електронних листів із посиланнями на підроблені сайти, які імітують роботу справжніх, або створення точної копії існуючої банківської веб-сторінки, аби змусити користувача ввести свої особисті фінансові дані) чи його різновид фармінг (при вході на веб-сторінку справжньої установи відбувається переспрямування на підроблену сторінку); правопорушення у сфері інформаційних ресурсів, приміром, дитяча порнографія чи розповсюдження піратського контенту, та ін.

Походження кіберзлочинів пов’язане зі, здавалося б, малошкідливим бажанням хакерів засвідчити свою високу майстерність за допомогою впровадження різних комп’ютерних вірусів. Але доволі швидко зловмисники зрозуміли, що це може давати великий зиск. Так виникла нова «галузь» злочинного бізнесу, котра почала застосовуватися в багатьох інших сферах – діяльності розвідок, промисловому шпіонажі, тероризмі й ін.

Слід також зазначити, що поширенню кіберзлочинності посприяла недосконаліть регуляторних механізмів, створення яких не встигало за стрімким розвитком всесвітньої комп’ютерної мережі. Кіберзлочинці миттєво реагують на всі новації у цій сфері, тоді як неповоротні державні структури й розробники систем інформаційної безпеки роблять це значно повільніше. У той час, коли злочинні кібератаки набувають загрозливої регулярності, стають усе більш складними й витонченими, виявляються вже постфактум або не виявляються зовсім, здійснюються віддалено й анонімно, існуючі системи контролю за несанкціонованим проникненням та противірусні програми дуже швидко застарівають і не в змозі забезпечити належний захист.

Сьогодні кібернетичні нападники за допомогою соціальної інженерії, різноманітних шахрайських трюків можуть атакувати через Інтернет найуразливішу ланку більшості кінцевих користувачів, їхніх безпекових моделей, переконуючи жертву, що вона має справу з легальним суб’єктом правовідносин. Мало того, постійне вдосконалення зловмисниками форм,

методів і засобів приховування себе і своїх цілей, як уже зазначалося вище, дає їм змогу діяти, не особливо хвилюючись про викриття, а про затримання чи засудження годі й говорити.

Злочинна діяльність в інформаційній сфері набуває масштабів величезної галузі тіньової економіки зі своїми виробниками, виконавцями, замовниками, постачальниками, споживачами тощо відповідних продуктів і послуг, перелік яких постійно зростає. Це, зокрема, отримання несанкціонованого й прихованого доступу до електронних систем, викрадення та зберігання різних даних, особистісних ідентифікаторів тощо, бот-мережі, хибне переадресування, ідентифікація користувача та багато іншого. Крім уже згадуваної анонімності, кіберпростір приваблює злочинців можливістю створення об'єднань, зокрема транснаціональних, виявити учасників яких та довести їхні зв'язки вельми проблематично.

На жаль, тенденції, які спостерігаються, свідчать про те, що в найближчій перспективі кібернетична злочинність, зокрема й організована, прогресуватиме. Насамперед це зумовлено зростанням доступності кібертехнологій для широкого користувача, коли, приміром, не складно придбати онлайн програмний інструментарій, за допомогою якого можна обходити безпекові заходи, ідентифікувати відкриті порти тощо. Тому, навіть пересічний користувач без особливих «хакерських» здібностей може стати кібернетичним правопорушником.

Інший чинник – це зміна контингенту користувачів Інтернету та доступності відповідних технологій. Так, у середині нульових років 21-го століття в країнах, що розвиваються, їх було значно більше, ніж у країнах розвинутих. Тому цілком логічно припустити, що кількість зловмисників та інтенсивність їхніх кібератак зростатиме, позаяк число об'єктів правопорушень змінюється набагато повільніше.

Кількість кіберзлочинів, зокрема й хакерських атак, може зростати лавиноподібно за рахунок розширення частотних діапазонів і застосування автоматизації, що дає змогу дуже швидко розповсюджувати шкідливий

кіберпродукт.

Подібного пояснення, як і поняття «кіберзлочин», потребують і формулювання дефініцій інших термінів, зокрема «кібертероризм», «кібероборона» тощо.

Стосовно терміна *«критично важливі об'єкти інфраструктури (критичні інфраструктурні об'єкти)»,* зауважимо, що запропоноване формулювання та розкриття цього терміна не передбачає виділення саме об'єктів такої інфраструктури, а вказує лише на «підприємства, установи та організації незалежно від форм власності».

Ми підтримуємо думку тих дослідників, які відстоюють доцільність прийняття Закону України «Про об'єкти критично важливої інформаційної інфраструктури» [118-119]. Проте, на наше переконання, безпосереднє створення системи забезпечення безпеки об'єктів критично важливої інформаційної інфраструктури повинно бути відображено у відомчому нормативному акті та включати відповідну сукупність заходів, а саме:

- встановлення рівнів забезпечення безпеки, які поділяються на такі види: загальний рівень, на якому заходи забезпечення безпеки об'єктів реалізується працівниками структурних підрозділів, співробітниками уповноважених державних органів, іншими уповноваженими особами; спеціальний рівень, на якому заходи реалізуються працівниками служби безпеки об'єкта; аналіз, визначення та моделювання загроз безпеці й інцидентів безпеки; проведення першочергових заходів, основними з яких є розробка: концепції забезпечення інформаційної безпеки об'єкта, положення про службу безпеки об'єкта, положення про підрозділ інформаційної безпеки тощо;

- підготовку типових планів: підвищеної готовності об'єкта до діяльності в умовах реалізації загроз; дій персоналу об'єкта при реалізації загроз безпеки та виникненні інцидентів безпеки; забезпечення безпеки в особливих умовах.

У визначенні терміна *«інцидент кібербезпеки (кіберінцидент)»* необхідно зазначити вид безпеки, а також замінити слово «зриву» на інше або надати ширше та зрозуміліше його тлумачення.

Також, на нашу думку, визначення терміна *«кіберзагроза»* не співвідноситься за обсягом інформації, наведеної у терміні «кібербезпека», та не відповідає визначенню цього терміну.

У тлумаченні терміна *«національні електронні інформаційні ресурси (національні інформресурси)»* застосований вираз «*у цифровій чи іншій нематеріальній формі*» є некоректним з огляду на то, що «цифрова» форма представлення інформації є матеріальною.

Аналіз законодавчого підходу до терміну *«національна телекомунікаційна мережа»* дає можливість висловити припущення порушення законодавчої техніки нормотворення. Адже використання виразів на кшталт «інших комунікаційних систем» є неоднозначним. Відповідно, при визначенні даного терміна необхідно чітко прописати перелік таких комунікаційних систем. Також звертає увагу той факт, що жодна телекомунікаційна мережа, зокрема й національна, з огляду на визначення терміну «телекомунікаційна мережа», наведеного у статті 1 Закону «Про телекомунікації» [93], не призначена для створення, оброблення, зберігання національних інформресурсів, надання спектру сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг, для надання послуг, зокрема із кіберзахисту, іншим споживачам.

З урахуванням наведеного, зазначений термін потребує доопрацювання та приведення у відповідність до чинного законодавства.

Визначення терміна *«система електронних комунікацій (комунікаційна система)»* не відповідає визначенню, даному в Директиві 2002/21/ЄС Європейського парламенту та ради від 7 березня 2002 [120] року про спільні правові рамки для електронних комунікаційних мереж та послуг (Рамкова Директива): «*електронна комунікаційна мережа* – комплекс активних і пасивних технічних засобів, ресурсів, споруд, призначених для передачі та/або прийому, маршрутизації, комутації електромагнітних сигналів дротовими, радіо, оптичними чи іншими електромагнітними системами та засобами, включаючи супутникові мережі, фіксовані (з комутацією каналів і з

комутацією пакетів, в тому числі Інтернет) та мобільні наземні мережі, електричні кабельні мережі в тій мірі, в якій вони використовуються для передачі сигналів, мережі, що використовуються для радіо і телевізійного мовлення, мережі кабельного телебачення, незалежно від типу інформації, що передається».

Отже, Закон України «Про основні засади забезпечення кібербезпеки України» радше є дорожньою картою для розробки майбутніх нормативних актів, а не всеосяжним законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам і найкращим практикам. Подальше вдосконалення правового забезпечення кібербезпеки в Україні передбачає виконання таких першочергових кроків:

– проведення аналізу чинного законодавства з метою виявлення норм, які суперечать Директиві NIS, а також неузгодженостей термінологічного характеру, внесення поправок відповідно до рекомендацій, вироблених на основі такого аналізу;

– розроблення стратегічної внутрішньої комунікації стосовно кіберінцидентів. Директива NIS вимагає від країн встановлення протоколів безпеки й комунікацій для операторів суттєвих послуг і провайдерів цифрових послуг;

– прийняття закону про критичну інфраструктуру та розробка на його основі відповідних підзаконних нормативно-правових актів;

– прийняття закону про державно-приватне партнерство у сфері кібербезпеки (Закон України “Про основні засади забезпечення кібербезпеки України” визначає варіанти державно-приватного партнерства, однак не визначаються механізми їх реалізації);

– розмежування повноважень державних органів у сфері забезпечення кібербезпеки, передусім шляхом внесення змін до законів, що визначають правовий статус і компетенцію Служби безпеки України та Державної служби спецзв’язку та захисту інформації;

– оцінювання реалізації Стратегії кібербезпеки 2016 року та розроблення Стратегії кібербезпеки на період 2021-2025 років і відповідного Стратегічного плану [108].

Упродовж останніх років нашою державою здійснено низку позитивних кроків для виконання своїх міжнародних зобов'язань щодо вдосконалення законодавства у сфері кібербезпеки, однак цей напрям роботи все ще потребує значної уваги та відповідних зусиль.

Оскільки розвиток правового забезпечення кібербезпеки в Україні пов'язаний з євроінтеграційними прагненнями України, дієвою для вдосконалення національного законодавства у сфері кібербезпеки з урахуванням умов Угоди про асоціацію між Україною, з однієї сторони, і ЄС та державами-членами, з іншої сторони (2014) буде імплементація досвіду та кращих практик країн ЄС і стандартів НАТО. Зокрема, найближчим часом Україна має розробити вимоги для операторів об'єктів критичної інфраструктури щодо інформування із зазначенням обставин, за яких вони повинні інформувати про інциденти, формату, шаблонів та процедури такого інформування, а також категоризації кіберінцидентів, встановити процедуру інформування інших країн про кіберінциденти, які можуть на них вплинути, з урахуванням вимог конфіденційності та комерційної таємниці, провести аудит чинного законодавства на предмет виявлення норм, які суперечать Директиві NIS, а також неузгодженостей термінологічного характеру, на законодавчому рівні розмежувати й конкретизувати повноваження та сферу відповідальності суб'єктів забезпечення кібербезпеки.

2.2 Теоретико-правові засади визначення об’єктів кібербезпеки України

Слід зазначити, що віртуальну кібернетичну сферу, комплекс проблем, пов’язаних з її використанням, викликами й безпекою, сьогодні дослідники називають здебільшого інформаційним простором, інформаційною безпекою тощо. Утім, на нашу думку, ці поняття не є тотожними. Як випливає з аналізу поглядів з цього приводу вітчизняних і зарубіжних дослідників, питання забезпечення інформаційної безпеки Інтернету вони вбачають складовою інформаційної безпеки. Це важливо як у контексті боротьби держави з загрозами в інформаційній сфері, кібертероризмом та іншими кібернетичними злочинами, так і в сенсі особистісному – захист персональних даних, фінансових інструментів тощо. Фахівці відзначають також застосування державами різних інформаційних технологій із метою завдання шкоди іншим країнам, їх економічного та політичного підпорядкування. Тому питання власне кібернетичної безпеки особи, суспільства й держави до останнього часу і науково розроблені слабо, і не мають належного нормативно-правового закріплення.

Повною мірою сказане вище стосується й поняття кібернетичного простору. Виходячи із проведених нами наукових розвідок, ми розглядаємо кіберпростір як специфічний інформаційний простір, котрий характеризується такими властивостями, як віртуальність, імітаційність, екстериторіальність, транскордонність, децентралізація, багатоканальність, гіпертекстовість. Він створений і функціонує за допомогою комп’ютерних та інших електронних засобів – телевізійних, супутникових, мобільного зв’язку тощо – на базі інформаційно-телекомунікаційних мереж, насамперед мережі Інтернет. Завдяки цьому цей простір має здебільшого параметри глобального інформаційного обсягу й виконує значну кількість функцій: комунікативну;

розміщення, накопичення й використання інформації; надання різноманітних соціально значущих послуг, передусім інформаційних; взаємодії, взаємозв'язку державно-владних інституцій із громадянським суспільством та кожним громадянином. Він є віртуальним чинником впливу як на свідомість окремого індивіда й груп людей, так і на масову свідомість, на усі без винятку сфери життєдіяльності суспільства.

У контексті визначення об'єкта правового забезпечення кібербезпеки України кіберпростір виступає водночас і об'єктом захисту, скажімо, інформаційних ресурсів, відповідних апаратних і програмних засобів тощо, і джерелом загрози для інших об'єктів національної безпеки. Ці загрози можна традиційно класифікувати за характером спрямованості на внутрішні й зовнішні, тобто такі, що виникають усередині національного сегмента інтернет-простору або ж зумовлені транскордонністю глобальної інформаційно-комунікаційної мережі. Однак не слід забувати, що однотипні загрози (приміром, кібернетичний тероризм чи інші хакерські атаки, комп'ютерні шахрайства, пропаганда насильства, расової, релігійної чи іншої ненависті тощо) можуть виходити як із середини, так і ззовні через екстериторіальність Інтернету. Останнє серйозно ускладнює можливість виявлення суб'єкта, від якого виходить загроза, джерело шкідливої інформації, оскільки Інтернет дає змогу реєструвати доменні імена сайтів в одній країні, а за допомогою різноманітних інструментів – пошукових систем, запитів, посилань тощо – поширювати інформацію в інших країнах.

Якщо ж вести мову про власне зовнішні загрози кібернетичній безпеці, то слід насамперед зважати на так звані інформаційні війни, які останнім часом набули особливого розмаху й нерідко призводять до вельми стрімкої зміни влади в деяких країнах. У таких війнах одним із головних напрямів «бойових дій» є формування суспільної думки, спрямування її у вигідному руслі, організація штучних масових кампаній за чи проти певного політичного курсу, партії, діяча тощо. Цьому явищу, яке отримало назву «астротерфінг», притаманне застосування спеціального програмного забезпечення (persona

management software), котре надає зловмисникам змогу створити в соціальних мережах ім'я, адресу, сайти, акаунти, тобто все те, що дає їм змогу ідентифікувати себе в Інтернеті як реальну особу. Астротерфінг (англ. astroturfing) – сучасний оплачуваний вид тролінгу, технологія маніпуляції суспільною думкою. Термін походить від назви «Astro Turf» – синтетичне покриття, яке замінює траву на стадіонах. Мета діяльності: поширення ідеї, події, факту або, навпаки, їх дискредитація, нівелювання значущості; формування потрібної суспільної думки, настроїв. Це також віртуальне зомбування Інтернет-користувачів. Використовується корпоративними лобістами, вірусними маркетологами, політтехнологами, спецслужбами. Іронічна назва – «п'ята колона Інтернету» [121, с. 21].

Традиційним у процесі визначення об'єкта правового забезпечення кібербезпеки України, є також визначення таких рівнів кібербезпеки, як безпека особи, суспільства й держави, в основу якого покладені конституційні принципи захисту життєво важливих інтересів зазначених суб'єктів. Але стосовно кібербезпеки вбачається доцільним надати пріоритет інтересам держави, позаяк від цього безпосередньо залежатиме й реалізація інтересів особи та суспільства. Тобто забезпечення кібербезпеки держави є передумовою особистісної та громадської кібернетичної безпеки.

Потреба виокремлення щодо інформаційних відносин, які виникають у кіберпросторі, особливого поняття «кібернетична безпека» зумовлюється також технічним, або технологічним чинником. Варто при цьому зауважити, що з технологічного погляду кібербезпеку, на відміну від безпеки інформаційної, не можна звести тільки до комп'ютерної безпеки, позаяк, крім власне технічного боку, кібернетична безпека містить інформаційну складову і той вплив, який вона чинить на всі сфери суспільно-політичного життя. Кібернетична безпека, як і та сфера, де вона регулює суспільні відносини, тобто кібернетичний простір, має два складники, котрі виводять її за межі безпеки суто інформаційної, істотно розширюючи діапазон дії, – інформаційний і технічний.

Разом з інформаційною безпекою існує окремий багатоаспектний напрям, який потребує окремого дослідження й розробки – кібернетична безпека. З урахуванням наведених вище міркувань, кожне з яких має певну рацію, ми виходимо передусім із специфіки об'єкта захисту – кібернетичного простору, котрий являє собою нерозривну єдність інформаційної й технічної (технологічної) складових, тобто інформації, яка циркулює й використовується з різною метою, та належних для цього технологічних умов.

Крім того, кібербезпека – це складова частина інформаційно-психологічної (духовної) безпеки, котра відображає стан інформаційного протиборства з реальними й потенційними геополітичними противниками й має сьогодні для України надзвичайно важливе значення та формує власний об'єкт правового забезпечення кібербезпеки. При цьому, інформаційно-психологічну безпеку ми розглядаємо як один із видів інформаційної безпеки, який характеризує стан захищеності від внутрішніх і зовнішніх загроз суспільного кібернетичного простору, загальнодержавних, військових і цивільних засобів масових комунікацій, а також суспільної свідомості.

Законом України «Про основні засади забезпечення кібербезпеки України» у статті 4 визначено об'єкти кібербезпеки та кіберзахисту. Так, до об'єктів кібербезпеки належать:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Законом визначено, що об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах

органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Від початку російської агресії на сході України кібератаки на підприємства та державні установи нашої країни стали численнішими й потужнішими. Ще наприкінці 2013 року під час Революції Гідності, за даними Міністерства оборони України, зафіксовано перші такі напади. Вже тоді понад два десятки українських підприємств і державних установ були уражені комп’ютерним вірусом «Uroboros» – так званим «хробаком», котрий здатен самостійно поширюватися локальними і глобальними комп’ютерними мережами [122]. Головне його призначення – викрадення інформації, зокрема паролів доступу до інформаційних ресурсів і персональних даних. Основними об’єктами атаки стали веб-ресурси органів державного управління, силових структур, великих промислових підприємств та засобів масової комунікації. Зухвалої й потужної DDoS-атаки зазнав у липні 2014 року офіційний веб-портал Президента України. Відтоді кібернетичні атаки все частіше спрямовувалися на фінансові й державні установи, об’єкти енергетики та безпекового сектору України.

Масштаби воєнних дій у кіберпросторі мало не щодня розширюються. Російська Федерація, за даними компанії «Zecurion Analytics», увійшла до числа країн із найрозвиненішим кібернетичним військом, витрачаючи на рік близько 300 мільйонів доларів на його утримання та розвиток [122]. Більше у цю сферу вкладають лишень Велика Британія, Китай і США.

Поняття кібернетичної безпеки включає сукупність захисних технологій, методів, способів і процесів для збереження цілісності програм, мереж і даних (інформаційних ресурсів) від кібернетичних (цифрових) атак.

Ці атаки провадяться зловмисниками з метою несанкціонованого (незаконного) доступу до інформаційних ресурсів, які захищаються, та копіювання (модифікації, трансформації, знищення тощо) відповідної інформації. У теперішній час кібернетичні атаки провадяться також задля дезорганізації (порушення) виробничих чи трудових процесів на підприємствах, в компаніях, організаціях або державах загалом.

У межах дослідження об'єкта правового забезпечення кібербезпеки України слід зазначити, що на сучасні безпекові виклики інформаційній сфері й вітчизняне, й міжнародне право реагують явно недостатньо, що створює сприятливі умови для хактивістських, екстремістських, терористичних суб'єктів для впливу на органи державної влади й досягнення інших злочинних цілей. Убачається, що шести статей розділу XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку» для адекватного реагування на всі злочини й загрози в інформаційній сфері явно замало. Тим паче, що ця сфера зачіпає сьогодні всі аспекти життєдіяльності людини, суспільства й держави, а не лише «використання комп'ютерів». Тому необхідність перегляду й оновлення вказаної нормативно-правової бази, диференційованого підходу як до загроз в інформаційній сфері, так і до складових цієї сфери (зокрема, різноманітних за рівнем і призначенням кіберсистем) цілком очевидна.

У цьому контексті варто зазначити недостатню реалізацію потенціалу правового захисту державного управління й систем керування об'єктами критично важливої інфраструктури. Ураховуючи значущість цих систем значно краще, ніж звичайні об'єкти, захищені фізично. Проте їх нормативно-правовий захист (особливо в сенсі юридичної відповідальності) практично не відрізняється. Тут, на наш погляд, може зарадити розвиток положень військового права, які стосуються інформаційної сфери, що значно підвищить рівень правового захисту складових інформаційної й кібернетичної сфер. Убачається за потрібне встановлення юридичної відповідальності за нові

склади правопорушень, пов’язаних з посяганням на системи державного, зокрема військового, управління та об’єкти критично важливої інфраструктури. При цьому кримінальна відповідальність за такі злочини має бути суворішим, ніж за «звичайні» комп’ютерні злочини. Удосконалення інформаційного безпекового законодавства на цій основі може, на нашу думку, привести його у відповідність до сучасних викликів і загроз.

Вважаємо, що необхідно також серед основних чинників національної безпеки враховувати показники кібер сфери, які відображають рівень наявних у ній правопорушень, посягань на системи державного й військового управління, об’єктів критичної інфраструктури. Звісно, подібні заходи потрібні й на рівні міжнародного права. Адже світова інформаційна сфера має бути захищена не лише від злочинних, а й від мілітаристських посягань. З метою забезпечення глобальної кібербезпеки міжнародно-правові норми в цій галузі мають враховувати військові потенції інформаційних технологій, регулювати діяльність відповідних сил і засобів. Природно, що безпека цивільних інформаційних об’єктів і критично важливої інфраструктури мають гарантуватися механізмами міжнародно-правової відповідальності та взаємними зобов’язаннями держав у межах дво- й багатосторонніх угод.

Для вдосконалення правового захисту систем управління (кіберсистем) об’єктів критичної інфраструктури пропонується розширити перелік злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів) зі встановленням суворішої відповідальності за посягання на такі об’єкти.

Отже, кібернетичну безпеку слід розглядати як самостійний вид безпеки, позаяк реалії сьогодення переконливо свідчать, що ця науково-правова категорія вийшла за межі інформаційного протиборства та військової безпеки і є елементом інформаційної сфери в цілому.

У цьому контексті кібернетична безпека – це також сукупність умов, які у фізичному, емоційно-психічному, духовно-освітньому, професійному, фінансовому, політичному та інших аспектах гарантовано забезпечують захищеність усіх компонентів інформаційних систем від якомога більшої

кількості загроз та негативних впливів у кіберпросторі або ж від руйнівних наслідків у разі похибок, нещасних випадків, псування, аварій та іншої шкоди в цій сфері.

Можна в такий спосіб витлумачити й предмет вивчення безпекової науки стосовно кіберсередовища: природні, соціально-економічні, соціально-політичні та техногенні процеси в контексті їхнього розвитку, взаємодії та утворення нових об'єктів і явищ, та їхніх елементів з навколишнім середовищем задля виявлення існуючих та потенційних небезпек, оцінювання відповідних ризиків та розробки адекватних методів і способів протидії, а також розробки належної нормативної бази для належної правової регламентації вимог, методик, механізмів, алгоритмів, застосування яких гарантує досягнення мети захищеності інтересів людини, суспільства й держави від наявних та можливих загроз.

Отже, із метою захисту всіх суб'єктів – від окремої особи до суспільства й держави в цілому – слід сформувати комплексну систему (доктрину, політику) їхньої безпеки, підґрунтям якої має стати кібербезпека. Себто створення захисту інформаційних систем від негативних впливів належить розпочинати саме з інформаційної безпеки як основи захищеності відповідних даних.

Що ж стосується кібернетичної безпеки, то в сучасних умовах, коли безліч суб'єктів усіх сфер життєдіяльності суспільства й держави збирають, обробляють і зберігають інформацію, необхідну їм для належного функціонування, персональні дані величезної кількості людей, важливість захисту цієї сфери важко переоцінити. Вказана вище й інша інформація є, переважно, конфіденційною, її втрата (витік, викрадення тощо) може призвести до негативних наслідків як для окремої особи, так і для спільнот, установ, держави.

Не дивно, що найпотужніших кібератак зазнають об'єкти критичної інфраструктури – ті, що безпосередньо забезпечують життєдіяльність, скажімо, міст, регіонів, країн, а то й усієї світової спільноти (об'єкти

енергетики, мережі постачання, транспорт, системи перероблення відходів та ін.). У той чи інший спосіб уся ця інфраструктура взаємодіє та керується за допомогою електронного обладнання, а від безпеки всіх інфраструктур, котрі взаємодіють, залежить їхнє стабільне функціонування, а відтак і нормальне існування суспільства.

Критичні інфраструктури (КІ) – це складні, багатоелементні, розподілені у просторі системи, стабільне функціонування яких критично важливе для економіки країни, усіх сфер людської життєдіяльності. Багатоступенева структура КІ складається з таких рівнів:

1) технічний – машини, устаткування, апаратура тощо;

2) соціальний – персонал;

3) організаційний – взаємодія експлуатаційних служб;

4) державне управління – державне регулювання відповідної сфери, нормотворчі й контрольні органи.

Складність критичних інфраструктур зумовлена їхньою вельми непростою структурою з нелінійними взаємозалежностями й різновекторними зв’язками елементів і рівнів системи та різних інфраструктур, а також складністю процесів і явищ, пов’язаних з функціонуванням КІ. Компонентами таких інфраструктур є технічні об’єкти, де провадяться певні дії, які можуть становити небезпеку: зберігання, переробка, транспортування різних видів енергії, небезпечних речовин, інформаційних потоків. У разі аварій тісні взаємозв’язки компонентів КІ можуть зумовити послідовне, каскадне їх наростання, коли охоплюється все більше елементів, а перебіг подій залежить від структури зв’язків між компонентами. Оскільки такі об’єкти можуть стати джерелом масштабних техногенних аварій і катастроф, то рішення стосовно їх нового будівництва чи, скажімо, модернізації приймаються тільки після ретельного всебічного вивчення можливих ризиків.

Останніми роками традиційні підходи до кібербезпеки стикнулися з вибуховим розвитком кіберзлочинності, розв’язуванням справжніх кібернетичних воєн: від стохастичних кібернападів на окремих осіб до

ретельно спланованих атак організованої злочинності та міждержавних актів агресії. Одним з останніх прикладів використання штучного інтелекту у військових цілях є вбивство іранського вченого-ядерника Мохсена Фахрізаде. Автономну зброю «контролювали онлайн із супутника», а люди безпосередньо в нападі на конвой Фахрізаде участі не брали. Іранське інформаційне агентство Fars повідомляло, що після вбивства Фахрізаде автомобіль нападників самознищився через вибух [123]. Тому, приміром, країни Євросоюзу для посилення кібербезпеки реагують на вказані виклики широкомасштабними програми та заходами. Так, ще у 2004 році для вироблення настанов і рекомендацій щодо захисту інформації було засноване Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) [124], котре згодом стало опікуватися й питаннями кібернетичної безпеки. Європейська комісія розробила Стратегію кібербезпеки [125], яка лягла в основу багатьох національних аналогічних документів у цій сфері [126]. Була також спланована та реалізована низка кібербезпекових заходів щодо налагодження в державах-членах ЄС відповідного управління, регулювання та координації, організації науково-дослідницької роботи. Це, наприклад: Директива щодо мережевої та інформаційної безпеки; програма з досліджень і розвитку «Обрій 2020»; налагодження міжорганізаційної та міжнародної співпраці у політичній та правоохоронній сферах; дії з кібербезпеки у Цифровому порядку денному для Європи [127] та ін.

Останній захід слід розглянути детальніше. Європейський Союз визначив першочергові заходи для посилення кібербезпеки в державах-членах, які вже впроваджені або впроваджуються в теперішній час. Ці заходи є складовою широкої всебічної програми «Цифровий порядок денний для Європи» [128]. Отже, вказані заходи передбачають:

– дія 28: посилення політики мережевої та інформаційної безпеки;

– дія 29: боротьба з кібератаками на інформаційні системи;

– дія 30: створення європейської платформи протидії кіберзлочинності;

– дія 31: аналіз доцільності створення Центру європейської протидії кіберзлочинності;

– дія 32: посилення боротьби з кіберзлочинністю та кібератаками на міжнародному рівні;

– дія 33: забезпечення готовності всього ЄС до дій із кібербезпеки;

– дія 34: дослідження розширення норм інформування про порушення безпеки;

– дія 35: настанови з упровадження правил забезпечення конфіденційності інформації в телекомунікаційних мережах;

– дія 36: забезпечення звітування про незаконний контент в Інтернеті та проведення інформаційно-роз'яснювальних кампаній щодо безпеки дітей в Інтернеті;

– дія 37: заохочення саморегулювання при використанні онлайн-сервісів;

– дія 38: впровадження в державах-членах загальноєвропейських команд реагування на комп'ютерні надзвичайні ситуації;

– дія 39: проведення в державах-членах навчань у формі симуляції кібератак;

– дія 40: запровадження в державах-членах «гарячих ліній» для скарг на шкідливий контент;

– дія 41: створення в державах-членах національних платформ для інформування про небезпеку;

– дія 123: проєкт директиви про мережеву та інформаційну безпеку;

– дія 124: стратегія кібербезпеки ЄС;

– дія 125: розширення Міжнародного альянсу проти сексуального насильства над дітьми в Інтернеті.

Для втілення вказаних планів та координування відповідних дій потрібні настанови й рекомендації із практичного впровадження заходів кібербезпеки в європейських реаліях. Насамперед задля цього низка документів про

впровадження європейської кібербезпеки користується загальновизнаними підходами та стандартами. Так, термін «кібербезпека» стосується корпоративного управління та надання безпекових гарантій, які виходять за межі традиційної інформаційної безпеки. Безпека кібернетична стосується специфічних форм складних атак у кіберпросторі, їхніх технічних і соціально-психологічних аспектів.

Величезна розмаїтість тлумачень кібернетичної безпеки нерідко призводить до хибного розуміння її сутності. Офіційна позиція ЄС із цього приводу така. Кібернетична безпека стосується здебільшого заходів і дій із захисту цивільного й військового сегментів кіберпростору від загроз, які можуть зашкодити взаємозалежним мережам та інформаційній інфраструктурі або пов'язаним з ними об'єктам. Завдання кібербезпеки – збереження цілісності й доступності інфраструктури й мереж та конфіденційності інформації, яка в них циркулює [129].

Важливе значення в окреслених процесах надається і державній політиці у забезпеченні кібербезпеки. Державна політика кібербезпеки має спиратися на наявну інформацію, зокрема й у разі відсутності офіційної оцінки та браку аналізу внутрішньої ситуації в країні. Організації мають послуговуватися офіційними джерелами, а також академічними й галузевими дослідженнями та матеріалами міжнародних і національних інституцій (приміром, Євробарометру [130-131], Європолу [132], статистичні дані ООН щодо кіберзлочинності [133], матеріали національних статистичних структур; інформація про інциденти з різних джерел, галузеві дослідження комерційних структур [134].

Події останніх років свідчать про збільшення кількості й потужності кібератак, їхній негативний вплив на об'єкти нападу зростає і стає тривалішим. У відкритих джерелах можна знайти додаткові дані про інциденти, пов'язані з конкретними кібератаками, фіаско, що його зазнали кібербезпекові заходи, тощо. Для формування достатньо обґрунтованої картини ця інформація може стати важливим генератором емпіричних даних, зокрема стосовно галузі

діяльності або розміру організацій. Але при цьому вбачається доцільним користуватися відкритими джерелами, які наводять матеріали оцінного характеру за різним критеріями, наприклад:

– щорічною оцінкою вартості витоку інформації «Інституту Понемона» [135];

– комерційними дослідженнями порушень інформаційної безпеки [136]);

– щорічними (як правило) комерційними дослідженнями інформаційної безпеки;

– дослідженнями команди реагування (CERT) на комп'ютерні надзвичайні ситуації [137].

Еволюція сучасного кіберпростору супроводжується виникненням нових загроз безпеці інформації та інформаційних технологій, а також виробленням відповідних захисних заходів. Такі тенденції закономірно приводять до розширення об'єкта правового забезпечення кібербезпеки. І це природно, позаяк ще з давніх-давен виробники будь-якої продукції, власники підприємств і комерсанти дбали про те, аби їхні виробничі секрети не потрапили до конкурентів, а також про фізичну безпеку засобів виробництва й персоналу. Згодом, коли виробництво почало набувати перших рис промислового, для опікування вказаними вище проблемами виникла відповідна спеціалізація – фахівець із безпеки компанії, чи, кажучи просто, – охоронець.

Зі зростанням обсягів виробничої, фінансової, дослідницької та іншої документації підприємства зіткнулися з потребою збереження секретних матеріалів – документів, креслень, листування й ін. – від оприлюднення, викрадення тощо. Тобто виникла необхідність у забезпеченні інформаційної безпеки. Таким чином, у контексті інформаційних технологій (IT) термін *«інформаційної безпека»* був уперше запроваджений у науковий і виробничий обіг. Початково забезпечення інформаційної безпеки полягало в обмеженні доступу до фінансової (бухгалтерської) інформації, різноманітної технічної та

управлінської документації, даних про патенти тощо. З цією метою ухвалювалися відповідні суворі правила (регламент) внутрішньої безпеки підприємства (організації). Збільшення числа комп'ютеризованих систем та автоматизованого інструментарію вивело ІТ-сферу на передній план, і на підприємствах з'явилися фахівці з інформаційної безпеки.

Початок третього тисячоліття позначився справжнім ІТ-бумом, коли комп'ютери з'явилися ледь не на кожному робочому місці й ледь не в кожній оселі, коли в руках пересічного користувача замість «звичайного» мобільного телефону опинилися смартфони, айфони і т. п. – міні-ЕОМ з величезною кількістю функцій. І, звісно, практично безмежні можливості відкрив Інтернет, право на доступ до якого резолюцією ООН у 2016 році було закріплено в переліку основних прав людини. Зростання числа гаджетів, девайсів, розумних речей, збільшення Інтернет-трафіку, потоків даних зумовило лавиноподібну діджиталізацію – перенесення у кіберпростір, у «хмару» все більшої кількості фінансових операцій, управління процесами, різних видів робіт. Відтак, виникла нагальна потреба захисту інформації саме в цифровому, кібернетичному середовищі.

Отже, кібербезпека – це спрямована саме на цифрове середовище нова стадія еволюції інформаційної безпеки, яку сьогодні переживає людство. Кібербезпека охоплює не тільки власне захист інформації, а й захист інформаційного-технологічного простору (поля комп'ютерних технологій) загалом та всіх його складових.

Поширення «Інтернету речей», криптовалют, криптобірж, систем електронного урядування й виборів, «розумних контрактів» та інших новітніх ІТ-технологій докорінно змінює кібернетичний простір. Вагомий внесок у розвиток теоретичних основ та правових засад інтернету речей зробив вітчизняний дослідник О. Баранов [138-140]. Однак не дивно, що відповідно зростає число зловмисних кібератак на глобальні критичні інфраструктури – системи енергопостачання, керування урядовими, фінансовими, промисловими й комерційними структурами, транспортом, загальні бази

даних. Досить лише згадати, якої шкоди завдала багатьом таким об'єктам в Україні (і в деяких інших країнах) хакерська атака із застосуванням різновиду комп'ютерного вірусу Petya у червні 2017 року.

Як уже зазначалося, кібербезпека включає в себе не тільки захист власне інформації. Це також захист від хакерських атак, комп'ютерних вірусів, викрадення, знищення чи підробки даних, що можуть призвести не лише до втрати інформації, а й до негативного впливу на роботу підприємства аж до її припинення, на продуктивність персоналу, використання даних проти людини або організації. Тобто об'єктом захисту кібербезпеки є сьогодні триєдність: системи – процеси – люди.

Потреба в особистій кібербезпеці надалі зростатиме, позаяк людина далі все більше залежатиме від комп'ютера та різноманітних гаджетів. Кібербезпека опікується захистом конфіденційної інформації та взаємодію з нею у процесі користування будь-яким пристроєм, аби не заразитися вірусом через, скажімо, розумний годинник чи пилосмок.

У серпні 2019 року на Всесвітній конференції зі штучного інтелекту в Шанхаї, де обговорювалися пов'язані з цією проблемою нагальні проблеми людства, Джек Ма та Ілон Маск зазначили: «*Ми ВЖЕ є кіборгами. Люди навіть не усвідомлюють, наскільки вони інтегровані з телефоном і комп'ютером. Коли ми забуваємо десь мобільний, то здається, ніби втратили частину тіла*». І це насправді так. Людина вже цілковито пов'язана зі своїми «мобілами», без яких не уявляє свого життя й не може зробити буквально ані кроку. Наш телефон – це спілкування, харчування, навчання, пересування, географія, погода, стан здоров'я та безліч інших можливостей, які допомагають нам у повсякденному житті.

З удосконаленням технологій, розвитком інформаційних систем та штучного інтелекту еволюціонує і зловмисний сегмент кібернетичної сфери – хакерство, комп'ютерні віруси, кібератаки тощо. Приміром, комп'ютерні віруси від часу їх створення вже неодноразово вдосконалювалися їхніми розробниками, зазнавали мутацій на кшталт їхніх біологічних аналогів. Так, із

1987 року такі віруси, проникаючи в систему, певним чином впливали на її роботу чи на зосереджену в ній інформацію – знищували («з'їдали»), шифрували, маніпулювали, трансформували, спотворювали. Приміром, вірус, котрий копіював дані аж до вичерпання місця на жорсткому диску, або вірус, що стовідсотково переобтяжував процесор.

Чергова істотна «мутація» сталася у 2012 році, коли в мережах з'явився вірус «ivchetoo», або «hallmark», котрий CNN назвала «найнебезпечнішим». Він призводив до фізичного згоряння жорсткого диску.

Однією з останніх вірусних мутацій і кібератак за її допомогою є вже згадуваний вище WannaCry, або Petya (2017 рік). Характерною особливістю цього вірусу було не те, що він шифрував дані, блокував доступ до них і вимагав за відновлення електронні гроші – Біткоїни. Головне, що він на доволі тривалий час зупинив роботу третини банківської системи всієї України. Це вельми негативно позначилося й на роботі авіатранспорту, метрополітену, деяких великих медіа- і промислових компаній. Дію вірусу першими відчули працівники бухгалтерій, котрі працювали з робочою програмою «1С» для подання бухгалтерської звітності, через яку вірус проникав у систему, а потім поширювався через неліцензійне програмне забезпечення. Petya показав, що кібератаки вірусних «мутантів» можуть призвести до тяжких наслідків, до зупинки роботи державних органів та інших об'єктів критичної інфраструктури. Таких масштабних проблем можна було б уникнути, якби об'єкти нападу та їхній персонал знали й дотримувалися базових правил кібербезпеки та кібергігієни.

Є всі підстави вважати, що подальші мутації кібератак можуть впливати на життєдіяльність і здоров'я людини. Приблизно від середини 2010-х років у світі стрімко поширюється новий IT-тренд на розумні пристрої і девайси – розумні годинники, холодильники, пилосмоки, фітнес-браслети, шоломи віртуальної реальності, окуляри доповненої реальності тощо. У 2016 році в Одесі під час конференції «BlackSeaSummi» вперше в Україні людині вживили електронний чіп у руку, котрою вона могла оплачувати рахунки, як

банківською карткою [141]. Згодом в інших країнах розпочали активно імплантувати чіпи, які замінюють ключі, географічні мапи, ідентифікаційні дані, а в 2019 році проект «xNT» почав розсилати своїм клієнтам чіпи для вживлення в руку [142]. Корпорація Apple започаткувала тренд на FaceID, який дає змогу ідентифікувати людину й розплачуватися на касі просто по обличчю.

Усе це яскраво засвідчує, що електроніка стає все ближчою до тіла, до м'язів, очей, до мозку людини, у прямому розумінні до її змісту. Тому існує серйозний ризик, що кібератаки можуть безпосередньо позначитися на фізичному стані людини, її здоров'ї. І чим ближче різнома апаратура наближена до тіла й мозку, тим більшого значення набуває захист відповідної інформації та її носіїв. Отже, наступною стадією відповідальності кібербезпеки має стати збереження інформації, процесів і девайсів, котрі щільно пов'язані з тілом і мозком, тобто фізичним життям людини.

Узагальнюючи сказане вище, зазначимо, що кібербезпека виникла як складова інформаційної безпеки, а нині – це еволюція інформаційної безпеки, оскільки від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації. «У руках» кібербезпеки сьогодні збереження системи, процесів, людського життя врешті-решт.

Для сучасних «інтелектуальних» атак у кіберпросторі характерним є те, що їм притаманна певна латентна стадія, тривалість якої може сягати кількох місяців, що вельми ускладнює процес їх виявлення. Тому нагальною вбачається потреба розроблення нових підходів до захисту телекомунікаційних мереж, об'єктів критичної інфраструктури, різних управлінських систем. Дієвість кібербезпеки може бути досягнута лише шляхом постійного комплексного застосування новітніх теоретичних напрацювань, організаційно-правових, криптографічних, технічних методів і засобів захисту.

У сучасних умовах світової глобалізації геополітична конкуренція

розгортається й загострюється не лише у традиційних межах, формах і методах. Протиборство поширюється також у штучно створеній віртуальній реальності – глобальному кібернетичному просторі електронних засобів масової комунікації. Відповідно визначити об’єкти правового забезпечення кібербезпеки України як завершену систему чи класифікацію неможливо. Така структура є динамічною та мінливою відповідно до національних та глобальних тенденцій змін у кіберпросторі. Тому перед кожною державою постає потреба створення ефективних засобів забезпечення своєї кібербезпеки.

За своєю руйнівною потенцією загрози кібербезпеці держави можна порівняти із загрозами воєнними у традиційному їх розумінні. Для нашої держави забезпечення кібербезпеки є сьогодні одним із пріоритетних напрямів забезпечення національної безпеки.

2.3 Система суб’єктів забезпечення кібербезпеки в Україні

Бурхливий технічний прогрес зумовив появу нових загроз як соціальній, так і індивідуальній безпекці, в результаті чого звична людині реальність вперше за всесвітню історію доповнена реальністю віртуальною - кіберреальністю. Кіберзагрози здійснили революцію в уяві людей про безпеку, правила й методи забезпечення національної безпеки тощо. У нашій країні для цих цілей був прийнятий Закон України «Про основи забезпечення кібербезпеки України», який, зокрема, вибудовує систему суб'єктів забезпечення кібербезпеки.

Передусім слід зазначити, що поняття «система суб’єктів забезпечення кібербезпеки» тісно пов’язане із поняттям «система забезпечення безпеки», як із більш загальним. На думку І. Тімкіна, «система забезпечення національної безпеки виступає як організаційна система державних та недержавних

інституцій, інших суб’єктів, які покликані вирішувати завдання забезпечення національної безпеки у визначений законодавством спосіб» [143]. М. Гетьманчук, В. Грищук, Я. Турчин вважають, що «загальна система забезпечення національної безпеки України – це єдиний державно-правовий механізм, у якому кожний суб’єкт безпеки виконує функції захисту національних інтересів у межах повноважень, які визначаються законодавством України» [144, с. 128]. Слід підтримати позицію Т. Ткачука, в тому, що «система забезпечення національної безпеки будується «від інтересів держави», більшість функцій, у тому числі у сфері забезпечення інформаційної безпеки, здійснюється саме державою, що дозволяє досягти балансу інтересів в інформаційній сфері. Щодо суспільного виміру інформаційної безпеки, то так звана «недержавна система безпеки» є не лише суб’єктом власного забезпечення, який самостійно визначає мету, принципи та методи забезпечення безпеки відповідно до законодавства України в межах загальної системи, але й становить об‘єкт забезпечення інформаційної безпеки з боку держави. У свою чергу, безпека людини становить складову метасистеми національної безпеки, яка об’єднує безпеку особи, суспільства та держави в різних сферах, зокрема в інформаційній» [2, с. 102]. Погоджуючись у цілому із таким підходом, вважаємо за необхідне уточнити, що система забезпечення кібербезпеки становить органічне поєднання спільною метою державних та недержавних інституцій, а також інших суб’єктів, які беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки. У цьому контексті важливе значення має розвиток державно-приватного партнерства, яке може мати різні форми: обмін інформацією, консультації, експертизи, сприяння й інші.

З цього приводу В. Бухарєв слушно зазначає, що «суб’єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки відносини між ними будуються на основі влади і підпорядкування, до того ж останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством» [145, с. 87].

Відтак суб'єктами забезпечення кібербезпеки, на думку науковця, є «державні органи та їх посадові особи, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки, які знаходяться у законній підпорядкованості між собою» [145, с. 88]. Це твердження є цілком справедливим, водночас вважаємо, що спектр суб'єктів забезпечення кібербезпеки не може обмежуватися тільки державними органами та їхніми посадовими особами. Якщо говорити про систему забезпечення національної безпеки в цілому, слід зазначити, що до її складу традиційно включають сили та засоби забезпечення національної безпеки [146, с. 42]. Це й стосується кібербезпеки.

Загальний перелік та засади розмежування компетенції суб'єктів забезпечення кібербезпеки визначаються у ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема, зазначеною статтею передбачено, що координація діяльності у сфері кібербезпеки здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони (РНБО) України. Таке повноваження ґрунтується на законодавчому розумінні кібербезпеки як складової національної безпеки і випливає із положень статті 106 Конституції України, згідно з якими Президент України забезпечує національну безпеку. Робочим органом РНБО України у вказаній сфері є національний координаційний центр кібербезпеки, котрий здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України [39].

Формування та реалізація державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю забезпечуються Кабінетом Міністрів (КМ) України. Уряд України також організовує та забезпечує необхідними силами, засобами й ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім

об’єктів критичної інфраструктури в банківській системі України). Кабінет Міністрів України є вищим органом у системі органів виконавчої влади, який реалізує свої функції безпосередньо та через міністерства, інші центральні органи виконавчої влади.

Суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібернетичної безпеки України, є: міністерства й інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні та контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності; Збройні Сили (ЗС) України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури; суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Тобто фактично забезпечення кібербезпеки є загальносуспільною справою, і перелік суб’єктів її забезпечення є невичерпним. У межах своєї компетенції суб’єкти забезпечення кібербезпеки здійснюють: заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; виявлення і реагування на кіберінциденти та кібератаки, усунення їхніх наслідків; інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробку та реалізацію запобіжних, організаційних, освітніх та інших заходів у сфері кібербезпеки, кібероборони та кіберзахисту; проведення аудиту інформаційної безпеки, зокрема й на підпорядкованих об’єктах та об’єктах, що належать до сфери їхнього управління; інші заходи із забезпечення розвитку та безпеки кіберпростору.

Законодавче підґрунтя забезпечення кібербезпеки, відповідно до якого визначається компетенція суб’єктів її забезпечення, становлять Конституція

України, Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Закони України «Про національну безпеку України», «Про Раду національної безпеки і оборони України», «Про Службу безпеки України», «Про Державну Службу спеціального зв'язку і захисту інформації України», Положення про Національний координаційний центр кібербезпеки тощо.

Одним із перших нормативно-правових актів, який визначив систему суб'єктів забезпечення кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [147]. У цьому документі вперше зустрічається термін «національна система кібербезпеки», куди входять головні учасники процесу захисту прав і свобод осіб у відносинах з приводу обробки та обміну інформацією у кіберпросторі [145, с. 90]. Зокрема, у Стратегії зазначається, що основу системи суб'єктів забезпечення кібербезпеки становлять Міністерство оборони (МО) України, Державна служба спеціального зв'язку та захисту інформації (ДСС) України, Служба безпеки (СБ) України, Національна поліція (НП), Нацбанк України, розвідувальні органи, на які мають бути покладені в установленому законом порядку спеціальні завдання. Натомість стаття 8 Закону України «Про основні засади забезпечення кібербезпеки України» [39] передбачає дещо інший перелік основних суб'єктів забезпечення кібербезпеки, що окремо виділяються в рамках загальної системи суб'єктів забезпечення кібербезпеки, передбаченої статтею 5 того ж Закону. До їхнього кола належать: РНБО України, Міністерство внутрішніх справ (МВС) України, МО України, Генеральний штаб ЗС України, СБ України, ДСС України, розвідувальні органи тощо. Ключова роль цих відомств у забезпеченні кібербезпеки зумовлена специфікою їх компетенції та основних напрямів діяльності, зокрема, можливістю вживати спеціальних заходів (у тому числі й заходів примусу) для підтримки належного рівня кібербезпеки, реалізуючи відповідну монополію держави.

Призначенням ДСС України є «забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону. ДСС України входить до складу сектору безпеки і оборони України. У сфері забезпечення кібербезпеки ДСС України займається формуванням та реалізацією політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури тощо» [90].

Національна поліція та СБ України наділені повноваженнями щодо припинення правопорушень, що посягають на кібербезпеку, та притягнення винних осіб до відповідальності. Зокрема, НП у сфері забезпечення кібербезпеки наділена повноваженнями щодо: «забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі» [148]. У своїй діяльності НП підпорядковується КМ України і спрямовується та координується через МВС України, на яке покладається реалізація повноважень щодо: створення і забезпечення функціонування

підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення та забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів тощо [33].

Служба безпеки України наділена повноваженнями щодо протидії правопорушенням у кіберпросторі відповідно до своєї компетенції. Призначенням СБ України є забезпечення державної безпеки, тож у Законі України «Про основні засади забезпечення кібербезпеки України» закріплено, що СБ України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [87].

Якщо вести мову про повноваження МО України та Генерального штабу ЗС України у сфері забезпечення кібербезпеки, то слід зазначити, що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» вони є майже ідентичними: зазначені державні органи здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [33]. Водночас відповідні повноваження

реалізуються кожним із цих державних органів у межах його законодавчо визначеної компетенції, відтак МО є координаційним політичним центром, який реалізує політику держави у сфері забезпечення кібербезпеки, тоді як Генеральний штаб є оперативним органом, діяльність якого спрямована на подолання реальної агресії та виконання бойових завдань у випадках, передбачених законодавством [145, с. 99].

Розвідувальні органи (Служба зовнішньої розвідки України, розвідувальні органи МО, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону [145, с. 200]) здійснюють у сфері забезпечення кібербезпеки розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки [33].

Важливе місце у системі забезпечення кібербезпеки займає Нацбанк України, який розробляє та впроваджує у свою діяльність сучасні електронні банківські технології, новітні платіжні та облікові системи тощо. Оскільки основною функцією Нацбанку, відповідно до Конституції України, є забезпечення стабільності грошової одиниці України, у сфері забезпечення кібербезпеки на нього покладається: формування вимог щодо кіберзахисту критичної інформаційної інфраструктури в банківській сфері; визначення порядку, вимог і заходів із забезпечення кіберзахисту та інформаційної безпеки в банківській системі України та для суб'єктів переказу коштів, контроль їх виконання; створення центру кіберзахисту Нацбанку, забезпечення функціонування системи кіберзахисту у банківській системі України тощо [39].

Надані суб'єктам забезпечення кібербезпеки повноваження прямо визначені у частині 5 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», зокрема зазначені суб'єкти в межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і

злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Здійснення конкретних заходів зумовлено саме компетенцією суб'єктів забезпечення кібербезпеки і залежить від їхніх завдань та повноважень.

Нами розглянута національна система забезпечення кібербезпеки. Їх аналіз звсвідчує, що при створенні такої системи звужено комплексний підхід до класифікації її складових. На наше переконання, таку систему суб'єктів слід розглядати у комплексному взаємозв'язку міжнародних і регіональних організацій, недержавних організацій, галузевих організацій, держави, приватного сектору та безпосередньо громадян. За такого комплексного підходу структура суб'єктів забезпечення кібербезпеки буде такою, як відображена у таблиці 2.1.

Таблиця 2. Суб'єкти забезпечення кібербезпеки

Категорія суб'єкта	**Представники**
Міжнародні й регіональні організації	Робоча група з телекомунікацій та інформації Азіатсько-Тихоокеанського економічного співробітництва – АТЕС (APEC-TEL); Європейське агентство мережевої та інформаційної безпеки – ЄМІАБ (ENISA); Об'єднаний центр передових методів кібернетичної оборони НАТО – ОЦПМКО (CCDCOE); Асоціація країн Південно-Східної Азії – АСЕАН

	(ASEAN); Організація економічного співробітництва та розвитку – ОЕСР (OECD); Група оперативного реагування на надзвичайні ситуації в комп'ютерних мережах OAS – КГРНС (CSIRT); Форум з управління Інтернетом – ФУІ (IGF); Міжнародна спілка електрозв'язку – МСЕ (ITU); Товариство Інтернету – ТІ (ISOC); Інтернет-корпорація з присвоєння імен і номерів (ICANN); Громадянська ініціатива Інтернет-політики «Меридіан» - ГІІП (CIIP Meridian); Ліонська група Великої вісімки, Підгрупа зі злочинності у сфері високих технологій; Організація Об'єднаних Націй; Рада Європи.
Недержавні організації	Правозахисні структури: Міжнародна правозахисна організація «Human Rights Watch»; «Міжнародна амністія» - МА (IA); «Репортери без кордонів» - РБК (RWB), Американський союз захисту громадянських свобод та ін.; фонди: «World Wide Web», «Shadowserver» тощо; аналітичні центри: Центр стратегічних і міжнародних досліджень – ЦСМД (CSIS), Американський центр стратегічних досліджень (RAND) та ін.
Галузеві організації	Дослідницько-аналітичний центр з питань функціонування служби доменних імен – ДАЦСДІ (DNS-OARC); Антифішингова робоча група (APWG); Робоча група з боротьби зі зловживаннями в системах передання повідомлень (MAAWG); Галузевий консорціум зі зміцнення безпеки в Інтернеті (ICASI); Науково-технічна рада з питань захисту інформації та науково-дослідницька група зі шкідливих кодів при Науковій раді з питань інформаційної безпеки (ISTSG); Міжнародна комісія зі стандартів Інтернету (IETF); Інститут інженерів з електротехніки та електроніки (IEEE); структури у сфері транспорту (органи безпеки та управління повітряним рухом в аеропортах тощо); інші галузеві структури, що

	опікуються управлінням критичною інфраструктурою та її охороною.
Держави	Міністерства: внутрішніх справ, закордонних справ, юстиції, інфраструктурні (транспорту), фінансів та ін.; розвідувальні й інші спеціальні служби; управління національної поліції, зокрема їх спецпідрозділи з кібербезпеки та боротьби з організованою злочинністю; комп'ютерні групи екстреної готовності – КГЕГ (CERT); спеціалізовані управління з питань кібербезпеки; управління оперативної безпеки.
Приватний сектор	Спеціалізовані структури із забезпечення безпеки в Інтернеті; розробники програмного забезпечення, виробники обладнання; кредитно-банківські структури, зокрема системи банківських електронних платежів; сервери електронної пошти; хостинг-провайдери; структури Інтернет-торгівлі тощо.
Фізичні особи	Власники й користувачі ПЕОМ.

Виходячи з цього, національна концепція кібербезпеки має охоплювати й об'єднувати три рівні її забезпечення, а саме: *держава – бізнес – окремі громадяни (користувачі)*. Пріоритетними в цьому сенсі для України, беручи до уваги найімовірніші потенційні цілі кібератак, убачаються такі напрями:

- захист об'єктів критичної інфраструктури, державних і приватних інформаційних систем і мереж;

- створення дійових механізмів міжрівневих комунікацій;

- підвищення поінформованості на всіх рівнях;

- забезпечення ефективного контролю за якістю обладнання, що використовується.

Слід зазначити, що однією з головних практичних безпекових проблем є визначення конкретного джерела кібератаки. Хоча, як зазначалося вище під час аналізу загроз, ми можемо доволі чітко розмежувати відповідних суб'єктів,

їхню мету й техніко-технологічні потенції. Достеменно з’ясувати відмінності між діями держав, «звичайних» злочинців і терористів чкладно через високу швидкість операцій, які проводяться в Інтернеті, можливість збереження при цьому анонімності та знищення слідів незаконного використання інформаційно-комунікативних технологій. У цьому контексті забезпечення інформаційної безпеки неабияку роль має відіграти широке міжнародне співробітництво.

Як зазначає В. Бурячок, «досвід іноземних країн та особливості українських реалій свідчать, що розв’язання основних завдань кібербезпеки неможливе без створення: міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки; центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам протиборчих сторін та впливу на їх інформаційно-телекомунікаційні системи; органів власної інформаційної і кібербезпеки – державних установ (відомств) та комерційних структур, які повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної політики щодо захисту як власного, так і спільного національного інформаційного і кіберпросторів» [149, с. 8-9].

Необхідно зазначити, що координаційні структури, які об’єднують та спрямовують діяльність суб’єктів забезпечення кібербезпеки, наразі створені та успішно працюють уже в багатьох країнах. Так, у 2017 року в Таллінні був створений Об'єднаний центр передових технологій з кібероборони НАТО. Центр отримав акредитацію НАТО, налічує 20 учасників - 17 членів НАТО і три країни-партнера. Основне завдання Центру - тренування фахівців з різних країн, які забезпечують безпеку в національному кіберпросторі. У Литві Міністерству оборони надано право координувати національну політику з

кібербезпеки, передбачається створення Національного центру кібербезпеки, Консультативної ради з кібербезпеки при Міністерстві оборони. У Чехії у 2017 році створено Національний офіс з кібербезпеки та інформації, до функцій якого входять вирішення проблем кібербезпеки, підтримка державних установ і підприємств у разі кібератак, профілактика злочинів у кіберпросторі, забезпечення безпеки інформаційної інфраструктури [150, с. 107].

На нашу думку, неможливо забезпечити достатній рівень кібернетичної безпеки людини, суспільства, держави, за відсутності ефективної співпраці всіх суб'єктів її забезпечення: правоохоронних органів, постачальників послуг та самих користувачів. У нашій державі тривалий час правоохоронні органи використовувалися для усунення конкурентів, отримання неправомірного вигоди на кшталт інформації з обмеженим доступом, яка має комерційну цінність, збирання компрометувальної інформації про особу тощо. Немає гарантії, що сьогодні такі випадки вже неможливі. За цих умов не варто чекати на те, що ефективними будуть саморегуляторні механізми (хоч б такі, як «гарячі лінії» для скарг на інциденти у кібернетичній сфері) і подальша співпраця між постачальниками послуг та правоохоронцями.

Завдяки належним розслідуванням у правоохоронних органах, за допомогою яких винні будуть притягнені до юридичної відповідальності, можна сприяти вирішенню цього проблемного питання. Водночас уже реалізовано перші спроби саморегуляції, коли постачальники послуг консолідували зусилля у протидії викрадачам телекомунікаційного устаткування, а також комерційних секретів. За умови, що цей проєкт буде вдалий, на його основі може постати справжній мультистейкголдеризм, без якого неможливо буде забезпечити кібербезпеку на системному рівні. Надважливо, щоб його також відповідно підтримали правоохоронні органи. У цьому визначальний зміст основи державної політики в досліджуваній нами сфері.

Так само важливо створити відповідні умови для того, щоб розвивалася індустрія кібернетичної безпеки – як у фінансовій (забезпечення пільгами,

прозорими тендерами на отримання бюджетного фінансового забезпечення, розвиток технопарків, співпраця закладів вищої освіти та приватного IT-сектору тощо) та організаційній площині (прозорі та зрозумілі правила, які диктує цей ринок). Корисний крок у цьому напрямі – гравцям ринку та державним установам, що опікуються цими питаннями, укласти відповідні меморандуми. Прикладом такого роду співпраці може слугувати підписаний Службою безпеки України з приватним акціонерним товариством «Укргідроенерго» та національною енергетичною компанією «Укренерго» Меморандум щодо протидії кіберзагрозам і розвитку ефективної системи кібербезпеки держави. Документ має забезпечити обмін інформацією з СБУ щодо кібернетичних загроз із використанням платформи MISP-UA зі стратегічно важливими підприємствами енергетичної галузі України. Обмін матеріалами, зокрема технологічною інформацією про реалізовані та потенційні кіберзагрози, відбуватиметься в режимі реального часу. Така міжвідомча взаємодія сприятиме ефективному реагуванню з боку української спецслужби на кібернетичні атаки, насамперед високого ступеня складності [151].

Варто зазначити, що співробітники Ситуаційного центру забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform) створили систему збору і обробки інформації щодо інцидентів кібербезпеки та обміну технічними даними про ідентифікатори компрометації інформаційних систем об’єктів критичної інфраструктури між суб’єктами сектору безпеки в режимі реального часу. Ця платформа широко використовується в усьому світі, а також відповідає міжнародним стандартам ЄС і НАТО та застосовується основними міжнародними суб’єктами у сфері кібербезпеки FIRST, CIRCL, CiviCERT, NATO NCI Agency [152].

Як бачимо, важливість людей, процесів та технологій для підтримки кібернетичної безпеки є однаковою. Рівень ефективності навіть найкращих технологій виявиться незадовільним у разі їхнього неправильного

застосування. Вкрай необхідно покращити обізнаність, просвіту та навчання згідно з чітко визначеними пріоритетами кібербезпеки, принципами, політикою, процесами, програмами, щоб забезпечити достатній рівень кібернетичного захисту, і їм варто приділяти особливу увагу у кожній сфері – політичній, законодавчій, регуляторній, бізнесовій, волонтерській. Із найкращих світових практик бачимо, що культури використання Інтернету, інформаційної гігієни треба навчати ще в межах дошкільної освіти.

Проте, окрім роботи з дітьми, мають здійснюватися й інші кроки. Слід забезпечити розробку окремих навчальних та інформаційних програм, якими могли б послуговуватися держслужбовці, правоохоронні органи, підприємці, громадські організації, індивідуальні користувачі. Окрему увагу слід приділити літнім людям.

Досить слушною є думка вітчизняних дослідників О. Довганя та І. Дороніна про те, що «поки не будуть сформовані суб'єкти, які безпосередньо займатимуться оперативним реагуванням на кіберінциденти, поки в цих суб'єктів не буде належної технічної бази та висококваліфікованих спеціалістів, що в свою чергу потребує належного фінансування, – всі заявлені в законопроекті положення так і залишаться на папері. Тепер справа за урядом, суб'єктами забезпечення кібербезпеки, які мають розробити вимоги до захисту критичних інфраструктур, нові стандарти і методики та забезпечити контроль за ефективністю кіберзахисту» [54, с. 26].

Ризик кіберзагроз наразі є актуальним для значної кількості суб'єктів: від приватних осіб до великих компаній, окремих галузей економіки та держав в цілому. На національному та міжнародному рівнях є усвідомлення того, що проблеми кібербезпеки можуть завдати шкоди національній безпеці та дієвому функціонуваннюя економіки держави. Тому ефективна організація системи суб'єктів забезпечення кібербезпеки набуває в сучасному світі непересічного значення. Вдосконаленню її діяльності мають сприяти розмежування компетенції державних органів, які є суб'єктами забезпечення кібербезпеки, та розвиток державно-приватного партнерства.

У 2017 році Президент України підписав Указ «Про Національний координаційний центр кібербезпеки», яким затверджено Положення про вказаний центр. До його основних завдань належить «аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо». Відповідно до Указу Президента України № 27/2020 [153] штат апарату РНБО розширено до 190 співробітників для забезпечення інформаційно-аналітичного, експертного, організаційного, матеріально-технічного забезпечення Центру, а також розширено повноваження Центру, який координує й контролює роботу суб'єктів сектору безпеки і оборони у сфері кібербезпеки.

Втім слід зауважити, що відповідні законодавчі новації, особливо в контексті змісту внесеного Президентом України законопроєкту № 3196 [154], зумовлюють ризик взаємного дублювання повноважень Центру кібербезпеки, СБ України та ДСС України. Тож це питання підлягає врегулюванню в ході подальшого вдосконалення системи суб'єктів забезпечення кібербезпеки. Так само потребують вдосконалення та розвитку питання державно-приватного партнерства у сфері кібербезпеки.

Загалом, важко говорити про ефективність національної системи суб'єктів забезпечення кібербезпеки. Функціонування національної системи кібербезпеки обмежується здебільшого тим, що до неї долучаються силові структури (Національна поліція, Служба безпеки України, Держспецзв'язок та ін.). Важливі питання майже завжди вирішуються без участі приватного бізнесу, та кіберспільноти й ІТ-сектору.

Немає також трансформаційного підходу до керування системою

національної кібербезпеки, який передбачає організацію, що впроваджувала б програму з кібернетичної безпеки, а також регулярний контроль за тим, як вона впроваджується.

Крім того, у зв'язку з особливостями деяких сегментів (охорони здоров'я, енергетики, телекомунікацій тощо) є нагальна необхідність створити окремі галузеві стандарти з кібернетичного захисту.

Ще одна значна проблема полягає в недостатній ефективності вітчизняної системи кібернетичної розвідки (Threat Intelligence). Існують приклади, коли від приватних організацій та волонтерських угрупувань держава отримує попередження про заплановані атаки. Проте, зважаючи на існуючі загрози, цього замало. У контексті обговорення кібернетичної безпеки представники влади висловлюють думку про неможливість розділення державної безпеки та «бізнесової». Бо, коли ми розглядаємо проблему кібернетичної безпеки, йдеться не лише про приватний сектор, а про державну безпеку [155] взагалі. Ми підтримуємо використання такого підходу. З огляду на це важливо розробити оптимальні механізми співробітництва між приватним сектором та державними органами, щоб належно забезпечувати кібербезпеку.

Окремою проблемною ділянкою є аудит кібернетичної безпеки. У межах системи координат НД ТЗІ, документ, що дозволяє проводити аудит, є тільки в акредитованих державних організацій. Сертифікати з інформаційної та кібербезпеки й ІТ-аудиту міжнародного зразка зараз не визнають, що негативно відбивається на якості аудиту.

Основною ідеєю реформи є перехід із моделі державного контролю за кібербезпекою, зокрема і в приватних структурах, на саморегуляцію, завдяки якій приватні користувачі та суб'єкти господарювання отримають можливість самостійного визначення і контролю з впровадженням стандартів кібернетичної безпеки в певних галузях.

Необхідно переосмислити, яке значення має держава для розбудови державної системи кібернетичного захисту, її роль та межі впливу. Очевидним

є те, що воно має полягати не у функції контролю (як сьогодні), а швидше фасилітації і сприяння вирішенню проблематики кібернетичної безпеки.

Першочерговим кроком має стати заміна НД ТЗІ на ефективніший і сучасніший базовий стандарт і запровадження галузевих стандартів кібернетичної безпеки. На цьому напрямі слід керуватися тими міжнародними стандартами, які вже були випробувані й визнані провідними країнами, особливо тими, які є нашими стратегічними партнерами.

Зокрема, досить дієвим з погляду практики його втілення, є розроблений у США NIST Cybersecurity Framework [156], яким, крім Сполучених Штатів, користуються японський та ізраїльський уряди. До того ж організації можуть обирати та запроваджувати NIST, ISO, Cobit та ін.

Вирішення питань, пов’язаних з регулюванням та контролем, можна покласти на галузеві регулятори або саморегулюючі організації. Прикладом останніх є NERC CIP у Сполучених Штатах, якими були розроблені галузеві стандарти з кібернетичної безпеки в енергетичному секторі.

Іншим позитивним прикладом галузевого регулювання, який варто було б розглядати з погляду можливого запровадження в Україні, є Health Insurance Portability and Accountability Act [157] (HIPAA) із підтримки безпеки, медичної інформації на електронних носіях у галузі охорони здоров’я або Ofcom для телекомунікаційної сфери та низку інших.

Беззаперечною та досить очевидною є ситуація, за якої сучасні кіберзлочини стають усе складнішими. Попри поширену думку, безпека є не станом, а є процесом. Окрім цього, покладатися винятково на фактор захисту зараз замало. З метою мінімізації збитків, завданих кібератаками, варто зосереджуватися не тільки на захисті, але й на правильному реагуванні на інциденти, наявності можливостей створювати такі загрози для противника в процесі інформаційного протиборства.

Підсумовуючи зазначене вище, слід наголосити на необхідності налагодження ефективної та дієвої системи обміну даними щодо кіберінцидентів та запровадження співпраці держави, приватних компаній та

дослідників на постійній основі, які повинні здійснювати свою діяльність не на засадах волонтерства, як зараз, а за встановленими правилами та чітко визначеними механізмами.

Якщо створити галузеві центри з реагування на кібернетичні інциденти (SOC) та центри інформаційного обміну про кібернетичні атаки (ISAC), з'явиться можливість вирішити цю проблему системно.

Ще один важливий висновок, за результатами проведеного аналізу, на якому варто зосередити увагу, необхідність створення незалежних платформ для співпраці – кіберцентрів, з метою ефективної протидії кібернетичним загрозам. Вони є інтеграційними платформами для кібергравців світового та національного рівня, де вони обмінюються своїми надбаннями в такій галузі як кібербезпека. Результатом таких інновацій в Україні буде змога оперативного реагування на кіберзагрози.

Подібна практика в інших країнах продемонструвала свою дієвість та результативність. Зокрема, кіберцентр на території Пітсбурга (США) функціонує вже більше 18 років [158]. У межах його діяльності правоохоронці, представники інститутів держави, IT-підприємств, освітніх установ об'єднують свої зусилля для того, щоб досягати цілей кіберзахисту. Такі центри працюють у численних передових країнах. У нашій державі немає ще ні одного.

Разом із тим, локальним SOC-и та ISAC-и варто напрацювати тісні зв'язки з подібними організаціями у міжнародному просторі. Обов'язково також варто залучити професійну спільноту.

Щоб оцінити наскільки захищеними є інформаційні системи, вбачається доцільним запровадження аудиту на предмет відповідності міжнародним стандартам. Аудити мають проводитися на регулярній основі, залучаючи незалежних (бажано, зовнішніх) фахівців, які мають міжнародні сертифікати.

Особливої уваги потребує розвиток bug bounty-програм, які мають стати дієвим механізмом, що виявляє вразливі місця інформаційних систем. Його зміст полягає в тому, що кожен може виявити недолік у системі компанії та

поінформувати про це власників, за що буде певним чином винагороджений.

В Україні така практика поки не так затребувана. А державні установи, підприємства та організації не поспішають впроваджувати такі програми ще й у зв'язку з тим, що немає відповідної нормативної бази та фінансування.

Важливий крок має полягати й тому, щоб створити експертну раду, яка б займалася питаннями кібернетичної безпеки за участі підприємців, професійних спільнот та держорганів. В обов'язки такої ради мають входити підготовка пропозицій до нормативно-правових актів цієї галузі, надання рекомендацій щодо функціонування державної системи кібернетичної безпеки та вирішення інших завдань і проблем, яким потрібна належна експертиза. Приклад ефективності функціонування такої організації – Національна Рада кібернетичної безпеки Нідерландів.

2.4 Актуальні питання протидії кіберзагрозам у сучасному кіберпросторі

Як і будь-яке досягнення науково-технічного прогресу, розвиток кіберпростору має як переваги, так і недоліки. До переваг можуть бути віднесені оперативність та розмаїття інформаційної взаємодії для ефективності розвитку всіх сфер людської діяльності, розширення можливостей використання всього обсягу накопичених людством знань, тоді як до недоліків - розширення можливостей несанкціонованого доступу з будь-якої точки до будь-якої іншої точки кіберпростору, зокрема й з протиправними намірами (саме такі можливості і розглядаються як загрози порушення нормального режиму функціонування кіберпростору, тобто кіберзагрози). Динамічний розвиток світового кіберпростору істотно підвищує небезпеку реалізації кіберзагрози, актуалізуючи значну кількість проблем забезпечення

кібербезпеки на глобальному та національному рівнях.

Сьогодні практично всі розвинені країни наразі розробили національні стратегії кібербезпеки, за якими здійснюватимуть захист своєї частини світового кіберпростору і участі в світовій кооперації вирішення виникаючих проблем. Розроблено та затверджено Міжнародний Стандарт ISO | IEC 27032-2012 «Інформаційні технології - технології безпеки - вимоги для кібербезпеки» [159], відповідно до якого поняття «кібербезпека» розглядається як узагальнювальне та включає в себе питання забезпечення безпеки систем, комунікацій і об'єктів, що входять до складу кіберпростору (інформаційної безпеки, безпеки мережевих структур, безпеки Інтернету, захисту критичної інформаційної інфраструктури тощо). До найважливіших положень Стандарту, на які мають орієнтуватися національні стратегії, належать міжнародне співробітництво в реалізації спільних рішень, а також тісний контакт суспільства, держави та бізнесу в забезпеченні кібербезпеки.

Визначення актуальних питань протидії кіберзагрозам передбачає виділення критичних сфер національного кіберпростору, які вимагають захисту, та їхньої специфіки. До таких критичних сфер мають бути віднесені: інформаційна безпека, яку слід розглядати у широкому значенні; безпека інформаційно-телекомунікаційного середовища, яка передбачає забезпечення безпеки всіх каналів і спеціальних систем зв’язку, що реалізують інформаційні взаємозв’язку будь-яких автоматизованих систем (систем органів державної влади, оборони, правопорядку, соціальної сфери, органів місцевого самоврядування, виробництва і технологічних процесів, корпоративних, громадських тощо) між собою і з зовнішнім світом; безпека автоматизованих систем управління і інформаційного забезпечення життєво важливих елементів національної інфраструктури.

У контексті загроз у кіберпросторі однією з основних проблем убачається здебільшого приватна належність інформаційно-комунікаційних мереж, тоді як на державу покладається значна частина відповідальності за їхню безпеку. При цьому інтереси вказаних суб’єктів зазвичай різняться, що,

звісно, не сприяє організації належного захисту інформаційної сфери з одночасним забезпеченням дотримання основних прав і свобод людини. Ситуація ускладнюється через глобальність як самої проблеми, так і методів та засобів її розв'язання.

На нашу думку, вагоме слово стосовно розробки міжнародно-правових норм щодо функціонування й захисту інформаційної сфери мають сказати міжнародні структури, створені для боротьби з кібернетичною злочинністю. З-поміж таких структур можна назвати, зокрема, Підгрупу Великої вісімки з питань високотехнологічної (кібернетичної) злочинності, Конгрес ООН з питань профілактики злочинності та кримінального судочинства, Конференцію Ради Європи з питань співробітництва у сфері боротьби з кіберзлочинністю та ін. Вони здатні виступити координаторами оптимізації національних законодавств у частині регулювання питань притягнення до відповідальності (зокрема й кримінальної) за правопорушення у цій сфері, ведення слідчих дій та інших процесуальних моментів, гарантування недоторканності приватного життя та збереження особистих даних, забезпечення мережевої безпеки, адекватного реагування на кібератаки тощо. Убачається, що ці міжнародні структури можуть також посприяти виявленню прогалин у системі нагляду, формуванню дійових методів суспільного контролю над діяльністю суб'єктів боротьби з кібернетичними правопорушеннями.

Особливої уваги це питання потребує тому, що вказані міжнародні структури при розробці заходів протидії кіберзлочинності питання контролю відсувають на задній план, зосереджуючись переважно на дієвості. А тим часом значні відмінності окремих національних законодавств, розрив у ресурсних і технічних потенціях різних країн ще більше актуалізують проблематику контролю й нагляду.

Приміром, величезні кошти у програми боротьби з кібернетичною злочинністю та вдосконалення відповідного законодавства вкладають уряди Великої Британії та США, тоді як чимало країн не мають не те що стратегій

забезпечення кібербезпеки та боротьби з різновекторними кіберзагрозами, а навіть базової інформаційної інфраструктури.

Брак технічних можливостей для ефективної боротьби з кібернетичними правопорушеннями, посилений слабким правовим забезпеченням, практично унеможливлює їх розкриття і притягнення винних до відповідальності. Звідси випливає потреба розроблення нормативно-правової бази сфери кібербезпеки й боротьби з кіберзлочинністю, зокрема й дійового регулювання питань суспільного контролю. Крім того, відсутність спеціальних державних наглядових інституцій підвищує загрози порушення прав людини на недоторканність приватного життя, свободу думки, об'єднань тощо.

Серед чинних міжнародно-правових документів у цій сфері слід назвати резолюції Генасамблеї ООН «Боротьба із використанням інформаційних технологій зі злочинною метою» (від 4 грудня 2000 року 55/63 і від 19 грудня 2001 року № 56/121), а також ухвалені Всесвітньою конференцією «Співробітництво проти кіберзлочинності», що відбулася 1-2 квітня 2008 року у Страсбурзі, «Головні принципи спільної роботи правоохоронних органів та інтернет-провайдерів у сфері боротьби з кіберзлочинністю». З-поміж відповідних регіональних правових актів варто виокремити Рекомендацію Ради Європи «Про боротьбу з комп'ютерними злочинами» (№ R(89)9) та Європейську конвенцію «Про боротьбу з кіберзлочинністю». Цей документ зобов'язує учасників Ради Європи передбачити в національних законодавствах повноваження відповідних органів, а також процедури для провадження розслідувань, зокрема для збирання електронних доказів у кримінальних злочинах, які вчинюються за допомогою комп'ютерних технологій.

Боротьби з кіберзлочинністю безпосередньо стосуються деякі правові акти щодо захисту прав людини міжнародного й регіонального характеру. Це, наприклад: ухвалений Генасамблеєю ООН у 1966 році Міжнародний пакт про громадянські й політичні права, де, зокрема, йдеться про права на недоторканність приватного життя (ст. 17), на свободу висловлення думки

(ст. 19) та на свободу об'єднань (ст. 22); Європейська конвенція з прав людини, Американська конвенція з прав людини, Африканська хартія прав людини і народів та ін.

Захист електронних даних теж входить до функцій згаданих вище міжнародних і регіональних організацій. Так, положення щодо захисту прав на недоторканність приватного життя та свободу висловлення думки під час розміщення персональних даних в електронних мережах, електронного листування тощо містять ухвалені Генасамблеєю ООН «Принципи регулювання комп'ютеризованих баз персональних даних», прийнята Радою Європи Конвенція «Про захист фізичних осіб при автоматизованій обробці персональних даних» та ін.

Уряди багатьох країн у своїх стратегіях кібербезпеки приділяють особливу увагу інфраструктурі, тісно пов'язаній з питаннями безпеки. Для оцінювання масштабу проблеми кібербезпеки і можливих загроз важливо розуміти взаємозв'язок між кібербезпекою та критичною інфраструктурою. Критична інфраструктура складається як з матеріальних (наприклад, будівель і споруд), так і віртуальних елементів (наприклад, систем і даних). Кожна країна може мати своє розуміння терміна «найважливіший», проте зазвичай це поняття може включати в себе елементи інформаційно-комунікаційних технологій (включаючи електрозв'язок, енергетику, банківську справу, транспорт, суспільну охорону здоров'я, сільське господарство та продовольство, водопостачання, хімічну промисловість, судноплавство, а також найважливіші державні служби). Кожен з цих секторів економіки має свої власні матеріальні ресурси, наприклад будівлі банків, електростанції, поїзди, лікарні і урядові офіси. Разом із тим, усі ці найважливіші сектори національної економіки залежать від інформаційно-комунікаційних технологій. Тому загальносвітові тенденції використання інформаційно-комунікаційних технологій роблять критичну інфраструктуру всіх секторів більш вразливою для кібератак.

Зокрема, актуальним для України є питання кіберзахисту цивільних

ядерних об’єктів. Слід ураховувати, що для цивільних ядерних об’єктів не існує універсальних стандартних рішень з інтеграції інформаційних технологій. Кожна атомна електростанція, з її архітектурою та топологією є унікальним об’єктом, на якому реалізовані оригінальні рішення з такої інтеграції. Відповідно, у кожному випадку мережам та ІТ-системам такого об'єкта притаманний унікальний набір вразливостей кібербезпеки, що істотно обмежує можливості і практичний сенс застосування операторами цивільних ядерних об'єктів накопиченого досвіду і кращих іноземних практик. Існує проблема довіри до ІТ-постачальників і необхідність забезпечення цілісності ланцюжків поставок ІТ-продукції, більшість з яких - транснаціональні компанії. Відсутність конкурентоспроможних вітчизняних рішень на ринку змушує використовувати імпортні аналоги обладнання та програмного забезпечення. На цей час ІТ-інфраструктура України (і це стосується не лише цивільних ядерних об’єктів) залежна від іноземних виробників і розробників, активно впроваджуючи їхні вирішення (від бібліотек програмного забезпечення до апаратних платформ і систем управління). Фактично на кожній з ділянок ІТ-інфраструктури з високою часткою ймовірності використовуються закордонні рішення з «невідомою» начинкою. Рішенням цієї проблеми видається популярна в світі аутсорсингова модель виробництва, згідно з якою розробка і виведення на ринок затребуваних продуктів можливі лише за умови тісної кооперації з зарубіжними та вітчизняними компаніями [160]. Це дає можливість на етапі проєктування сформувати концепцію нового продукту, пред’являючи йому затребувані ринком сучасні вимоги та передати стороннім спеціалізованим виробникам види робіт, які не є профільними для підприємства.

Системний підхід до питань кібербезпеки на рівні держави включає в себе не тільки підвищення обізнаності щодо існування ризиків у кіберпросторі, створення національних структур, що займаються питаннями кібербезпеки, а й встановлення необхідних взаємин між різними групами учасників (держава, науково-дослідні інститути, розробники та виробники інфокомунікаційних

рішень, замовники і споживачі), зокрема й між галузями економіки, для розвитку аутсорсингових моделі виробництва. Тож складність внутрішньої ІТ-інфраструктури й інтенсивність потоків даних на об’єктах критичної інфраструктури потребують комплексного підходу до кібербезпеки, який принципово виходить за рамки тільки реагування на інциденти.

Слід зазначити, що кібератаки проти об’єктів критичної інфраструктури не підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинів і їх розслідування. Найвідомішим механізмом такого роду є Будапештська конвенція про боротьбу з комп'ютерними злочинами, прийнята Радою Європи в 2001 році і відкрита для підписання всіма країнами [161]. Схожа ситуація має місце щодо регіональних угод у сфері кібербезпеки, а також двосторонніх угод. Кіберінциденти на цивільних ядерних об’єктах та інших об’єктах критичної інфраструктури також не підпадають під дію юридично необов'язкових транскордонних механізмів співпраці, таких як альянс Міжнародного союзу електрозв’язку (МСЕ) і міжнародного державно-приватного партнерства ІМПАКТ або FIRST (міжнародний Форум взаємодії між центрами реагування на інциденти кібербезпеки) [162]. Крім того, наразі не вироблена міжнародна система стандартизації щодо специфічних ІТ-продуктів і сервісів, які поставляються операторам об’єктів критичної інфраструктури, немає загальних критеріїв і стандартів аудиту кібербезпеки на таких об’єктах.

Збільшення кількості користувачів інтернету і розширення послуг онлайн послуг (за даними Gemius, станом на червень 2019 року в Україні число користувачів Інтернету становило 24,8 млн осіб [163]) призвело до зростання кіберзлочинності, насамперед у фінансовій сфері. До найістотніших особливостей цього виду злочинів зазвичай відносять особливу складність їх розкриття та розслідування, надзвичайно високу їхню латентність, прозорість національних кордонів для злочинців і відсутність єдиної правової бази для боротьби з ними, нерідко особливо великий розмір збитку, високопрофесійний склад осіб, які вчиняють такі злочини.

Сьогодні активно оцифровується сфера внутрішньої безпеки: документи, що засвідчують особу, камери відеоспостереження, електронні запити у кримінальних справах, перехоплення повідомлень стільникового зв'язку, системи моніторингу та збирання інформації тощо. Все це не тільки актуалізує проблему захисту персональних даних, а й уможливлює використання ІТ-комунікацій в організації громадських протестів або терористичних актів, а також управлінні можливими конфліктами. Саме тому суспільство потребує твердих гарантій стійкості до кібератак та інших критичних ситуацій, незалежно від того, чи спрямовані такі атаки проти державних органів, комерційних підприємств або фізичних осіб.

Активне використання кіберпростору впливає і на людську особистість, зумовлюючи, окрім залежності від Інтернету, також інші проблеми, зокрема, використання зловмисниками методів соціальної інженерії та вразливостей, пов'язаних із використанням Інтернету речей.

Можливості Інтернету речей (IoT) дозволять віддалено керувати автомобілями, персональними медичними системами або змусити «розумний» холодильник здійснювати покупки, які не входили в плани власника. Мобільний банкінг двє можливість претворити будь-який гаджет в пристрій з функцією оплати. Однак, ототожнюючи фінансові відносини з ІТ-технологіями, не варто забувати і про поширення розкрадань грошових коштів, збої в роботі систем електронного банкінгу і, як наслідок, зростання операційних і репутаційних ризиків кредитно-фінансових організацій [164, с. 64]. Наразі найбільший потенціал підвищення безпеки систем електронного банкінгу за допомогою ІТ вбачається у використанні біометричних данниях (відбитки пальців або системи розпізнавання зовнішності) для посвідчення особи користувача.

Головна небезпека IoT полягає в тому, що ІТ-системи створюють нові точки доступу для зловмисників, які оперують у кіберпросторі – хакерів, кракерів тощо. Так, точкою входу до системи може стати мережевий принтер, який надає хакерам маршрут доступу до комп'ютерів у мережі фінансової

організації, або мобільний пристрій, який має доступ до системи радіозв'язку високотехнологічного автомобілю тощо [165]. При цьому кіберзлочинці йдуть завжди на крок попереду, вони нападають раптово й можуть використовувати нешаблонні способи атак, до яких неготові не лише пересічні користувачі «розумної техніки», але й служби безпеки та правоохоронці. У зв'язку з цим розробники та виробники засобів захисту змушені шукати нові рішення в умовах жорсткого ліміту часу, оскільки найбільша шкода виходить саме від так званих атак «нульового дня» (коли засобів протидії «інноваційним» атакам у кіберпросторі ще не винайдено). У деяких випадках захищатися взагалі доводиться від того, про що є вкрай поверхове уявлення: немає даних про кількість подібних атак, про способи, за допомогою яких безпосередньо здійснюється «вірусна інвазія» до програмного забезпечення, про алгоритмах дій зловмисників у певних ситуаціях тощо [166].

Ці та низка інших важливих проблем кібербезпеки IoT стали підставою для випуску Технічним комітетом Європейського інституту телекомунікаційних стандартів (ETSI) з кібербезпеки стандарту кібербезпеки в Інтернет речей TS 103 645 [167].

Документ встановлює базовий рівень безпеки для споживчих товарів, підключених до Інтернету, і закладає основу для майбутніх схем сертифікації IoT.

Згаданий стандарт, у частині захисту персональних даних, крім іншого, передбачає:

Положення 4.8-1. Виробники пристроїв і постачальники послуг зобов'язані надавати споживачам чітку і прозору інформацію про те, як, ким і з якою метою використовуються їхні персональні дані. Це також відноситься до третіх сторін, які можуть бути залучені, включаючи рекламодавців.

Положення 4.8-2. Якщо особисті дані обробляються на основі згоди споживачів, ця згода має бути отримана належним чином.

Положення 4.8-3. Споживачам, які дали згоду на обробку своїх персональних даних, повинна бути надана можливість відкликати згоду в

будь-який час.

Минулого року Каліфорнія стала першим штатом США, де був прийнятий закон про кібербезпеку щодо IP-пристроїв (Закон № SB-327). Цей нормативно-правовий акт набрав чинності у 2020 р. «У законі викладені вимоги до виробників пристроїв, які напряму чи опосередковано підключаються до інтернету. Такі пристрої повинні передбачати «розумні» функції безпеки для запобігання несанкціонованому доступу, знищенню, зміні чи крадіжці інформації. Положення закону спрямовані на захист звичайних користувачів. Законодавчі ініціативи щодо більш масштабних корпоративних рішень ще попереду».

Уряд Великобританії у 2019 році випустив Звід практичних правил для забезпечення безпеки IP. У цьому нормативному акті акцентується на тому, що потрібно забезпечити кібербезпеку пристроїв, а не працювати над оновленням програмного забезпечення для посилення безпеки.

У цьому контексті загострюється ще одна глобальна загроза – застосування штучного інтелекту виробниками зброї.

У звіті міжнародної громадської організації PAX зазначено, що щонайменше 30 світових виробників зброї займаються розробкою подібних систем озброєнь, і, як виявилося, вони роблять це набагато швидше, ніж політики домовляються про регулювання цього питання. Серед розробників американські оборонні фірми Lockheed Martin, Boeing і Raytheon, китайські державні конгломерати AVIC і CASC, ізраїльські фірми IAI, Elbit і Rafael, Ростех Росії і турецька STM [168].

Велике занепокоєння у противників роботів-убивць викликає розгортання штучного інтелекту в наступальних системах, які будуть вибирати й атакувати цілі самостійно, без людського контролю. Досі незрозуміло, як ця зброя буде відрізняти комбатантів від цивільного населення або оцінювати пропорційність удару у відповідь. Юридичні експерти також не знають, хто буде нести відповідальність, якщо така автоматична зброя порушить міжнародне право. Без контролю людини ця зброя могла б

полегшити розв’язання війни, зробивши її механічно жорстокою. У результаті застосування роботів-убивць порушить основні правові та етичні принципи і дестабілізує міжнародний мир і безпеку, як зазаначає автор звіту Р. Слайпер.

Окрім указаного вище, особливо актуально знову постає проблема «іноземної залежності». Як пересічні громадяни, так і оператори об’єктів критичної інфраструктури, державні органи й електронний уряд користуються іноземними операційними системами та антивірусними продуктами, що не сприяє забезпеченню кібербезпеки. У країні також використовується імпортне мережеве обладнання, яке може обслуговуватись зарубіжними розробниками дистанційно, а відтак - у «потрібний» момент виведено з ладу.

Крім того, існують і інші фундаментальні проблеми, що виникають унаслідок розвитку інформаційно-комунікаційних технологій та Інтернету речей [169]. Так, психологи попереджають про загрози інтелектуальної деградації особистості через надмірно тривале перебування в мережі, ігроманії, манії переслідування, острах втратити свой комунікатор, порушення пам’яті (здатності запам’ятовувати числа та факти), виснаження інтуїції, що загалом може привести до ослаблення інтелектуального потенціалу людини [170]. До того ж постійне використання зовнішніх пристроїв знижує рівень щастя (умовне значення міжнародного індексу щастя, Happy Planet Index) населення. Інтернет-залежність сприяє також імплементації населенню сторонніх культурних кодів, нав’язуванню вигідної іноземним державам світоглядної картини [171].

Відтак розвиток заходів щодо зміцнення кібербезпеки має здійснюватися на відмінній від інших держав базі, а в ідеалі слід формувати власну програмну платформу. Крім того, слід розробляти свої криптографічні програми. Зокрема, партнерські відносини з вітчизняними розробниками ІТ-технологій, криптографічних засобів захисту тощо дають державі не лише безпосередньо технології, знання, фахівців, але й можливість прийняття своїх, контрольованих рішень. Відповідно, в усіх розвинених країнах існують компанії з розробки антивірусів та інших рішень у сфері кібербезпеки.

Цілком зрозуміло, що без участі пересічних користувачів мережі боротьба з кіберзлочинністю навряд чи буде достатньо ефективною. Тому, вбачається необхідним залучати їх до заходів із роз'яснення прав користувачів всесвітньої мережі Інтернет, етичних аспектів її функціонування, варіантів і механізмів комп'ютерних шахрайств, викрадення особистих реквізитів та інших інтернет-злочинів.

Таблиця 2.2. Джерела кібернетичних загроз [172-174]

Критерій класифікації	**Зміст загрози**
Загрози існуванню нації	Спеціальні (розвідувальні) служби держави застосовують для збирання відкритої інформації та шпигунства стосовно інших країн (не тільки ворожих, а й союзних) або недержавних суб'єктів кібернетичних атак комп'ютерні технології. Проти ворожих країн (суб'єктів) з метою дезінформації, залякування, дестабілізації, аж до кібернетичної війни, можуть здійснюватися кібератаки. Можуть здійснюватися перехоплення персональних даних та їх використання. Подекуди це відбувається без передбаченого законом санкціонування та належного демократичного контролю, що порушує права людини. Приватні корпорації чи підприємства займаються промисловим шпигунством, диверсіями тощо, нерідко залучаючи для цього хакерів, організовані злочинні угруповання тощо). Як і в разі державних спецслужб, корпорації, збираючи, аналізуючи й використовуючи значні обсяги персональних даних, обмінюючись ними з іншими суб'єктами (як приватними, так і державними), можуть порушувати права людини.

За деструктивним впливом на основні сегменти національного кіберпростору:	
Хакери	У теперішній час хакерство, яке розпочиналось зі зламування комп'ютерних мереж для професійного вихваляння або ж із хуліганською метою, все більше набуває кримінального характеру. Усе більш витонченими й доступними стають засоби для здійснення кібератак, інструкції щодо застосування яких не важко знайти в Інтернеті. Тому сьогодні для проникнення у віддалені мережі вже не треба мати, як раніше, глибокі знання й віртуозне володіння комп'ютерними технологіями.
Хактивісти	Хактивізм (англ. *hack* – прорубуватися, проникати та *acktivism* – активність, діяльнісність*)* – соціальне явище, соціальний протестний рух за допомогою хакерства – незаконного проникнення у певні веб-сайти чи поштові сервери з метою їх пошкодження, викривлення, спотворення чи руйнації для досягнення певних політичних цілей.
Кібер-диверсанти із невдоволених користувачів	Цей контингент являє собою неабияку загрозу, позаяк це зазвичай люди, котрі непогано обізнані з принципами функціонування мережі й можуть скористатися цим для пошкодження системи, викрадення конфіденційної інформації чи з іншою протиправною метою. Як з'ясували фахівці ФБР США, ймовірність організації кібернетичних атак користувачами системи вдвічі вища ніж зовнішніми суб'єктами.
Терористи	З метою досягнення своєї мети терористи намагаються спричинити масові людські жертви, вивести з ладу чи знищити об'єкти критичної інфраструктури, створити

	загрози національній безпеці, дестабілізувати економіку, порушити моральний стан суспільства, підірвати авторитет державної влади тощо. У теперішній час ті терористичні угруповання, які ще не мають технічних можливостей і фахівців для проведення кібератак, усе частіше звертаються до «послуг» організованих злочинних структур або ж намагаються отримати відповідні знання та фахівців, що сьогодні цілком реально.
Ботнет	Бот – програма у складі ботнету, яка приховано впроваджується у пристрій зловмисної зацікавленості й дає хакерові змогу, використовуючи ресурси комп'ютера жертви, провадити певні дії. Заражаючи такими програмами значну кількість пристроїв, хакери користуються ними для здійснення й координування кібератак, фішингу, перебору паролів на віддалених системах, розсилання спаму й інших шкідливих незаконних операцій. На рику нелегальної торгівлі широкий асортимент подібних «послуг» користується неабияким попитом.
Фішери	Фішинг (англ *phishing* – виуджування) – незаконний спосіб отримання персональної інформації – паролів, номерів банківських рахунків чи кредитних карт тощо шляхом розсилання від імені банку електронних листів з посиланнями на підроблені сайти, які імітують роботу справжніх, або створення точної копії існуючої банківської веб-сторінки, аби змусити користувача ввести свої особисті фінансові дані; використовуються також шпигунські й інші шкідливі програми, спами). Фішери – окремі особи чи групи, котрі використовують указаний вид інтернет-шахрайства у своїх протиправних

	цілях чи з метою перепродажу добутих даних.
Спамери	Спамери – це фізичні чи юридичні особи, котрі з метою реклами займаються розповсюдженням незатребуваної електронної пошти – спаму, який нерідко містить недостовірну або приховану інформацію. Розсиланням спаму може також приховуватися фішинг, поширення шпигунського чи шкідливого програмного забезпечення, кібератаки тощо.
Виробники шпигунського чи шкідливого ПЗ	До цієї категорії належать фізичні чи юридичні особи, котрі виробляють шпигунське чи шкідливе програмне забезпечення і шляхом його розповсюдження здійснюють кібератаки.
Педофіли	Можливості всесвітньої мережі – електронна пошта, спеціалізовані файлообмінні сервіси, піринговe програмне забезпечення, соціальні мережі, чати тощо – все частіше використовується педофілами з метою обміну дитячою порнографією та задля пошуку потенційних жертв і знайомства з ними.

Таблиця 2.3 Види кібернетичних загроз

Вид загрози/критерій	**Підвид загрози**	**Зміст та приклади**
Порушення цілісності даних	Пропаганда, дезінформація	Зміна (викривлення) даних чи впровадження хибних даних для впливу на суспільно-політичні процеси, результати економічної, бізнесової діяльності або ж із метою дестабілізації обстановки (правлячих режимів) в іноземній країні.
Для викривлення, спотворення, знищення		

даних чи порушення їхньої цілісності в інший спосіб можуть застосовуватися хакерські методики		
	Залякування	Кібератаки здійснюються з метою примусити приватних чи державних власників веб-сайтів змінити (видалити) їхній зміст або ж усю політику ресурсу.
	Знищення	Систематичне цілеспрямоване нищення певних даних іноземної держави чи конкурента. Зазвичай здійснюється в комплексі з іншими підривними заходами у процесі відповідних операцій.
Доступ Створення умов, коли законні користувачі не в змозі отримати доступ (або цей доступ ускладнений) до певних серверів (ресурсів), що їх надає система (атаки на відмову в обслуговуванні)	Зовнішня інформація	Подібні й інші атаки на державні та приватні ресурси відкритого доступу (інформаційні сайти державних структур, ЗМІ та ін.).
	Внутрішня інформація	Кібератаки на локальні мережі державних чи приватних структур – управління об’єктами критичної інфраструктури, транспорту,

		аварійно-рятувальних служб, кредитно-банківських установ, системи оперативного управління, корпоративні сервіси електронної пошти тощо
Конфіденційність даних Кібернетичні атаки зі злочинним умислом спрямовані на різноманітні джерела (ресурси) конфіденційної інформації юридичних та фізичних осіб	Шпигунство	Шпигунська діяльність держав щодо іноземних країн, фізичних та юридичних осіб; здобуття конкурентними суб'єктами інформації про своїх опонентів.
	Викрадення персональних даних	Фішинг та подібні кібератаки з метою у шахрайський спосіб з'ясувати персональні дані користувачів, зокрема номери їхніх банківських рахунків, а також упровадження вірусів для зняття даних із комп'ютера жертви тощо.
	«Крадіжка особистості» (викрадення персональних даних)	З метою викрадення персональних даних особи та використання їх для вчинення протизаконних дій застосовуються вірусні троянські й аналогічні програми.
	Пошук інформації в інтернеті	Технології пошуку інформації з відкритих джерел застосовуються з метою здобуття різноманітної інформації, зокрема персональних даних.
	Шахрайство	Цей злочин нерідко вчинюється за допомогою спаму, який розповсюджується через електронну пошту.

Шкідливі дії в кіберпросторі з погляду порушення властивостей інформації та інформаційних мереж вчиняються з метою:

– порушення конфіденційності шляхом несанкціонованого доступу до

наявних в інформаційній системі даних;

– порушення цілісності шляхом несанкціонованих змін чи модифікації інформаційних систем і даних, що в них зберігаються;

– порушення доступності шляхом зловмисного перешкоджання доступу до інформаційних систем і даних, що в них зберігаються.

За походженням можна виокремити природні й антропогенні (рукотворні) загрози. До перших належать загрози, пов'язані з явищами природи, стихійними катаклізмами – буревії, повені, пожежі, землетруси, цунамі тощо, а також загрози техногенні, пов'язані з технічними проблемами. Натомість антропогенні загрози випливають із дій людини стосовно інформації, комп'ютерних систем і мереж. Вони поділяються на неумисні й умисні. З-поміж останніх загроз можна виокремити адресні атаки, ціллю яких є певна інформаційна система або ж об'єкт критичної інфраструктури, а також безадресні атаки, котрі не мають конкретної цілі (приміром, розповсюдження шкідливих програм) [176-178].

Слід зауважити, що саме рукотворні загрози є головними викликами інформаційній безпеці, про що свідчить зростання й урізноманітнення методів і засобів зловмисних дій у кібернетичному просторі. Джерелом таких дій і відповідних загроз стають численні суб'єкти, котрі мають достатні знання й можливості для вчинення шкідливих дій в інформаційному середовищі.

Серед основних суб'єктів (джерел) кіберзагроз можна виокремити такі:

– держави, які використовують відповідні кіберзасоби для збирання інформації та розвідувальної діяльності (зокрема, економічне шпигунство задля отримання переваг в економічній, політичній, військовій та інших сферах); деякі держави вдаються до засобів інформаційної війни з метою обмеження противної сторони у прийнятті рішень, отримання стратегічних і тактичних переваг, руйнації окремих об'єктів (критичної інфраструктури, зокрема й пов'язаних з оборонною сферою);

– бізнесові структури: приватні компанії-конкуренти, котрі прагнуть здобути важливі дані щодо опонентів задля отримання ринкових переваг –

виробництво, ціни, розробки, асортимент тощо;

– кримінальні угруповання, котрі вдаються до кібернетичних атак з метою грошового зиску; засоби, що при цьому застосовуються, найрізноманітніші: фішинг, спам, шкідливі програми для інтернет-крадіжок, комп'ютерного вимагання, викрадення персональних даних тощо;

– міжнародне корпоративне шпигунство, метою якого є економічне, промислове шпигунство, викрадення значних коштів; нерідко користуються послугами хакерів, надаючи їм відповідні засоби;

– мережеві оператори, котрі використовують ботнет (мережу) дистанційно керованих зламаних систем задля розповсюдження спаму, фішингу, провадження узгоджених атак та ін.;

– розробники шкідливих програм і програм стеження – окремі особи чи організації, котрі створюють і застосовують указаний продукт із протиправною метою;

– розробники фішингових схем, котрі створюють і застосовують їх для викрадення коштів, персональних даних тощо;

– працівники підприємств (компаній, установ), які мають доступ до внутрішньої конфіденційної інформації (інсайдери), зокрема до комп'ютерних систем, а тому можуть викрадати дані або завдавати шкоди. До цих суб'єктів належать також некваліфіковані чи халатні співробітники, тимчасово наймані працівники, котрі можуть неумисно зашкодити системі через необережність;

– спамери, котрі використовують схеми фішингу, поширюють у мережі повідомлення, які містять приховані або хибні дані, а також шпигунські й вірусні програми, здійснюють кібератаки (приміром, «відмова в обслуговуванні» – DDoS);

– терористи, котрі ставлять за мету виведення з ладу чи руйнацію об'єктів критичної інфраструктури або ж втручання у їхнє функціонування, що може призвести до значних людських жертв, становить серйозну загрозу національній безпеці через підрив економіки країни, морально-психологічного стану суспільства. Ця категорія для отримання грошового

зиску та важливої інформації також використовує шпигунські й інші шкідливі програми, фішингу та ін.;

– хакери, котрі зламують закриті інформаційні системи й мережі з різних мотивів. Це може бути перевірка фахових здібностей, самоствердження, демонстрація певної громадянської позиції, отримання незаконного фінансового зиску;

– хактивісти, котрі з метою розміщення матеріалів політичного характеру атакують поштові сервери та веб-сторінки.

Усе наведене вище переконливо свідчить, що для забезпечення кібербезпеки необхідні здійснення комплексу заходів, скоординовані зусилля державних органів, бізнесових структур та окремих громадян. Особливо це стосується злагодженої взаємодії державного й приватного секторів, позаяк в останньому перебуває значна частина мереж і критичної інфраструктури. Неабиякого значення набуває підвищення загальної відповідальності за безпекову сферу, налагодження дійової міжрівневої взаємодії та ефективного зворотного зв’язку.

Узагальнення даних проведеного вище дослідження дає підстави сформувати загальну концепцію загроз кібернетичній безпеці, котра містить такі складові як інформаційні війни, кібернетичне шпигунство, кібертероризм, кібернетична злочинність. Є також змога зіставити вказані види загроз з їхніми головними суб’єктами, зазначивши переважну мотивацію зловмисного використання інформаційно-комунікативних технологій та основні об’єкти можливих кібератак (див. табл. 2.4).

Таблиця 2.4. Загрози кібербезпеці

Види загроз	**Суб’єкти загроз**	**Мотивація**	**Об’єкт атаки**
Інформаційна війна	Держави	- здобуття переваг в інформаційній сфері; - досягнення військово-	- інформаційні системи й мережі, пов’язані з військовою сферою;

		політичних переваг.	- системи управління та прийняття рішень; - системи й мережі, пов'язані з озброєнням; - об'єкти критичної інфраструктури.
Кібернетичне економічне шпигунство.	Держави	Досягнення політичних та (або) економічних, військових зисків.	Державні та (або) корпоративні, приватні інформаційні системи й мережі.
Кібернетичне шпигунство.	- політичні та (або) громадські діячі; - інсайдери.	- досягнення політичних та (або) ідеологічних зисків; - особиста вигода.	
Промислове та (або) економічне шпигунство.	- бізнесові конкуренти; - міжнародні корпоративні шпигуни.	Економічні вигоди.	
Кібернетична злочинність	- оператори ботнету; - інсайдери;	- матеріальний зиск (кошти); - самоствердже-	- державні та (або) корпоративні,

	- організовані угруповання; - спамери; - хакери; - хактивісти; - розробники шкідливих програм.	ня; - демонстрація громадянської позиції; - авторитет; - помста тощо.	приватні інформаційні системи й мережі; - об’єкти критичної інфраструктури.
Кібертероризм	- терористичні угруповання; - окремі терористи.	Соціально-політичні цілі.	- державні системи й мережі управління та прийняття рішень; - об’єкти критичної інфраструктури.

Розглянемо детальніше визначені види загроз.

Інформаційні війни. У теперішній час способи й засоби воєнних дій зазнали істотних змін, що зумовлено розвитком інформаційно-комунікативних технологій та їх активним впровадженням у військову сферу. Не менш активно розробляються воєнні доктрини й концепції, котрі неодмінно враховують чинники уразливості цих технологій.

Зазначимо, що поняття «інформаційна війна» почало входити в науковий обіг у США на початку 90-х років 20-го століття. Ще більше воно поширилося після «першої інформаційної війни», як інколи називають кампанію «Буря в пустелі» 1991 року. Коаліція застосувала тоді інформаційні технології і як специфічну зброю, і для проведення розвідувальних заходів, аналізу поточної ситуації й тилового забезпечення, координації воєнних операцій тощо. Це сприяло мінімізації людських, а також матеріальних втрат.

Кібернетичне шпигунство. Стрімка інформатизація життєдіяльності світової спільноти кардинально змінила підходи до феномена інформації – її створення, використання, циркуляції, зберігання. У теперішній час колосальні обсяги інформації переведені в цифрову форму й у ній зберігаються, а мережеві системи забезпечують доступ до неї. Загальна поширеність новітніх технологій і механізмів доступу до інформації зумовила те, що до кібернетичних засобів шпигунства з різних мотивів вдаються не лише держави, а й недержавні суб'єкти. Головною метою такого шпигунства є отримання доступу до державної таємниці, різної конфіденційної інформації економічного, комерційного характеру, інтелектуальної власності.

Економічне кібернетичне шпигунство. Можливості традиційних видів державного шпигунства для здобуття таємних даних (закритої інформації) щодо економічної, військової та інших важливих для національної безпеки сфер іноземної держави значно розширилися з розвитком інформаційно-комунікативних технологій. Слід зазначити, що економічна спрямованість таких шпигунських зазіхань останнім часом превалює.

Загроза несанкціонованого витоку таємної інформації. Загрози національній безпеці зростають не лише через державне економічне кібернетичне шпигунство, а й через відповідну діяльність інсайдерів, котрі, маючи доступ до важливих конфіденційних і секретних даних, виходячи з особистісних переконань чи меркантильних міркувань, передають цю інформацію представникам іноземних країн, хактивістам чи іншим зацікавленим суб'єктам.

Найяскравішим прикладом реалізації загрози з боку інсайдерів і хактивістів є надання американським військовиком Б. Меннінгом секретних даних, до яких він мав доступ, міжнародній некомерційній організації «Вікілікс», котра оприлюднила їх у 2010 році на своєму сайті. Публікація матеріалів дипломатичного листування США, великого масиву документів щодо воєнних дій в Афганістані й Іраку та багатьох інших завдала серйозного удару по іміджу американського уряду, їх дипломатів та спецслужб.

Кібернетична злочинність. Потужні потенції мережі Інтернет, інших інформаційних технологій не могли не привернути увагу як окремих осіб, так і організованих злочинців. Зумовлено це насамперед можливістю отримання величезних незаконних баришів при високому рівні анонімності й порівняно незначних витратах.

Кібернетичний тероризм. Звісно, не лишилися осторонь інформатизації й різноманітні терористичні організації та угруповання. Застосування інформаційно-комунікативних технологій підвищило ефективність їхньої злочинної діяльності, прискоривши перехід до децентралізованої мережевої структури від застарілої ієрархічної.

Для провадження своєї діяльності терористи активно використовують Інтернет, здійснюючи через глобальну мережу планування «операцій», зв'язок, збирання інформації, фінансові оборудки, рекрутування й навчання нових членів тощо. Приділяючи особливу увагу питанням фінансування, терористи все більше вдаються з цією метою до злочинів у кіберпросторі. Є дані, що шахрайство з банківськими картками, викрадення інформації, персональних даних тощо приносять терористам останнім часом більше зиску, ніж традиційна нелегальна торгівля наркотичними засобами [179]. Крім того, терористи все частіше вдаються до послуг тих кримінальників і груп, які спеціалізуються на кібернетичних злочинах, мають відповідну техніку й навички, що дає змогу ретельніше планувати та проводити мережеві фінансові оборудки, операції, пов'язані з контрабандою наркотиків, зброї та ін.

Як бачимо, терористи використовують практично весь спектр відомих кібернетичних злочинів. Тому часто не вдається достеменно визначити джерела й мотиви такого злочину й однозначно віднести його до кібертероризму.

Слід також зазначити, що з огляду на можливості, які відкрили інформаційно-комунікативні технології, терористичні організації й угруповання кардинально оновили свої злочинні доктрини та стратегії. Так, вони вдаються до методів і засобів, котрі зазвичай притаманні державним

збройним силам, зокрема до застосування найпоширеніших видів інформаційних операцій та елементів інформаційних війн.

Таким чином, інформатизаційна глобалізація зумовила нові безпекові реалії, змінивши механізми й інструментарій традиційних загроз національній безпеці, джерелом яких є державні органи, а також недержавні суб'єкти – терористи, злочинці, котрі у своїх протиправних цілях використовують інформаційно-комунікативні технології.

Сьогодні безпекова практика послуговується трьома базовими принципами систем захисту, запропонованими теорією інформаційної безпеки:

1) *цілісність* – забезпечення існування інформації у не викривленому стані;

2) *конфіденційність* – обмеження доступу до певної інформації осіб, котрі не мають на це повноважень, із метою її втаємничення;

3) *доступність* – забезпечення безперешкодного доступу до інформації відповідно до повноважень певних суб'єктів.

Заходи щодо протидії загрозам кібербезпеці власне й провадяться з метою реалізації вказаних властивостей інформації й системи та запобігання небезпекам у цій сфері. Захист інформації, забезпечення кібербезпеки передбачають перманентний процес підтримання й удосконалення функціонування захисних систем. Система захисту інформації, кібернетичного простору – це комплекс методів, засобів, заходів та відповідних спеціальних структур, спрямований на забезпечення безпеки системи та інформації, котра в ній обертається. Крім того, ці заходи мають передбачати й морально-етичні аспекти, про що говорив, зокрема, Л. Хофман [180]. Виходячи з викладеного, захисні заходи щодо кіберсфери можна класифікувати на законодавчі (правові), організаційно-адміністративні, фізичні й технічні (апаратно-програмні) і морально-етичні.

У плані національно орієнтованого забезпечення кібербезпеки цікавий досвід Китаю, де діє програма «Золотий щит», яка фільтрує зміст інтернет-

сайтів. Відповідна програма отримала неофіційну назву «Великий китайський фаєрвол», адже її використання забезпечує надходження даних від інтернет-провайдера не безпосередньо до користувача, а на спеціальний «сервер захисту», який вирішує, що саме можна показати споживачу. Водночас важливим є дотримання балансу між безпекою кіберпростору, психолого-інформаційною безпекою людини та доступністю інформації (за результатами «Золотого щита» в Китаї в різний час потрапляли під заборону Google, Wikipedia і Youtube [181]).

Для організації кіберзахисту в Україні сьогодні створена низка структур (наприклад, Ситуаційні центри при Службі безпеки України та Державній службі спеціального зв'язку та захисту інформації України [182]), які беруть участь у забезпеченні кібербезпеки. Вони займаються удосконаленням законодавства, вивченням і сертифікацією технічних засобів, забезпеченням інформаційного захисту систем органів державної влади, розслідуванням злочинів і виявлених кібератак, а також вжиттям заходів для їх припинення й подальшого недопущення. Втім, аналіз роботи зазначених структур свідчить про те, що вона здебільшого не збалансована і не синхронізована, відтак забезпечення безпеки кіберпростору неоднаково ефективно здійснюється в усіх напрямах. При цьому в методологічному плані вжиті заходи орієнтовані переважно на стримування процесів, які об'єктивно розвиваються, тому баланс кібербезпеки може бути порушений за рахунок витрачання відносно незначних ресурсів.

Вивчення зарубіжного досвіду забезпечення кібербезпеки також свідчить про значну диспропорцію рівня готовності до протидії кіберзагрозам на національному рівні, а також можливості використання передових напрацювань в Україні. Видається за доцільне при розробці державних програм (концепцій, стратегій) передбачити необхідність створення й розвитку системи постійного моніторингу кіберзагрози, розвитку національних систем оперативного виявлення кібератак удосконалення системи взаємодії державних органів, що беруть участь у забезпеченні

кібербезпеки, і громадських організацій, що працюють у сфері забезпечення інформаційної безпеки, організацію проведення науково-технічних робіт з проблем кібербезпеки тощо.

Також слід ураховувати, що розвиток засобів кіберзахисту часто супроводжується одночасним розвитком засобів нападу в кіберпросторі. Кіберзброя вже існує у світі як окремий клас озброєння. Провідні ІТ-держави відкрито заявляють про створення власного озброєння і підрозділів для ведення кібервійни [183], адже в сучасних умовах практично кожен політичний або воєнний конфлікт супроводжується протиборством у кіберпросторі. І якщо технологіями для проведення кібератак поки що володіє обмежена кількість країн, між якими вже виникають відкриті протистояння в кіберпросторі, дослідження в цій галузі ведуться багатьма країнами.

Загалом розвиток інформаційних технологій – процес із потужним потенціалом та надприбутковий бізнес. Наприклад, у Кореї обсяг системи E-learning (навчання за допомогою Інтернету і мультимедіа) щорічно зростає на 8,2%, і вже працює близько 20 віртуальних університетів. Разом з тим, існує дуже мало систематизованої інформації про безпеку в кіберпросторі, поданої в доступній формі. В Україні також є гостра необхідність запуску програми навчання населення. Вона повинна бути розрахована не тільки на вузькоспеціалізовані структури, а й на вивчення основ кібербезпеки в школах і інститутах, а також навчання людей, які вийшли з шкільного та студентського віку. Для інформування та навчання необхідно, в тому числі, створити інформаційно-консультаційний центр, де користувачі зможуть отримувати відповіді на питання, пов’язані з кіберзагрозами й кіберзахистом. Одним із перших кроків у цьому напрямі може вважатися, наприклад, створення у 2017 році інформаційної площадки (Antivirus.ua), місією якої є створення умов для обміну кваліфікованою інформацією між рядовими користувачами, експертами, представниками ЗМІ, навчальних закладів тощо.

Отже, ураховуючи швидку інформатизацію, масштаби потенційних наслідків злочинів у кіберпросторі, недостатню кіберзахищеність об’єктів

критичної інфраструктури та ризики, пов’язані з розвитком психологічної Інтернет-залежності, національні уряди та міжнародна спільнота повинні приділити серйозну увагу розвиткові систем кібербезпеки на національному та глобальному рівнях. Першочергові кроки в цьому напрямі повинні передбачати розробку необхідної нормативно-правової бази і підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду в цій сфері. Зокрема, перспективний підхід до забезпечення кібербезпеки об’єктів критичної інфраструктури має передбачати: забезпечення кібербезпеки на етапі проектування об’єктів критичної інфраструктури; виявлення мережевих подій, реагування на них, а також моніторинг мережевого трафіку в режимі реального часу для всіх ІТ-контурів об’єктів критичної інфраструктури; введення нових вимог до постачальників критично важливих ІТ-комплектуючих об’єктів критичної інфраструктури (наприклад, зобов’язання постачальника розкривати оператору цивільних ядерних об’єктів вихідний код прошивки програмних логічних контролерів після підписання контракту на постачання); впровадження рішень з криптографічного захисту інформації, а також цифрових підписів і захищених міток часу на всіх мережевих рівнях об’єктів критичної інфраструктури для надійнішого захисту цілісності та конфіденційності даних.

Розробка та впровадження рішень із криптографічного захисту інформації так само, як і розробка власних операційних систем, мережевих платформ, комунікаторів тощо, на сучасному етапі є необхідними заходами для забезпечення кібербезпеки (як кібербезпеки об’єктів критичної інфраструктури й інших технічних об’єктів, так і інформаційно-психологічної безпеки людини в кіберпросторі) на національному рівні.

На глобальному рівні, зважаючи на те, що не всі кібератаки підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинам, для забезпечення кібербезпеки важливим є передбачити зобов’язання країн не вдаватися в кіберпросторі до дій, метою яких є завдання збитків

інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави, відповідно до підходів, окреслених у Резолюції 60/45 Генеральної Асамблеї ООН «Досягнення у сфері інформатизації і телекомунікацій у контексті міжнародної безпеки» [184].

2.5 Досвід забезпечення кібербезпеки у зарубіжних країнах

Сьогодні питання забезпечення кібербезпеки хвилюють усе світове співтовариство, адже глобальний інформаційний простір на цей час налічує більш як 4.1 млрд. користувачів. У кіберпросторі стикаються інтереси країн та їхніх об'єднань, корпорацій, фінансових груп, політичних партій та рухів, неурядових організацій тощо, а також активно діють різні кримінальні групи (хакери) і міжнародні терористи, здійснюється економічне і військове шпигунство, робляться спроби виведення з ладу об'єктів критичної інфраструктури [185, с. 125-126]. Тож бурхливий розвиток інформаційних технологій та їх використання численними акторами для досягнення своїх політичних, економічних та інших цілей виводить проблеми забезпечення кібербезпеки на перший план.

Відсутність в Україні достатнього законодавчого забезпечення кібербезпеки в умовах гібридної війни значно підвищує ризики руйнування національної системи кібербезпеки, розвитку деструктивних впливів на національну безпеку, а також підривається впевненість в українській складовій забезпечення європейської та світової кібербезпеки. Національний координаційний центр кібербезпеки, який є робочим органом РНБО України, на сьогодні позбавлений можливості повномаштабно й системно здійснювати координацію щодо законодавчого та нормативно-правового забезпечення

ефективної системи кібербезпеки в Україні, в основі якої був би комплексний аналіз ситуації у цій галузі, викликів, існуючих та ймовірних небезпек і врахування інтересів кожного учасника та суб'єкта і яка б інтегрувалася до європейської та глобальної міжнародних систем кібербезпеки, мала б достатню фінансову, організаційну, технічну, кадрову підтримку. У зв'язку з цим необхідно вивчати зарубіжний досвід, створюючи в нашій країні ефективну систему, за якою забезпечуватиметься правовий та організаційний аспекти кібернетичної безпеки, імплементації окремих аспектів у національну практику, а також розширення співпраці в досліджуваній сфері.

Як нами уже зазначалося, кібербезпека - досить широке поняття, яке охоплює різні засоби і підходи до забезпечення безпеки в кіберпросторі. Згідно з визначенням Міжнародного союзу електрозв'язку, кібербезпека становить набір засобів, стратегії і принципи забезпечення безпеки, гарантії безпеки, підходи до управління ризиками, дії і практичний досвід, страхування й технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації і користувача. Кібербезпека включає заходи захисту та дії, що дають змогу здійснити захист кіберпростору як у цивільній, так і військовій сфері від загроз, які пов'язані з його взаємозалежними мережами і інформаційною інфраструктурою або можуть завдати їм шкоди [186, с. 133].

Відповідно до зростаючої ролі кіберпростору багато держав створюють свої національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 країн з інших частин світу мають власні національні стратегії кібербезпеки [187]. З урахуванням євроінтеграційного курсу України особливий інтерес у цьому контексті становить досвід забезпечення кібербезпеки в країнах ЄС.

Ухвалена Стратегія кібербезпеки Європейського Союзу 2013 року – це перший всеосяжний документ системного характеру у цій галузі. У ньому охоплено кожен аспект кібернетичного простору: внутрішній ринок, правосуддя, внутрішня та зовнішня політика.

Окрім Стратегії, відбулися розробка та ухвалення законодавчої пропозиції посилити безпеку інформаційних систем Євросоюзу.

Міжнародна політика Європейського Союзу щодо кіберпростору має низку визначених Стратегією пріоритетних напрямів, серед яких доцільно виокремити такі:

– засади свободи та відкритості: стратегією визначаються принципи, за якими реалізуються основоположні людські та громадянські права в кіберсередовищі;

– використання законодавчої бази Європейського Союзу в кібернетичному просторі аналогічно до фізичного світу. Що важливо в цьому аспекті, це той принципово важливий підхід, відповідно до якого відповідальним за безпеку цього простору є як пересічні громадяни, так і держави загалом;

– потенціал кібернетичної безпеки повинен розвиватися за допомогою співробітництва та партнерства, до якого залучені міжнародні партнери й організації, приватний сектор та громадянське суспільство [188].

З визначених напрямів випливає один суттєвий висновок: кібербезпека є справою всіх: самої людини, приватного сектору, суспільства й держави. Тільки в межах цього симбіозу вбачається можливість побудови суспільства у якому індивіди будуть почуватися безпечно в кіберпросторі. Досягнути цього можливо за умови дії декількох складових:

1) тісної співпраці держави в особі відповідальних за кібербезпеку органів та приватного сектору і громадян. Така співпраця насамперед полягає у взаємному обміні інформацією;

2) розвитку та практичного втілення таких категорій як «екологія інформації», «інформаційна гігієна», «критичне мислення у споживачів інформації», розвиток інформаційної культури, а також усвідомлення необхідності навчання дітей та молоді інформаційній культурі та гігієні.

Водночас слід ураховувати, що країни ЄС різняться за рівнем соціально-економічного й технологічного розвитку, рівнем розвитку цифрової економіки

та масштабами використання Інтернету. У зв'язку з цим у цілій низці країн ЄС національна стратегія з кібербезпеки розроблена недостатньою мірою незважаючи на вимоги Європейської комісії.

Виходячи з показників глобального рейтингу кібербезпеки (враховує показники країни в п'яти сферах: правові норми у сфері кібербезпеки та їх виконання; технічні заходи й наявність відповідних інструментів для їх реалізації; організаційні заходи у сфері кібербезпеки; розвиток потенціалу кібербезпеки; участь у міжнародному співробітництві щодо її забезпечення [189, с. 36]), найпередовішими в галузі розробки та застосування національних стратегій кібербезпеки серед країн-членів ЄС є Норвегія, Естонія, ФРН, Австрія, Угорщина, Нідерланди [189, с. 36]. Найменш успішними в плані кібербезпеки серед країн, що входять у ЄС, є Румунія, Болгарія, Бельгія, Португалія, Греція [189, с. 15].

У Нідерландах, як вважає асоціація виробників програмного забезпечення BSA [190], найрозвиненіша та найбільш «зріла» система кібернетичної безпеки, як з погляду правової підтримки, так і з погляду технологій та організації. Ця країна через кожні два роки переглядає свою Національну Стратегію кібербезпеки, а Національний Центр кібербезпеки, який є національним CERT (англ. ***c****omputer* ***e****mergency* ***r****esponse* ***t****eam*, CERT) із низкою додаткових повноважень, здійснюється розробка та запровадження всіх процедурних та технологічних питань стосовно безпеки в кіберпросторі. Цей же Центр активно співпрацює з Аналітичними та інформаційними центрами (ISACs), які дбають про те, щоб критична інформаційна інфраструктура за секторами була у безпеці.

Створення «Гарячої лінії» meldpunt-kinderporno.nl ініціював голландський Інтернет-провайдер для протидії дитячій порнографії як приватна структура, проте зрештою цю ініціативу підтримало Міністерство юстиції Нідерландів.

До слова, саме Нідерланди були ініціаторами створення загальноєвропейських мереж «гарячих ліній» – InHope [191] і перші

впровадили у своїй національній практиці.

Що стосується менш успішних країн у сфері забезпечення кібербезпеки, наприклад Румунії, її Національна стратегія забезпечення кібербезпеки, прийнята у 2013 р., передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також відповідність балансу основних прав і свобод громадян та інтересів національної безпеки, збільшення поінформованості щодо ризиків і загроз, пов'язаних з діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм. Держава виступає координатором заходів із забезпечення кібербезпеки, які спрямовані на досягнення таких цілей: адаптація законодавства до динаміки розвитку конкретних кіберзагроз; встановлення мінімальних вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури та її стійкість; усвідомлення й запобігання ризикам кібербезпеки; використання можливостей кіберпростору для просування національних інтересів, цінностей та цілей у кіберпросторі; сприяння та розвиток співробітництва між державним і приватним секторами на національному рівні, а також міжнародне співробітництво у сфері кібербезпеки тощо [192].

Виходячи з ключових правових актів Румунії, можемо констатувати, що особливістю державної політики забезпечення кібербезпеки є розвиток культури кібербезпеки користувачів комп'ютерів і телекомунікаційних систем, їхня поінформованість щодо потенційних ризиків, а також про можливості їх мінімізації. Збільшення поінформованості щодо ризиків і загроз, пов'язаних із діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм потребує ефективної комунікації й співробітництва між усіма учасниками діяльності в цій сфері. Тож Румунська держава бере на себе роль координатора заходів, здійснюваних на національному рівні, забезпечуючи кібербезпеку відповідно до визначених під керівництвом ЄС і НАТО підходів [193, с. 65].

Забезпечення кібернетичної безпеки Польщі покладається на Агентство внутрішньої безпеки (ABW), яке у 2013 році розробило стратегію кібербезпеки, а у 2015 році - Доктрину кібербезпеки Польщі. Під егідою ABW створено урядову команду реагування на комп'ютерні інциденти (CERT) [194], яка здійснює забезпечення та розвиток можливостей органів державного управління щодо захисту від кіберзагроз, передусім - від загроз критичній інфраструктурі [195, с. 69]. З ініціативи ABW також було створено Центр криптології при Міністерстві національної оборони, який здійснює захист інформації, забезпечує кібероборону та проведення наступальних кібероперацій [196].

Особливий інтерес становить досвід і практика забезпечення кібербезпеки в таких країнах, як ФРН. Слід брати до уваги те, що економіка Німеччини перебуває в епіцентрі різного роду кібератак і промислового шпигунства й помітно страждає від них, тому питання кібербезпеки для неї є одним із ключових. Відмінною рисою німецького підходу до забезпечення кібербезпеки є його комплексний і фундаментальний характер. Ще в 2005 р. в ФРН був розроблений і прийнятий «Національний план захисту інформаційної інфраструктури», а у 2007 році - «План реалізації захисту критичних елементів інфраструктури».

Створене в 1991 р. Федеральне управління з інформаційної безпеки Німеччини (BSI), яке є складовою МВС, є головним органом, відповідальним за національну кібербезпека ФРН. Цей орган формує політику і план дій в області інформаційної безпеки з метою запобігання, визначення і реагування на інциденти і кризи в цій сфері. BSI, зокрема, випускає попередження та оповіщення про віруси й інші шкідливі програми в IT-продуктах та послугах, дає рекомендації з протидії шкідливим програмам і діям, а також організовує інформаційний обмін з більш ніж 50 000 недержавних організацій, включаючи малий і середній бізнес.

У 2011 році у ФРН була прийнята нова Федеральна стратегія кібербезпеки [197, с. 11], орієнтована насамперед на захист критично

важливих інформаційних структур і виявлення додаткових можливостей в сфері забезпечення їхнього безкризового функціонування. Федеральна стратегія передбачає, що: безпека інформаційних технологій забезпечується спільними зусиллями громадянського суспільства і держави, при цьому комплекс інструментів захисту від кіберзагроз постійно розширюється; за допомогою Національного центру кібербезпеки (Nationales Cyber-Abwehrzentrum, NCAZ) відбувається оптимізація оперативного співробітництва між усіма органами державної влади та забезпечується захист від кібератак критично значущих об'єктів національної IT-інфраструктури та економіки; координація превентивних заходів і міждисциплінарних підходів у сфері кібербезпеки в державному і приватному секторах покладається на Національну раду кібербезпеки, що виступає додатковою сполучною ланкою IT-управління на федеральному рівні за участю різних міністерств та інших федеральних органів; ефективний контроль за злочинністю в кіберпросторі включає в себе цілий комплекс інститутів за участю підприємців і компетентних правоохоронних органів для розробки відповідних рекомендацій [198, с. 28-29].

У квітні 2017 році збройні сили ФРН також створили кіберкомандування (Cyber and Information Space Command, CIS), на яке покладається протидія хакерським і шпигунським атакам. Згідно з розробленим Бундесвером планом, до 2021 року чисельність CIS становитиме 14,5 тис. співробітників.

Францією була повністю переглянута своя політика оборони та нацбезпеки у 2008 та 2013 роках. В її межах відбувалися запобігання та реагування на кібернапади, що було визначено головними пріоритетами в організації нацбезпеки.

У липні 2009 року відбулося створення Французького агентства мережевої та інформаційної безпеки (ANSSI, Національне агентство з питань інформаційного захисту) [199], пріоритетом якого стало розширення можливостей оперативного реагування на постійно зростаючі кіберзагрози. Цей орган є міжміністерським агентством при кабінеті прем’єр-міністра.

ANSSI набуло більшої ваги на початку 2011 року, коли Агентство перетворилося на національний орган захисту інформаційних систем.

Після того, як було створено Агентство, Франція опублікувала національну стратегію оборони та безпеки інформаційних систем у 2011 році. Білою книгою у 2013 році була підтверджена кіберзагроза і конкретно визначена небезпека саботажу, ціллю якого є критична інфраструктура.

Європейська Комісія та Європейська служба зовнішньої діяльності (EEAS) у лютому 2013 року презентували стратегію кібербезпеки ЄС. У розрізі цієї стратегії Франція займається активним сприянням запровадженню п’яти головних напрямів:

– загальної стійкості ЄС (разом з органами організації);

– боротьби з кібернетичною злочинністю;

– кібербезпеки у Спільній політиці безпеки і оборони;

– промислових питань;

– міжнародної політики щодо кібернетичного простору.

Позитивною практикою правового забезпечення системи кібербезпеки є досвід Австрії. Австрійську Стратегію кібербезпеки ухвалили у 2013 році. Це частина загальнішої Національної стратегії з безпеки ІКТ. Вона є деталізованою програмою дій із визначенням завдань із кібернетичної безпеки та безпеки інформаційно-комунікаційних технологій та заходів, необхідних, щоб їх досягнути. У Національної команди реагування на випадки надзвичайних комп’ютерних подій CERT.at [200] є коло широких та доволі чітко прописаних повноважень.

Стратегія кібербезпеки Австрії визначає, що звичайні напади на Австрію стали малоймовірними в недалекому майбутньому, натомість актуальними стають нові проблеми глобального співтовариства [201]. Зокрема, як загрози в кіберпросторі, так і продуктивне його використання практично не обмежене, тому напади з кіберпростору та зловживання його можливостями становлять безпосередню загрозу безпеці та належному функціонуванню державного апарату, економіки, науки й суспільства. Відтак одним з головних пріоритетів

Австрії є реалізація всеосяжної політики кібербезпеки, за якої зовнішня й внутрішня безпека, а також усі аспекти цивільної й військової безпеки тісно пов'язані та взаємозалежні. Забезпечення кібербезпеки здійснюється у проактивному форматі, що передбачає запобігання загрозам кіберпростору або мінімізацію їх впливу, а також базується на співробітництві у сфері забезпечення кібербезпеки на європейському й міжнародному рівнях. Центральним органом у сфері забезпечення кібербезпеки є Центр боротьби з кіберзлочинністю (Cyber Crime Competence Center) Федерального міністерства внутрішніх справ Австрії. На нього також покладається здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю [202].

У країні є певні інституціалізовані (та численні неформальні) державно-приватні партнерські ініціативи (такі, приміром, як Австрійський центр безпеки інформаційних технологій – Centre for Secure Information Technology Austria/A-SIT [203] та Kuratorium Sicheres Österreich). Останній, наприклад, позиціонує себе як міст між бізнесом, наукою, адміністрацією та політикою з 1975 року. «Наша місія: активний розвиток питань безпеки, які мають високий пріоритет для всіх нас» - зазначено на офіційному сайті організації [204].

Також функціонує Austrian Trust Circles, метою якого є інформаційний обмін, покликаний захистити критичну інформаційні структуру за окремими секторами економічної системи та розробити специфічні для окремих секторів плани з оцінювання ризиків. Austrian Trust Circles – це спільна ініціатива CERT.at разом з австрійським урядом [205]. Активізовано «гарячу лінію» stopline.at, куди можна подати скаргу щодо дитячої порнографії, онлайн пропаганди націонал-соціалістичної символіки та іншого небажаного контенту.

Фінляндія займає перше місце за рівнем цифрової грамотності у рейтингу країн ЄС, а також друге місце – за показником поширення мережі широкосмужного зв'язку [206]. Стратегія кібербезпеки Фінляндії, затверджена у 2013 році, передбачає, що загрози, які виходять з кіберпростору,

стають усе серйознішими, адже кібератаки можуть використовуватися як засіб політичного й економічного тиску разом із військовими засобами, і закладає таке бачення кібербезпеки: Фінляндія може забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях; громадяни, органи влади та юридичні особи можуть ефективно використовувати безпечний кіберпростір, що є результатом здійснення заходів кібербезпеки на національному й міжнародному рівнях; держава має бути готова до протидії кіберзагрозам. Розслідування кіберінцидентів у Фінляндії здійснює поліція, натомість організація кіберзахисту покладається на Сили оборони Фінляндії. Військовий кіберзахист включає в себе розвідку, кібератаки та ведення кібервійн, а також «інтелектуальне попередження» загроз [207].

Якщо вести мову про організацію забезпечення кібербезпеки в країнах Європи в цілому, слід зауважити, що у 2013 році була представлена стратегія кібербезпеки ЄС під назвою «Відкритий, безпечний і надійний кіберпростір». Метою цієї стратегії є підвищення стійкості та нарощування потенціалу у сфері кібербезпеки країн-членів ЄС, включаючи посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення інформаційної безпеки, розробку принципів координації міжнародної політики в області кібербезпеки. Серед інших значущих актів, спрямованих на формування єдиної політики ЄС із протидії кіберзагрозам, слід відзначити «Директиву ЄС з кібербезпеки» [208]. Відповідно до цієї директиви, країни-члени ЄС спільно з Європейською Комісією та Європейським агентством з мережевої та інформаційної безпеки (ENISA) повинні створити групу взаємодії. Основними функціями цієї групи є обмін інформацією між її учасниками, а також боротьба із загрозами й інцидентами у сфері кібербезпеки. Крім того, у директиві міститься вимога створити мережу національних груп з метою організації швидкої і ефективної операційної взаємодії й підтримки країн-членів ЄС для вирішення транскордонних інцидентів в кіберпросторі. Ця директива, розроблена Європейською комісією і схвалена Європарламентом, набула чинності в серпні 2016 р. З цього моменту

почався процес імплементації основних положень директиви в національному законодавстві країн - членів ЄС і визначення операторів, які будуть на практиці забезпечувати кібербезпеку у Європі.

Ще одним заходом, покликаним посилити кібербезпеку ЄС, стало запропоноване Європейською комісією у 2017 році введення сертифікатів для цифрової продукції і цифрових послуг, що випускаються в країнах ЄС. Із полгляду Єврокомісії, сертифікація може відігравати вирішальну роль в посиленні безпеки і розвитку єдиного європейського ринку цифрових продуктів і послуг, оскільки сертифікати будуть дійсними на всій території ЄС і зможуть гарантувати відповідність продуктів і послуг вимогам кібербезпеки [197].

Важливим кроком на шляху захисту даних користувачів комп'ютерних мереж також став загальний регламент ЄС про захист даних (General Data Protection Regulation, GDPR), розроблений і схвалений Європейським парламентом ще у 2016 році, який набрав чинності у травні 2018 року. Цей регламент, покликаний регулювати поширення та використання особистих даних громадян країн ЄС, встановлює норми, відповідно до яких користувачі з країн ЄС мають право знати, як саме використовуються їхні персональні дані, які вони надають про себе в комп’ютерних мережах. Нові правила є екстериторіальними та поширюються на операторів, які обробляють персональні дані європейців не тільки в країнах ЄС, а й за його межами [197].

Досить прогресивним кроком ЄС на шляху забезпечення кібербезпеки стало створення на початку березня 2020 року, з ініціативи Литви, кібернетичних сил Євросоюзу швидкого реагування (Cyber Rapid Response Team, CRRT [209]), до складу яких увійшли представники шести європейських країн (Естонія, Литва, Польща, Нідерланди, Румунія, Хорватія,). Це було остаточно погоджено 4 березня в Загребі (Хорватія) у Меморандумі про взаєморозуміння. Документ юридично дозволяє роботу таких груп у юрисдикціях різних країн, визначає механізм роботи CRRT, правовий статус, ролі і процедури. Створені цивільними і військовими експертами, CRRT

приєднаються до нейтралізації та розслідування небезпечних кіберінцидентів практично або, за необхідності, фізично [210]. Статус спостерігача у даному об'єднанні отримали Бельгія, Греція, Іспанія, Італія, Франція, Словенія і Фінляндія.

Розвідслужби Литви у 2019 році оголосили, що в кіберпросторі Литви простежується шкідницька діяльність кібернетичних потужностей Росії і Китаю. У традиційній оцінці загроз нацбезпеці зазначається, що найбільшу загрозу для безпеки інформаційних систем і інформації, що зберігається в них, є кібершпіонаж розвідслужб Росії, а новим фактором ризику може стати розвиток технологій 5G, якщо не буде приділятися належна увага надійності постачальника послуг або продуктів інформаційних технологій [211].

Позитивними прикладами для України можуть слугувати практичні знання, яких набула Естонія, єдина пострадянська країна, що має значні успіхи у створенні системи кібернетичного захисту.

2007 року Естонії випало бути першою країною-членом НАТО, кіберпростір якої було атаковано хакерами, і цей напад підтримувала інша держава. Захист країни в кіберсередовищі здійснювався громадянами – кваліфікованими ІТ-інженерами, які разом обміркували і взялися до впровадження системи захисту. Естонці створили такі стандарти кібернетичної безпеки, які пізніше перейняло НАТО задля впровадження у своєму оборонному та безпековому сегменті. Зараз у світі є 32 центри, які користуються саме естонськими стандартами. На цей час у країні, яка має населення 1,2 мільйони людей, функціонує 5 кібернетичних центрів. Актуальність естонського досвіду для України пов'язана з багатьма аспектами: спільним минулим, територіальною близькістю, однаковими зовнішніми чинниками, які викликали в Естонії потребу оперативного створення системи кібернетичного захисту.

Країни Балтії чітко усвідомили потенційний вплив від ескалації конфлікту в Україні на їхню безпеку. Передусім це Польща та країни Прибалтики. Саме ці країни безпосередньо відчули близькість загроз

(наприклад, популяризація в соціальних мережах Латвії ідеї «Латгальської народної республіки», на кшталт терористичних організацій ДНР та ЛНР, звинувачення МЗС РФ у дискримінації Латвією російськомовного населення спонукало прибалтів провести чіткі паралелі з українським питанням) [212].

В умовах спроб переділу сфер впливу Балтія залишається однією з найвразливіших ланок європейської безпеки. У разі загострення конфліктних ситуацій на східних кордонах України, а також посилення дипломатичного протистояння щодо Росії, остання демонстративно намагатиметься нарощувати військову присутність на кордонах з балтійськими країнами.

Найвразливішою з країн Балтії є Естонія, найбільш східне місто якої — Нарва — налічує 90 % етнічних росіян. У разі російської агресії в цьому напрямку під сумнів будуть поставлені не лише політичні запевнення щодо безпеки, як це сталося з Будапештським меморандумом, а й союзницькі зобов'язання країн-членів НАТО.

За таких умов Україна є важливим стратегічним партнером, який може стати вирішальним у врегулюванні проблеми безпеки в країнах Балтії. Першим практичним кроком у цьому напрямі є налагодження співпраці між Україною, Польщею та Литвою, вигідної для всіх країн регіону Східної Європи.

Для зміцнення своєї безпеки Україні необхідно встановлювати тісніші контакти з Мінськом у всіх сферах, роблячи акцент на сфері інформаційній, яка залишається поки що поза увагою сторін. Розвиток двостороннього українсько-білоруського співробітництва буде сприяти вирішенню багатьох проблем, що виникли в умовах кризи європейської безпеки. Сама ж Білорусь уже опосередковано втягнута в цей процес і не може розглядатись як нейтральна сторона в межах майбутнього протистояння на тлі «великих торгів» щодо подальшої долі Східної Європи. Однак є група країн, які недооцінюють масштабність загроз із боку Росії. Це країни Центральної Європи, які мають відносно невизначене ставлення до того, що відбувається в Україні.

Це Болгарія, Словаччина, Чехія, Угорщина. Насправді дуже дивує, що, перебуваючи у минулому столітті у радянському Варшавському блоці, вони не цілком усвідомлюють загрозу від поведінки Росії. Ці країни на засіданнях Ради ЄС або відмовчуються з українського питання, або займають невизначені чи не надто проукраїнські позиції. Зрозуміло, що тут важливу роль відіграє фактор їхньої енергетичної та фінансової залежності від Росії.

Деякі з перерахованих кроків ЄС у сфері кібербезпеки при відповідній адаптації та коригуванні можуть бути корисними Україні. До таких кроків, як видається, належать, наприклад, визначення або створення єдиного державного органу з питань кіберзахисту, здатного відповідати на кібератаки, сертифікація цифрових продуктів і послуг, заходи із захисту персональних даних користувачів комп'ютерних мереж, що передбачають значні штрафи за незаконне використання цих даних.

Очевидним є той факт, що кіберзагрози сьогодні переважно мають глобальний характер. А тому й на міжнародному рівні постає необхідність концентрації зусиль та створення спільних механізмів забезпечення кібербезпеки. Яскравим таким прикладом є підписання першого в історії договору між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак під час проведення зустрічі на вищому рівні глав держав та голів урядів країн — учасниць Північноатлантичного альянсу, яка проходила у 2016 році у Варшаві.

Актуальним для нас є досвід Індії у забезпеченні кібербезпеки. Ця країна, яка сьогодні займає лідерські позиції у сфері інноваційного та науково-технічного розвитку, у 2019 році, за даними аналітичних досліджень була визнана однією з найменш захищених країн у сфері кібербезпеки [213].

Індія пройшла через важливу стадію інформаційного розвитку, коли у 2015 р. була прийнята національна програма «Цифрова Індія», націлена на забезпечення електронного доступу громадян до послуг, які надає держава, через розвиток всесвітньої мережі та вдосконалення інфраструктурного аспекту зв'язку [214]. Головними пріоритетами стали: надати кожному

можливість широкосмугового доступу, поширювати мобільні технології, створити систему, за якою надавалися б цифрові державні послуги, створити нову модель економічної діяльності, в основі якої лежать послуги, розвивати соціальні медіа, розвивати освіту та навчання, розширювати коло можливостей для молодих людей тощо. Пріоритетними сферами діяльності стали: цифрова економіка, цифрова ідентифікація особистості (система adhaar охопила у 2019 році понад 90 % населення), розбудова електронного державного врядування (втілення програми e-Kranti: National e-Governance Plan 2.0), розвиток смарт-міст [215].

В Індії доволі потужна система правового регулювання галузі інформаційного захисту, проте, в цій країні існують суттєві інформаційні загрози, зокрема, враження комп'ютерної та мобільної техніки шкідливими програмами, напади на фінансові структури та банківські установи, відсутність захисту ринку криптовалюти й інші [216].

Незважаючи на наявність належного правового поля, характер інформаційних атак в Індії стає все більш руйнівним і масштабнішим за зоною ураження та результатами їхнього використання. Внаслідок цього можуть поглибитися численні проблеми не лише стосовно інформаційної безпеки, а й у політичній, економічній, суспільній безпеці Індії, адже атак зазнають вкрай значущі інфраструктурні компоненти суспільства. У небезпеці опинилася низка важливих національних ініціатив, таких як «Розумні міста», «Електронне управління», «Управління цифровою публічною ідентичністю», від втілення яких залежить, наскільки ефективною буде стратегія розбудови країни у цілому. Крім того, Індію вважають одним із найкращих варіантів для аутсорсингової діяльності у світі, тому ключові світові бренди – Apple, Sapient, Citi Bank, HSBC, Bank of America, DSM та інші – кожний створив свій глобальний центр доставки, центр надання послуг та сервісної підтримки в Індії [217]. Тож недостатня інформаційна безпека може мати вплив не лише на власне державу, але й відобразитися на міжнародних бізнес-партнерах, чиїм інтересам шкодитимуть кібератаки або завдаватиметься шкода, якщо стратегії

оперативного реагування на них будуть неефективними.

Важливий етап у справі побудови своєї системи кібернетичної безпеки відбувся на Мюнхенській конференції з безпеки (2012 р.), у межах якої спеціалісти в ІКТ-сфері з Індії повідомили, що планують створити свої мікропроцесори і скоротити імпорт програмного забезпечення у військовому сегменті та збільшити інвестиції у свої проекти. У цьому ж році було запропоноване створення командного центру, щоб відстежувати критичну інфраструктуру та ліквідовувати прогалини в системі кіберзахисту [218].

Скандал зі Сноуденом 2013 року виявив, що Сполучені Штати негласно спостерігають і за Індією. Тож там почали у прискореному режимі розробляти національну стратегію щодо кібербезпеки. «Національній політиці у галузі кібербезпеки» належить статус першого індійського доктринального документа, націленого на забезпечення комплексного бачення державних пріоритетів, приватного сектору та соціуму щодо того, як вирішувати питання кібернетичної безпеки, а також закладення основ для систематизованих та узгоджених дій кожної зацікавленої сторони для того, щоб пріоритети втілювалися практично [218].

Основними цілями втілення стратегії були такі: створення ефективної системи захисту персональних даних осіб, фінансових і банківських даних та інформації, що має важливе значення для держуправління і безпеки, від несанкціонованих випадків доступу та кібернападів; підвищення рівня надійності функціонування ІКТ-систем та їхнє повномасштабне запровадження у кожен сектор економічної системи; підготовка необхідного числа (приблизно 500 тисяч) фахівців упродовж майбутніх 5 років задля того, щоб зробити інформаційний простір держави безпечнішим та надійнішим [219].

Кібербезпека, відповідно до синтезу докторинальних та законодавчих підходів, розглядається як діяльність, спрямована на захист інформації та інформаційних систем (мережі, комп’ютери, бази даних, центри обробки інформації та додатки), застосовуючи відповідні процедурні та технічні заходи

безпеки. Із цього погляду кібербезпека - це досить широке поняття, що включає кожен вид націленої на захист діяльності.

Поняття кіберзахисту окреслюється як вужчий виду діяльності, що стосується певних аспектів та організацій. Основне, чим відрізняється кібербезпека від кіберзахисту в мережевому просторі, - це характер небезпек для того, що повинне бути убезпеченим, із застосуванням всього доступного інструментарію. Кібернетичний захист є оборонною дією, спрямованою на боротьбу з деструктивною діяльністю супротивників, в яких є політична, квазіполітична або економічна мотивація, від чого залежать національна безпека, громадська безпека або економічна розбудова суспільства [219].

У 2019 році на Індію двічі здійснювалися кібератаки на такі вкрай важливі інфраструктурні об’єкти як атомна електростанція Куданкулам та Індійська організація космічних досліджень. І попри те, що напади не відмітилися суттєвими збитками або шкодою, це стало достатньою причиною для продовження Індією активної участі в обговоренні проблематики кібернетичної безпеки на кожному рівні міжнародної співпраці. Аналогічно до міжнародного тероризму та захисту довкілля співробітництво - це необхідна умова протидії кіберзагрозам транскордонного характеру. Національна політика кібербезпеки 2013 року не враховувала ці нюанси, і не було створено механізму, за яким би відстежувалася та оцінювалася ефективність виконання визначених завдань. У зв’язку з цим пріоритети реалізуються дещо хаотично, через що держава стала неспроможною вирішити поставлені завдання. Тож ці проблеми Індія намагатиметься нівелювати, реалізуючи нову Національну політику у сфері кібернетичної безпеки на 2020-2025 роки [220].

Доволі вагомим етапом розвитку сегменту кібербезпеки Індії стала й побудова у 2018 році своєї кібернетичної оборони. Так, була створена військова агенція з питань кібербезпеки – Оборонна кіберагенція, яка повинна взаємодіяти з апаратом національного радника з безпекових питань. Було заплановано, що агенція забезпечить підготовку тисячі фахівців, які опікуватимуться кібербезпекою армії, ВМС та ВПС Індії, а також

займатимуться наступальними операціями у кіберсередовищі. У перспективі ця структура повинна стати повноцінним кіберкомандуванням [221].

Як бачимо з досвіду Індії, досить важливими кроками на шляху створення повноцінної та ефективної системи кібербезпеки держави є розробка й реалізація короткострокових та середньострокових державних програм з урахуванням змін та динаміки кіберзагроз. Іншим важливим аспектом таких процесів є концентрація зусиль не тільки на кібероборонi, а й застосування активних заходів кіберзахисту, по суті впровадженні політики активної оборони в кіберпросторі.

Аналіз нормативних документів, які стосуються питань забезпечення кібербезпеки нашої держави, різних країн, дає можливість узагальнити та виокремити найбільш значущі для них загрози в цій сфері.

Статус головних небезпек для національного кіберпростору стратегії більшої частини країн надають:

1. Кібершпигунству та воєнним діям, які підтримує або про які поінформована держава. Усім технологічно розвиненим країнам та корпораціям доводиться ставати об'єктами кібершпигнуства, яке має мету отримати державні або промислові таємниці, персональні дані або іншу цінну інформацію [222]. Так, вкрай резонансною кібератакою стали дії КНДР проти компанії "SonyPictures Entertainment", у результаті чого порушники одержали конфіденційні дані, зокрема інформацію стосовно комерційних операцій фірми [223].

2. Використанню глобальної мережі задля терористичних цілей. Терористичні угрупоуваннями використовують Інтернет, щоб здійснювати пропаганду, збирати кошти і вербувати людей [222].

3. Кіберзлочинності: крадіжка персональної інформації та відмивання грошей, одержаних в незаконний спосіб. Злочинці займаються продажем інформації щодо номерів банківських карток, паролів від серверів та шкідливого програмного забезпечення [222].

Зазначимо, що національними законодавствами держав зазвичай

регулюються аспекти захисту таких речей, об’єктів та процесів як [224]:

1. Персональні дані (у Естонії, Канаді, Нідерландах, Швеції, Фінляндії, Іспанії).

2. Електронна комерція та електронні транзакції, платіжні інструменти (у США, Канаді, Польщі, Естонії, Італії).

3. Діти (у США).

4. Важливі об’єкти інфраструктури та інформаційних систем (у Франції).

Досить цікавим у досліджуваному контексті є досвід Ізраїлю. Зокрема розширення у 2018 році повноважень Національного кібердиректорату (National Cyber Directorate, NCD) — провідного державного агентства з питань кібербезпеки [225]. Розширення повноважень стосувалися передусім оцінки ризиків для національних мереж, планування захисту та відновлення, а також управління державними та приватними структурами. Ці зміни на експертному рівні були оцінені неоднозначно [226]. Проте, як зазначають в Уряді, пояснюються постійним зростанням загроз у кіберсфері.

Цікаво, що в Ізраілі розділені функції цивільних та військових органів. Так, NCD повинен оцінювати загрози, виявляти уразливі місця в національних системах та обмінюватися інформацією в режимі реального часу, однак у нього немає повноважень вживати заходів у відповідь на атаки. Передбачається, що активні дііу кіберпросторі провадитимуть військові, а також спецслужби Ізраїлю.

У структурі NCD створено два органи: Центр протидії кіберзагрозам (цю функцію виконуватиме команда реагування на комп’ютерні надзвичайні події CERT-IL) і Центр раннього виявлення та верифікації для попередження про атаки та зменшення їхнього шкідливого впливу. Останній має сприяти обміну даними про ситуацію в інформпросторі між державними та приватними організаціями. Це робитиметься, зокрема, і через створення та наповнення національної бази даних із маркерами загроз. Запропонована база викликала значні суперечки в ізраїльському суспільстві, адже йдеться про збирання та

обробку великих масивів приватної та корпоративної інформації [225].

Основними правовими документами політики Ізраїлю у сфері кібербезпеки є Національна кіберініціатива 2010 та Резолюція уряду № 3611 від 7 серпня 2011 року, яка є планом дій Національної кіберініціативи [227].

Слід зауважити, що в Ізраїлі не тільки успішно розвивається сфера кібербезпеки, а й проводяться власні розробки кіберзброї. Такі ініціативи мають за мету створити в Ізраїлі аналог Інтерполу в кіберпросторі, а також запровадити систему обміну інформацією між усіма суб'єктами кіберзахисту у поєднанні зі спроможностями державного та приватного секторів [228, с. 49]. Досвід співпраці державного та приватного секторів у сфері забезпечення кібербезпеки може бути корисним для національної практки.

Таким чином, можна констатувати, що Ізраїль має значні можливості протистояти дедалі більшим кіберзагрозам. Разом з тим, нові положення породжують дискусії, що підкреслює складнощі у підтриманні рівноваги необхідності гарантування національної безпеки та захисту фундаментальних громадянських прав.

Виходячи з аналізу забезпечення кібербезпеки у зарубіжних країнах, зокрема Ізраїлі, вважаємо за доцільне запропонувати окремі напрями вдосконалення національної практики у досліджуваній сфері. Зокрема, доповнити Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242/2016 [99] у частині вдосконалення основних завдань цього органу. У цьому контексті пропонується розширити пункт 3 указаного Положення, додавши до основних завдань Центру такі:

– впровадження в Україні стандартів безпеки мережевих та інформаційних систем;

– визначення критеріїв, за якими буде складатись перелік операторів базових послуг та провайдерів цифрових послуг;

– контроль за дотриманням мережевої нейтральності й міжнародних та європейських стандартів та заборон введення окремих національних

стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами;

– аудит системи мережевої та інформаційної безпеки;

– організація та підтримка системи сповіщення про кіберінциденти, системи аудиту й впровадження заходів мережевої та інформаційної безпеки;

– забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема щодо персональних даних та захисту комерційних інтересів операторів і провайдерів.

В Україні є свій досвід, коли у 2015 році були намагання втрутитися до системи енергопостачання, яка, крім того, включає і ядерну енергетику. Європейські країни, передусім Німеччина, вже були об'єктами схожих атак. Не менше значення має проведення різних операцій в кіберсфері, спрямованих на перешкоджання нашим демократичним процесам. Ми вже ставали свідками дезінформаційних кампаній проти референдумів, як, наприклад, стосовно Brexit у Великій Британії чи Угоди про асоціацію з Україною в Нідерландах. Операції, які покликані підмінити результати волевиявлення, зараз перетворюються на нову норму.

Основна проблема ефективного забезпечення кібербезпеки полягає у створенні в ЄС єдиного європейського політичного простору. Значна активність в цій сфері керівних органів ЄС стикається з нездатністю низки країн в повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Слід також ураховувати, що паралельно з реакцією ЄС на актуальні кіберзагрози безперервно з'являються все нові загрози кібербезпеки, на які держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати. Переважно це відбувається через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору. Проте, не дивлячись на ці проблеми, система забезпечення кібербезпеки в країнах ЄС досить швидко розвивається і вдосконалюється, чому сприяє настільки ж швидке накопичення досвіду

регулювання і координації дій країн - членів ЄС у сфері кібербезпеки.

В умовах розробки Україною національного законодавства у сфері кібернетичної безпеки (з урахуванням умов Угоди про асоціацію між Україною та ЄС [229]) дієвим може бути врахування досвіду ЄС, перспективних майбутніх планів, програм і проєктів, а також участь у спільних європейських проеєктах із забезпечення кібернетичної безпеки.

При цьому вважаємо за необхідне підкреслити надважливість проблем забезпечення кібернетичної безпеки всіма суб'єктами її забезпечення, як національного так і міжнародного рівня і визначити її як свій пріоритет стратегічного значення. Необхідним є створення команд фахівців-консультантів з питань кібербезпеки на всіх рівнях: від захисту комерційних секретів до розробки правової бази та формування державної політики. Питання кібернетичної безпеки має бути окресленим чіткіше, стати більш зрозумілим і вимірюваним. Компанії, які включає критична інфраструктура, повинні нести відповідальність за рівень своєї готовності й захисту, адже припинення діяльності тієї чи іншої організації в сучасних динамічних реаліях може призвести до руйнівних наслідків та загроз національній безпеці держави.

Нам слід покращити наші партнерські відносини у плані обміну набутими знаннями. Україна володіє надзвичайним досвідом практичної реалізації протидії кіберзагрозам. Вона стала кібернетичним фронтом, на якому Росія проводить випробування своєї нової кіберзброї, котру зможе використовувати у всьому світі. У зв'язку з цим підтримка України повинна стати пріоритетним завданням для країн ЄС, оскільки так вони подбають і про свою безпеку. Безумовно, Україна сьогодні має позиціонуватися як потужний форпост європейської безпеки. На нашу думку, визріла потреба переглянути концепції європейської безпеки. Росія своєю загарбницькою поведінкою продемонструвала, що цивілізованими способами неможливо протистояти її агресії. Результати такої діяльності нікчемні. Відповідно, потребують змін основні акценти концепції європейської безпеки. І це стосується, зокрема,

світових безпекових процесів.

Безпеку у Європі визначають чотири основні фактори: НАТО, ЄС, стратегічна присутність США й відносини з Росією. Україна не є членом ні НАТО, ні ЄС, стратегічна присутність США теж відчутна на рівні консультацій та моральної підтримки. У зазначеному контексті хотілося б погодитись з думкою професора О. Власюка, який зазначив, що «гібридна війна», яку Російська Федерація розгорнула проти України, не закінчується, власне, самою Україною, бо це цивілізаційна війна, війна ідентичностей і смислів, об'єктивно й суб'єктивно спрямована проти Західного світу. Як і в XIII столітті, питання стоїть руба: чи переможе Золота Орда, фактичною спадкоємницею якої є РФ, чи переможе Західна цивілізація, форпостом якої на Сході є нинішня Україна [230].

Україна, перебуваючи в епіцентрі масштабного цивілізаційного експерименту, не може отримати те, що пообіцяли їй світові лідери, коли ми позбувалися ядерної зброї, – безпеки.

Безумовно, у межах Будапештського меморандуму українським лідерам в той час слід було передбачити потенційні загрози й виписати більш чіткі механізми гарантування нашої безпеки, проте формальний бік цього документа проігнорували передусім США та Англія.

Звертаючись до питання міжнародних гарантій безпеки, слід зазначити, що в процесі активної міжнародної дискусії гарантії незастосування ядерної зброї проти неядерних держав отримали умовну назву «негативні», а гарантії допомоги у разі нападу — «позитивні». Проте неядерним державам так і не вдалося домогтися юридичних гарантій (навіть «негативних») у формі міжнародного договору, конвенції або іншого багатостороннього документа. Якщо говорити про міжнародні гарантії безпеки, надані Україні, їх можна назвати декілька:

— Будапештський меморандум [231];

— Тристороння заява президентів України, США і Росії [232];

— Хартія про особливе партнерство між Україною та Організацією

Північно-Атлантичного договору 1997 року [233], яка містить посилання на гарантії безпеки Україні як без'ядерній державі, надані у Будапешті в 1994 році, а також нагадує: «Союзники по НАТО продовжуватимуть підтримувати суверенітет і незалежність України, її територіальну цілісність, демократичний розвиток, економічне процвітання та її статус без'ядерної держави, а також принцип непорушності кордонів як ключові фактори стабільності та безпеки у Центрально-Східній Європі та на континенті в цілому».

Визначені нами міжнародні документи на сьогодні виявилися неспроможними гарантувати суверенітет та територіальну цілісність нашої держави. Такий приклад досить негативно характеризує концепцію міжнародної безпеки як таку, що неспроможна на практиці втілити взяті на себе зобов'язання щодо інших країн.

Водночас слід відверто визнати, що українська дипломатія у 90-х роках не скористалася історичним моментом і, перебуваючи в полоні ілюзій щодо початку нової ери в міжнародних відносинах, не спромоглася повною мірою виконати своє головне завдання — забезпечення національних інтересів і безпеки України [234].

Основна думка, яку Україна має доносити Європі та світові: те, що відбувається в Україні, не є внутрішнім українським конфліктом, і навіть не двостороннім конфліктом (війною) з Росією, а загрозою всьому світові. Адже поведінка Москви свідчить про те, що Україна є не так її самоціллю, як інструментом для вияву незадоволення своєю позицією у світі. І поки Росія не отримає місця, якого, на її власну думку, заслуговує, вона не заспокоїться. Тому ніхто не може і не повинен відчувати себе у безпеці. Цю тезу треба поширювати усіма каналами, використовуючи усі міжнародні інструменти.

Отже, те, що відбувається сьогодні в Україні, не внутрішній конфлікт і навіть не війна з Росією, а загроза всьому світу. Російська агресія проти України засвідчила вразливість сучасних систем міжнародної безпеки. Прикладом такого висновку можуть слугувати абсолютно недієздатна Рада

безпеки ООН, неефективність та часто непрофесіоналізм представників ОБСЄ, що поставило під сумнів здатність Ради безпеки та організації в цілому досягти цілей, закріплених у Статуті ООН.

Анексувавши Крим та ведучи воєнні операції, Росія порушила базові принципи європейської безпеки. Європейська безпека була заснована на недопущенні застосування сили для досягнення політичних або стратегічних цілей, а також на наявному стратегічному та військовому балансі в Центральній і Східній Європі, де поважають територіальну цілісність та свободу кожної держави обирати свою зовнішньополітичну лінію та стратегічне спрямування. Насправді те, що відбувається наразі в Україні, формуватиме характер європейської безпеки на десятиліття вперед. Незалежна, цілісна, стабільна Україна та демократичні цінності мають вирішальне значення для стабільної, безпечної та демократичної Європи. При цьому, тема кібербезпеки матиме першочергове значення у майбутньому співробітництві України та Євросоюзу.

Європейський Союз повинен розпочати роботу над оновленням своєї стратегічної концепції безпеки, основою якої має стати чітке усвідомлення, що Україна — це наріжний камінь безпеки в Європі. Проте, як вчить нас історія, захищати і себе, і Європу маємо самотужки. Це нас гартує, це насторожує й лякає наших ворогів, і це робить нас сильними.

Висновки до розділу 2

Серед пріоритетних напрямів наукових досліджень, у цьому розділі були ткакі: аналіз стану правового забезпечення кібербезпеки в Україні, дослідити систему суб'єктів забезпечення кібербезпеки в Україні, визначити та обґрунтувати пріоритетні напрями протидії кіберзагрозам як на національному так і на глобальному рівнях, дослідити досвід забезпечення кібербезпеки зарубіжних країн та, на цій основі, обґрунтувати оптимальні напрями для вітчизняної практики. За результатами проведеного дослідження можемо зробити такі основні висновки:

1. Аналіз національного законодавства у сфері кібербезпеки дав змогу виокремити низку принципова важливих недоліків, зокрема запропоноване визначення «кіберпростору» в Законі «Про основні засади забезпечення кібербезпеки України» виключає з поля правового впливу автономні автоматизовані системи управління (наприклад, об'єктів атомної енергетики), які, саме з огляду на вимоги безпеки, є автономними.

Надане визначення терміна «кіберпростір» також суб'єктно обмежує «простір» лише інформаційними (автоматизованими), телекомунікаційними та інформаційно-телекомунікаційними системами, тобто автоматизованими системами. Крім того, у Законі не надано визначення терміна «середовище», що призводить до невизначеності у тлумаченні терміна «кіберпростір».

Доведено доцільність у визначенні терміну «*кіберзлочин*» словосполучення «міжнародними договарами» замінити словосполученням «міжнародним правом». Такий підхід забезпечить єдність термінологічного тлумачення на рівні національного та міжнародного законодавства.

Встановлено, що законодавчий зміст терміна *«критично важливі об'єкти інфраструктури (критичні інфраструктурні об'єкти),* не передбачає виділення саме об'єктів такої інфраструктури, а вказує лише на «підприємства,

установи та організації незалежно від форм власності». Тут ми підтримуємо думку тих дослідників, які відстоюють доцільність прийняття Закону України «Про об'єкти критично важливої інформаційної інфраструктури».

Обґрунтовано, що визначення терміна *«кіберзагроза»* не співвідноситься за обсягом інформації, наведеної у терміна «кібербезпека», та не відповідає визначенню цього терміна.

Наведено науково обґрунтовані аргументи, що Закон України «Про основні засади забезпечення кібербезпеки України» радше є дорожньою картою для розробки майбутніх нормативних актів, а не всеосяжним законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам і найкращим практикам.

2. У контексті визначення об'єкта правового забезпечення кібербезпеки України, доведено, що кіберпростір виступає водночас й об'єктом захисту, скажімо, інформаційних ресурсів, відповідних апаратних і програмних засобів тощо, і джерелом загрози для інших об'єктів національної безпеки. Традиційним, у ході визначення об'єкта правового забезпечення кібербезпеки України, є також визначення таких рівнів кібербезпеки, як безпека людини, суспільства й держави, в основу якого покладені конституційні принципи захисту життєво важливих інтересів зазначених суб'єктів. Але стосовно кібербезпеки вбачається доцільним надати пріоритет інтересам держави, позаяк від цього безпосередньо залежатиме й реалізація інтересів особи й суспільства. Тобто, забезпечення кібербезпеки держави є передумовою особистісної та громадської кібернетичної безпеки.

Аргументовано, що визначити об'єкти правового забезпечення кібербезпеки України як завершену систему чи класифікацію не можливо. Така структура є динамічною та мінливою відповідно до національних та глобальних тенденцій змін у кіберпросторі. Тому перед кожною державою постає потреба створення ефективних засобів забезпечення своєї кібербезпеки.

3. Науково обґрунтовано, що систему суб'єктів забезпечення

кібербезпеки держави, людини і суспільства слід розглядати у комплексному взаємозв'язку міжнародних й регіональних організацій, недержавних організацій, галузевих організацій, держави, приватного сектору та безпосередньо громадян. За такого комплексного підходу структуру суб'єктів забезпечення кібербезпеки можна відобразити наступним чином: міжнародній регіональні організації, недержавні організації, галузеві організації, держава, приватний сектор, громадяни.

Запропоновано розробити оптимальні механізми співробітництва між приватним сектором та державними органами у сфері забезпечення кібербезпеки. У цьому контексті виокремлено такі пріоритетні напрями: розвиток кіберрозвідки, аудит кібербезпеки, взаємний обмін інформацією щодо кіберзагроз, заміна НД ТЗІ на ефективніший і сучасніший базовий стандарт і запровадження галузевих стандартів кібернетичної безпеки, створення галузевих центрів реагування на кібернетичні інциденти (SOC) та центри інформаційного обміну про кібернетичні атаки (ISAC), створення незалежних платформ для співпраці – кіберцентрів із метою ефективної протидії кібернетичним загрозам.

У розділі акцентовано увагу, що дискусійні аспекти законодавчого визначення базових категорій можуть слугувати певними причинами деформацій самої мети та предмету правового регулювання, а також неправильного визначення комплексу заходів щодо правового забезпечення кібербезпеки.

4. У розділі на основі системного підходу виділено такі основні джерела кіберзагроз:

– держави, які використовують відповідні кіберзасоби для збирання інформації та розвідувальної діяльності (зокрема, економічне шпигунство задля отримання переваг в економічній, політичній, військовій та інших сферах);

– бізнесові структури: приватні компанії-конкуренти, котрі прагнуть здобути важливі дані щодо опонентів задля отримання ринкових переваг – про

виробництво, ціни, розробки, асортимент тощо;

– кримінальні угруповання, котрі вдаються до кібернетичних атак із метою грошового зиску; засоби, що при цьому застосовуються, найрізноманітніші: фішинг, спам, шкідливі програми для інтернет-крадіжок, комп'ютерного вимагання, викрадення персональних даних тощо;

– міжнародне корпоративне шпигунство, метою якого є економічне, промислове шпигунство, викрадення значних коштів; нерідко користуються послугами хакерів, надаючи їм відповідні засоби;

– мережеві оператори, котрі використовують ботнет (мережу) дистанційно керованих зламаних систем задля розповсюдження спаму, фішингу, провадження узгоджених атак тощо;

– розробники шкідливих програм і програм стеження – окремі особи чи організації, котрі створюють і застосовують указаний продукт із протиправною метою;

– розробники фішингових схем, котрі створюють і застосовують їх для викрадення коштів, персональних даних тощо;

– працівники підприємств (компаній, установ), які мають доступ до внутрішньої конфіденційної інформації (інсайдери), зокрема й до комп'ютерних систем, а тому можуть викрадати дані або завдавати шкоди. До цих суб'єктів належать також некваліфіковані чи халатні співробітники, тимчасово наймані працівники, котрі можуть неумисно зашкодити системі через необережність;

– спамери, котрі використовують схеми фішингу, поширюють у мережі повідомлення, які містять приховані або хибні дані, а також шпигунські й вірусні програми, здійснюють кібератаки (приміром, «відмова в обслуговуванні» – DDoS);

– терористи, котрі ставлять за мету виведення з ладу чи руйнацію об'єктів критичної інфраструктури або ж втручання у їхнє функціонування, що може призвести до значних людських жертв, становить серйозну загрозу національній безпеці через підрив економіки країни, морально-

психологічного стану суспільства. Ця категорія для отримання грошового зиску та важливої інформації також вдається до шпигунських та інших шкідливих програм, фішингу та іншого;

– хакери, котрі зламують закриті інформаційні системи й мережі з різних мотивів. Це може бути перевірка фахових здібностей, самоствердження, демонстрація певної громадянської позиції, отримання незаконного фінансового зиску;

– хактивісти, котрі з метою розміщення матеріалів політичного характеру атакують поштові сервери та веб-сторінки.

5. Аналіз нормативних документів, які стосуються питань забезпечення кібербезпеки нашої держави, різних країн, дав можливість узагальнити та виокремити найбільш значущі для них загрози в цій сфері. Так, статус головних небезпек для національного кіберпростору стратегії більшої частини країн надають:

– кібершпигунству та воєнним діям, які підтримує або про які поінформована держава. Усім технологічно розвиненим країнам та корпораціям доводиться ставати об’єктами кібершпигунства, яке має мету отримати державні або промислові таємниці, персональні дані або іншу цінну інформацію. Так, вкрай резонансною кібератакою стали дії КНДР проти компанії «SonyPictures Entertainment», в результаті чого порушники одержали конфіденційні дані, зокрема інформацію стосовно комерційних операцій фірми;

– використанню глобальної мережі задля терористичних цілей. Терористичні угрупованнями використовують Інтернет, щоб здійснювати пропаганду, збирати кошти і вербувати людей;

– кіберзлочинності: крадіжка персональної інформації та відмивання грошей, одержаних у незаконний спосіб. Злочинці займаються продажом інформації щодо номерів банківських карток, паролів від серверів та шкідливого програмного забезпечення.

Виходячи з аналізу забезпечення кібербезпеки в зарубіжних країнах, у

розділі запропоновано доповнити Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242/2016 у частині вдосконалення основних завдань цього органу. У цьому контексті пропонується розширити пункт 3 указаного Положення, додавши до основних завдань Центру такі:

– впровадження в Україні стандартів безпеки мережевих та інформаційних систем;

– визначення критерії в, за якими буде складатися перелік операторів базових послуг та провайдерів цифрових послуг;

– контроль за дотриманням мережевої нейтральності та міжнародних та європейських стандартів та заборон введення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами;

– аудит системи мережевої та інформаційної безпеки;

– організація та підтримка системи сповіщення про кіберінциденти, системи аудиту й впровадження заходів мережевої та інформаційної безпеки;

– забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема щодо персональних даних та захисту комерційних інтересів операторів та провайдерів.

Основні наукові результати цього розділу викладено також у працях автора: [235-242].

РОЗДІЛ ІІІ
ТЕОЕРТИКО-ПРАВОВИЙ АНАЛІЗ СУЧАСНИХ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ЛЮДИНИ ПІД ЧАС ВИКОРИСТАННЯ КІБЕРПРОСТОРУ

3.1. Системний аналіз правового регулювання кібербезпеки людини

Інформатизація і глобалізація життєдіяльності світової спільноти, опанування людством кібернетичного простору, спричинені цим нові загрози й виклики унаочнили важливість правового забезпечення кібербезпеки людини, суспільства й держави, інформаційної безпеки загалом. Як бачимо, сучасна міжнародно-правова термінологія, як-от «глобальні проблеми», «нові виклики й загрози» тощо, повною мірою притаманна й інформаційній сфері та, відповідно, інформаційно-правовій науці. Що стосується нових викликів і загроз у цій сфері, то пов’язані вони насамперед із терористичними проявами (кібертероризмом), кіберзлочинністю із застосуванням новітніх технологій, розповсюдженням у глобальних мережах контенту, спрямованого на інформаційно-психологічний вплив, залякування користувачів, заклики до насильства, розпалювання расової, міжнаціональної, міжконфесійної та іншої ворожнечі, тощо.

Підтримуємо думку тих учених, які право людини на кібербезпеку відносять до прав четвертого покоління [243-244]. Цей вид прав четвертого покоління в Україні розвинувся з прийняттям у 2016 році Стратегії кібербезпеки України, що в подальшому розвинувся в Законі України «Про основні засади забезпечення кібербезпеки України».

Розглянемо детальніше складову вказаного права – право людини на кібербезпеку, котре в цьому дослідженні визначаємо як закріплену в

законодавстві можливість людини користуватися інформацією, доступ до якої не має законодавчих обмежень, та комплекс державно-правових заходів щодо захисту громадян від шкідливої для них інформації.

Сутність права людини на кібербезпеку полягає в:

1) можливості реалізації «права на забуття», тобто обов'язку оператора пошукової системи мережі Інтернет на вимогу користувача – фізичної особи припинити надання відомостей про покажчики сторінок сайту в мережі, котрі дають змогу отримати доступ до певної інформації про заявника, якщо вона є недостовірною, неактуальною, такою, що втратила для особи значущість, або розповсюджується з порушеннями встановлених законодавством вимог. Це дозволяє особі – користувачу Інтернету видаляти певну інформацію про себе, контролюючи поширення її в мережі;

2) можливості «цифрового спілкування» з державними та самоврядними органами, отримання державних адміністративних послуг в електронному вигляді. У теперішній час ця форма закріплена законодавчо, поступово вдосконалюється й набирає все більшої популярності, дозволяючи громадянам заощаджувати час, матеріальні, фізичні й психологічні ресурси;

3) захисті персональних даних, конфіденційної інформації у процесі користування інформаційним (кібернетичним) простором, здійснення особою своєї цифрової ідентичності. З погляду права така ідентифікація являє собою унікальну сукупність вираженої в цифровій формі інформації про особу, за допомогою якої відбуваються міжособистісні стосунки, правові відносини, реалізуються права й обов'язки. Людина отримує свій унікальний ідентифікатор (код), котрий є одним із засобів захисту інформації від несанкціонованого доступу, що дає змогу безпечно звертатися до органів державної влади, віддалено здійснювати фінансові операції, надсилати користувачам авторизовані повідомлення, провадити інші різноманітні дії в кібернетичному середовищі;

4) захисті інформації, що циркулює в системах інтернет-банкінгу, від несанкціонованого доступу. Останні є досить популярними, позаяк дають

змогу в будь-який час, у будь-якому місці, з будь-якого пристрою, котрий підключений до Інтернету, отримати доступ і здійснювати різноманітні фінансові операції. У цьому разі засобами забезпечення інформаційної (кібернетичної) безпеки особи є аутентифікація особи, застосування цифрового підпису й зовнішніх електронних пристроїв, шифрування інформації тощо;

5) захисті від негативного інформаційного впливу, поширення протиправного контенту (зокрема, і в Інтернеті), що забезпечується дією автоматизованої інформаційної системи ведення й використання бази даних про сайти, котрі містять інформацію, заборонену до розповсюдження в Україні, певне обмеження анонімності в мережі Інтернет тощо.

Зазначимо, що наведений перелік основних складових права людини на кібербезпеку не є вичерпним і закритим. З розвитком інформаційного суспільства й технологічних можливостей кібернетичного середовища він, безперечно, буде видозмінюватися.

З-поміж основних ознак права людини на кібербезпеку варто, на нашу думку, виокремити такі:

1) можливість його реалізації за допомогою застосування цифрових інформаційно-комунікаційних технологій;

2) запобігання інформаційним впливам на особу, спрямованість на захист від несанкціонованого доступу до особистої інформації;

3) передбачення потреби застосування гарантій і правових, і технічних;

4) певна стандартизація реалізаційних процедур;

5) змога дистанційної реалізації.

Стосовно ж кореляції права людини на кібербезпеку з інформаційними і цифровими правами, то вважаємо, що обсяг першого менший, оскільки воно спрямоване на захист винятково особистої інформації від несанкціонованого доступу й запобігання негативним інформаційним впливам на особу. Натомість до цифрових належить права, здійснення яких або відбувається в цифровому середовищі, або спрямоване на забезпечення доступу до нього, а

до інформаційних, крім того, – у сфері пошуку інформації, її отримання, виробництва, передання й розповсюдження.

Як бачимо, право людини на кібербезпеку – це своєрідна, специфічна сукупність прав, котрі реалізуються, зокрема, за допомогою цифрових, інформаційно-телекомунікаційних технологій з метою захисту приватної, особистої інформації від несанкціонованого доступу та запобігання шкідливим впливам на особистість. Формування вказаної сукупності прав належить до четвертого покоління прав людини й зумовлене технологізацією й інформатизацією суспільства.

Підхід до наукової розробки проблематики правового забезпечення кібербезпеки людини передбачає насамперед визначення предмета правового регулювання та його специфіки, аналіз положень вітчизняного й міжнародного інформаційного та іншого дотичного законодавства, а також відповідного понятєво-термінологічного апарату. Таким чином, більш широкий підхід, що ґрунтується не лише на власне правовому регулюванні, а й на питаннях правового забезпечення, вбачається оптимальним для досягнення мети даного дослідження. Мається на увазі вивчення не тільки наявної нормативно-правової бази, ненормативних актів державних органів, а й положень документів стратегічного планування, правозастосовної практики тощо.

Ми погоджуємося з думкою вітчизняного дослідника В. Фурашева, який під «інформаційною безпекою» розуміє «стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через:

− негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації;

− негативні наслідки застосування інформаційних технологій;

− несанкціоноване порушення режиму доступу до інформації з

подальшим її розповсюдженням та використанням» [245, с. 168].

Отже, під *правовим забезпеченням кібернетичної безпеки людини* як складової правового забезпечення інформаційної безпеки взагалі розуміємо сукупність законодавчих, інших нормативних і ненормативних правових актів державних органів, документів стратегічного планування, правозастосовної практики, які стосуються створення умов для втілення в життя суб'єктивного права людини на кібербезпеку, захищеність від внутрішніх і зовнішніх загроз під час користування кіберпростором. Саме відповідні суспільні відносини це і є предметом даного теоретико-правового дослідження, що базується на організаційно-правовій проблематиці, пов'язаній із забезпеченням кібернетичної безпеки людини в динамічних умовах розвитку глобального інформаційного суспільства.

На нашу думку, у теперішній час існує чітка взаємозумовленість між прогресом глобального інформаційного суспільства та ефективністю правового забезпечення кібернетичної безпеки особи. А між тим, останнє має сьогодні низку істотних недоліків. Це, зокрема: лакуни й суперечності наявної нормативно-правової бази, неповне охоплення нею суспільних відносин, що мають регулюватися й забезпечуватися; серйозні проблеми відповідної правозастосовної практики; низька ефективність наявних правових механізмів протидії викликам і загрозам кібернетичній безпеці тощо.

Слід наголосити на особливій правовій природі суспільних відносин, які виникають у глобальному кіберпросторі у зв'язку із протидією загрозам і викликам кібербезпеці особи, суспільства й держави. Ці відносини являють собою вагому частину всього комплексу інформаційних правовідносин, котрі виникають у процесі оперування інформацією (пошуку, отримання, зберігання, передавання, розповсюдження тощо) й регулюються нормами самостійної правової галузі – інформаційним правом.

Вказані відносини мають свої особливості, які вирізняють їх з-поміж інших правовідносин. По-перше, вони виникають, здійснюються і припиняються у процесі обігу інформації. А по-друге, вони складаються

навколо досить специфічних об’єктів, а саме: інформації, інформаційних об’єктів і технологій, кіберпростору, а також феноменів, на які спрямовані інформаційні права та обов’язки.

О. Золотар у своїй докторській дисертації робить справедливий висновок про те, що «розуміння інформаційної безпеки людини як правової категорії повинно ґрунтуватися на комплексності її як соціального явища, а також враховувати її внутрішню будову» [246, с. 13]. На наше переконання таке твердження поправу відноситься й до кібернетичної безпеки.

З урахуванням безумовної потреби дотримання в інформаційних відносинах оптимального балансу інтересів особи, суспільства й держави у цьому дослідженні головна увага приділяється головному суб’єктові вказаних відносин – людині в контексті належного правового забезпечення її кібернетичної безпеки. При цьому вбачається важливим дослідити питання інформаційної право- та дієздатності, тобто інформаційно-правової суб’єктності.

Заслуговує особливої уваги думка відомого вченого В. Пилипчука про те, що «державна інформаційна політика, у т.ч. з питань захисту приватності, прав і безпеки людини в інформаційній сфері, та система інформаційної безпеки мають бути спрямовані на ефективний захист об’єктів національної безпеки: людини і громадянина – їх конституційних прав і свобод; суспільства – його духовних, морально-етичних, культурних, історичних, інтелектуальних та інших цінностей; держави – її конституційного ладу, суверенітету, територіальної цілісності й недоторканності» [247, с. 41].

У контексті інформаційно-правових відносин щодо протидії викликам і загрозам кібернетичній безпеці людини інформаційну правоздатність можна визначити як установлену, гарантовану й захищену державою можливість або спроможність особи брати участь в інформаційних суспільних відносинах. Відтак, у сфері кібернетичної безпеки людина набуває певних юридичних прав, а також обов’язків, що передбачають юридичну відповідальність за практичну реалізацію цих прав.

Натомість, *інформаційну дієздатність* у ролі складової інформаційної правосуб'єктності можна визначити як: спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав, брати на себе певні правові обов'язки, а також нести юридичну відповідальність у разі неправомірної поведінки.

Що стосується другої важливої складової аналізованих правовідносин, пов'язаних із протидією викликам і загрозам кібербезпеці особи, – їхнього об'єкта, то в контексті цього дослідження його можна визначити так: стан захищеності особи від внутрішніх і зовнішніх загроз в інформаційній сфері, при користуванні кіберпростором. Зауважимо, що рівень такої захищеності безпосередньо зумовлює стан забезпечення національних інтересів, істотно впливає на поступ глобального інформаційного суспільства.

Ше один складник правовідносин, що розглядаються є їхній зміст, котрий становлять юридичні права й обов'язки їхніх суб'єктів – особи, суспільства, держави та інших учасників інформаційних правовідносин.

На нашу думку, основними інформаційними потребами особи є реалізація таких прав:

– отримання достовірної інформації про всі сфери життєдіяльності суспільства й держави – діяльність державних та самоврядних органів, судової влади, надзвичайні ситуації, стан демографії, екології тощо;

– відносини з органами держави та самоврядування за допомогою цифрових технологій, отримання адміністративних послуг в електронному вигляді;

– судовий захист на базі системи електронного судочинства;

– використання механізмів цифрової демократії – електронного голосування, мережевої комунікації із владними органами, у тому числі громадський контроль за їхньою діяльністю та можливість впливу на прийняття управлінських рішень;

– цифрові взаємини на ринку фінансових послуг на основі цифрової економіки, інтернет-банкінгу, електронного фінансового документо- та

грошового обігу та інших технологій тощо.

Вважаємо, що такий підхід в умовах глобального інформаційного суспільства є доцільним задля вдосконалення законодавства, котре регулює відносини в інформаційній сфері, а також розвитку міжгалузевого комплексного правового інституту правового забезпечення інформаційної безпеки людини.

Таким чином, при з'ясуванні правової природи відносин у сфері забезпечення кібернетичної безпеки особи слід комплексно дослідити усі перелічені вище її складові – суб'єкт (людина у глобальному кіберпросторі, котра потребує належного правового забезпечення своєї безпеки при користуванні кібернетичним простором), об'єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов'язків усіх учасників зазначених суспільних відносин).

Немає жодних сумнівів, що визначальним правовим чинником при цьому, генератором розв'язання головних правових проблем у вказаній сфері є система прав і обов'язків. У ній втілюються основні принципи взаємин особи й держави, унормовуються правила, стандарти поведінки, які суспільство (через відповідні державні інституції) визнає доцільними, корисними й обов'язковими для своєї нормальної життєдіяльності.

Задля кращого розуміння правової природи правовідносин щодо протидії викликам і загрозам кібербезпеці особи вбачається доцільним звернути увагу на особливості методики їхнього правового регулювання, яка, виходячи із базових методів правового регулювання, набуває в цьому міжгалузевому правовому інституті своїх специфічних, унікальних способів і прийомів. Інституту правового забезпечення кібернетичної безпеки особи, як і всій галузі інформаційного права, притаманна методика правового регулювання, котра діалектично сполучає імперативний і диспозитивний підходи. Отже, особливості методу інформаційного права полягають у поєднанні способів правового регулювання, які визначені принципами й

основними напрямами державної політики у цій сфері.

У своїй «Філософії права» Г.В.Ф. Гегель, погоджуючись із твердженням, що метою держави є щастя громадян, писав: «Це, звісно, правильно: якщо їм зле, якщо їхні особисті цілі не досягаються, якщо вони не бачать, що їх досягнення можливе лише за допомогою держави, то остання стоїть на порцелянових ногах» [248, с. 265]. У цьому контексті Г.Ф. Шершеневич зазначав, що не можна оминати увагою, пригнічувати особисті інтереси, «але головне в тому, щоби узгодити їх з інтересами цілого» [249, с. 111].

Відповідно до гегелівської діалектики будь-який розвиток відбувається як перманентний процес: теза (твердження, або покладання) – антитеза (заперечення цього твердження) – синтез (зняття суперечностей, або заперечення). У результаті синтезу тези й антитези виникає якісно новий стан, який, утім, не означає зникнення його вихідних складників. За Гегелем, зняття суперечності, означає також збереження тези й антитези, але в певній більш високій, гармонійній іпостасі.

Ґрунтуючись на цій методології та всебічному аналізу актуального стану взаємин особа – суспільство – держава, спробуємо виявити чинники внутрішньої суперечливості, ознаки діалектизму, притаманні сучасному інформаційному суспільству. Основними з-поміж них, на нашу думку, є такі:

– суспільна інертність, неспроможність через певні об’єктивні й суб’єктивні причини належним чином скористатися науково-технічними надбаннями;

– зростання кількості й потужності викликів і загроз у процесі розвитку й удосконалення інформаційного суспільства; тобто уразливість і ризики для інформаційного (кібернетичного) середовища випливають із динаміки, перманентного прогресу цього феномену;

– проблематичність сприйняття особою постійно, лавиноподібно зростаючих обсягів інформації, що зумовлює виникнення певних внутрішніх запобіжників, фільтрів, коли людина визначає важливе й потрібне для себе ще перед сприйняттям інформації, підсвідомо її «фільтруючи»;

– проблема достовірності інформації, що циркулює в кіберпросторі, надмірна завантаженість кіберсередовища відвертою дезінформацією, шкідливою чи забороненою інформацією і т.п.;

– проблеми впровадження інформаційних технологій (нерівномірність, недовіра до, скажімо, електронного урядування замість паперового, яке відточувалося багато віків, тощо);

– сприйняття новітніх інформаційних технологій у сфері автоматизації як тимчасових через те, що вони постійно вдосконалюються, допрацьовуються, замінюються більш сучасними тощо, тобто не мають усталеної форми;

– проблема можливості анонімності й водночас ідентифікації суб'єктів кіберпростору в умовах глобалізації, транскордонності інформаційного суспільства.

Вагомим чинником поступального розвитку інформаційного суспільства є якомога повніше залучення до глобальної інформатизації кожного члена інформаційного суспільства – суб'єкта інформаційних відносин, усвідомлення ним тих можливостей і переваг, які несуть інформаційно-телекомунікаційні технології.

Домогтися цього можна тільки в разі забезпечення державою інформаційної, кібернетичної безпеки особи як атрибутивного чинника інформаційного суспільства. Однак, сьогодення свідчить, що рівень такого забезпечення суттєво стримує потенції всебічного прогресу інформаційного суспільства, розвитку і впровадження новітніх інформаційних технологій.

Що стосується конкретних інтересів особи при використанні кібернетичного простору, то це насамперед гарантування доступу до інформації, забезпечення можливості користування величезними можливостями сучасних кібертехнологій, зокрема, механізмами електронної демократії (самоврядування, адміністративні, судові та інші послуги тощо). І саме через брак або ж повну відсутність відповідних гарантій і механізмів забезпечення кібербезпеки особи процеси впровадження кібертехнологій і

розвиток інформаційного суспільства, гальмуються й не отримують належної суспільної підтримки.

Слід зазначити, що сьогодні поряд з такими усталеними безпековими іпостасями, як «національна», «державна», «інформаційна», надзвичайно актуалізувалася, сягнула загальнонаціонального рівня проблема кібернетичної безпеки особи. Для з'ясування сутності цього феномену треба розуміти як його статичні, так і динамічні параметри. При цьому статика, яка характеризує певний «стан», не здатна повною мірою охопити й відобразити сутність явища й відповідного поняття.

З огляду на викладене під *кібернетичною безпекою особи* розуміємо такий стан її захищеності, який визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.

Виникнення й розвиток глобального інформаційного простору, який вбирає в себе всі створені людством інформаційні потоки, актуалізували низку не лише власне технічних питань. Саме існування такого простору породжує також багато проблем морального плану. Постійне зростання вимог до забезпечення інформаційної безпеки особи й зумовлюється глобалізацією й активізацією інформаційних взаємин у сучасному суспільстві.

Отже, позаяк інформаційна держава об'єктивно стає середовищем людської життєдіяльності, то для забезпечення необхідного рівня її безпеки потрібна ефективна система спеціальних заходів. Для своєчасного виявлення і знешкодження наявних та потенційних інформаційних загроз, запобігання їм, ліквідації негативних наслідків у разі їхньої реалізації до комплексу таких заходів мають входити усебічний он-лайн моніторинг електронного врядування. Цілком зрозуміло, що при цьому має дотримуватися ієрархія інтересів особи, суспільства й держави, їхній оптимальний баланс.

Таким чином, результати проведеного аналізу основоположних нормативно-правових актів, останнім часом ухвалених чи висунутих як

проєкти, у сфері захисту особи, суспільства й держави від загроз і негативних впливів в інформаційному просторі дають підстави для висновку про засади правового регулювання інформаційної безпеки особи, що склалися в теперішній час і в умовах систематизації інформаційного законодавства потребують усвідомлення важливості й відповідної уваги до цього інституту інформаційного права з боку законодавчої влади. Не зайвим убачається підкреслити небезпеку при вирішенні глобальних безпекових питань держави й суспільства загалом неоминути при цьому увагою головну складову інформаційної безпеки – кібернетичну безпеку людини, кожної окремої особи.

В умовах постійного розвитку глобального інформаційного суспільства проблема правового забезпечення кібербезпеки особи набуває нових сенсів. Сьогодні безпековий чинник стає одним із найважливіших, якщо не визначальним, з-поміж факторів, котрі зумовлюють саму можливість існування інформаційного суспільства, яке передбачає не стільки власну долученість кожного до інформатизаційних процесів, скільки активну участь в них. Це означає не лише позитивне ставлення особи до розвитку й удосконалення інформаційно-комунікаційних технологій, а й чітке усвідомлення доцільності й корисності їх використання, налаштування на їх застосування у своїх інтересах. Водночас, як засвідчив аналіз інформаційних відносин, їх суб’єкти нерідко ставляться до цих інформаційних ресурсів, інформаційно-комунікаційних технологій та їхніх можливостей як до руйнівних, якщо й не шкідливих, то принаймні таких, що не обіцяють особливої користі.

Коло інтересів людини в умовах функціонування інформаційної держави досить широке. Так, завдяки розвитку механізмів електронної демократії особа має змогу реалізувати свою громадянську активність на новому рівні міжособистісних взаємин, стосунків з органами державної влади й місцевого самоврядування, громадськими, комерційними та іншими структурами. Це також можливість шляхом запровадження електронного врядування спрощеного отримання якісних адміністративних послуг в

електронному вигляді, реалізація права на правовий захист завдяки, зокрема дійовому електронному судочинству. Уже сьогодні більшість людей визнала безумовну зручність інтернет-банкінгу, електронної комерції та інших аспектів розвитку цифрових інструментів фінансово-кредитних відносин. Про повноту реалізації інформаційних прав особи в умовах сучасних мережевих ЗМІ та інших електронних джерел годі й говорити.

Ефективна реалізація цих та інших інформаційних інтересів особи можлива лише в разі системного вдосконалення відповідного законодавства з обов'язковим урахуванням інформаційно-безпекових аспектів. Якщо ж відсутні або не налаштовані належним чином механізми й інструменти взаємодії громадян з електронною державою, то виникає системний розлад в інформаційних відносинах. Це аж ніяк не сприяє формуванню повноцінного інформаційного суспільства, де кожен його суб'єкт (колективний чи індивідуальний) усвідомлює корисність і потенції інформаційно-телекомунікаційних технологій, має реальну змогу втілити свої інформаційні права і свободи, будучи при цьому захищеним від внутрішніх і зовнішніх викликів і загроз. Сьогодні розвиткові інформаційного суспільства, більш активному впровадженню названих цифрових технологій, заважає певна недовіра до них громадян через брак ефективних механізмів і надійних гарантій забезпечення інформаційної (кібернетичної) безпеки особи.

Так, усе більш актуальною стають сьогодні проблеми достовірності, правдивості інформації, що надходить із різних джерел, їхньої переобтяженості дезінформаційними матеріалами, шкідливою, забороненою інформацією. Чимало питань виникає і навколо реалізації права на недоторканність приватного життя в умовах бурхливого розвитку інтернет-комунікацій, можливості унормування права на так зване «цифрове забуття» та інших подібних проблем.

Крім того, розвиток, ускладнення інформаційно-телекомунікаційних технологій нерідко супроводжуються відставанням безпекових аспектів, а тому виникає ситуація, коли суб'єкти інформаційних відносин не можуть

адекватно протистояти сучасним кібернетичним атакам. Передувсім це стосується пересічних інтернет-користувачів.

Відтак, створення ефективних механізмів захисту інформаційних прав і свобод людини вбачається одним із невідкладних завдань у сфері вдосконалення вітчизняного законодавства, адже можливість суб'єктів інформаційних відносин захищати свої права, свободи та інтереси, має випливати із самого факту функціонування електронної держави. Вважаємо, що для втілення в життя ідеї інформаційної безпеки особи потрібне побудова комплексної моделі інформаційної безпеки. Зробити це можна шляхом створення *Концепції інформаційної безпеки особи*, котра містила би провідні принципи й завдання державної політики у цій сфері, напрями, механізми й очікувані результати її реалізації.

Упевнені, що ухвалення такої Концепції сприятиме формуванню сприятливого інформаційного (кібернетичного) середовища, а саме: оптимізації інформаційних відносин загалом, підвищенню відповідальності держави за забезпечення й реалізацію особою своїх інформаційних прав, свобод і законних інтересів в умовах глобального інформаційного суспільства.

Проблеми інформаційної безпеки особи безпосередньо пов'язані з таким важливим аспектом, котрому слід, на нашу думку, приділити пильну увагу, як формування культури інформаційної безпеки особи. Зробити це можна шляхом вироблення й удосконалення знань, умінь і навичок, компетенцій і здібностей, розвитку у людей правової свідомості, відповідального ставлення до питань користування інформаційно-телекомунікаційними технологіями, кібернетичним простором.

3.2. Критерії класифікації загроз безпеці людини у кіберпросторі

Широко застосовуване сьогодні поняття «інформаційний» стосовно сучасного суспільства замінило собою цілу низку термінів на його позначення, як от: постіндустріальне, постбуржуазне (пост капіталістичне), постринкове, пост радиційне, постісторичне, технотронне, програмоване, компетентне (засноване на знаннях – «the knowledgeable society») [250], конвенціональне [251] тощо. Поняття «постіндустріальне», на думку Д. Белла, є більш змістовним для означення суспільства, натомість його характеристика як інформаційного дозволяє надати поняттю точнішого специфічного навантаження. І хоча це «навантаження» учений вважав руйнацією понять, якими зазвичай послуговувалися для аналізу суспільних відносин, у своїх працях він користувався обома термінами – постіндустріальне суспільство й інформаційне суспільство [252].

У свою чергу, М. Кастельс пропонував користуватися в таких випадках терміном «інформаціональне суспільство». Дослідник уважав, що інформація, інформування в сенсі передання певного знання завжди відігравали важливу роль, тоді як для відображення певної атрибутивної властивості особливої форми соціальної організації більше підходить термін «інформаціональний». Зазначена властивість полягає в тому, що в теперішній історичний проміжок усі способи транслювання інформації перетворилися на підстави економіки, структурування суспільства та здійснення владних повноважень [253, с. 42-43].

За такої досить значної непослідовності концептуальних підходів деякі дослідники визначають інформаційне суспільство як «високу стадію розвитку постіндустріального суспільства» (Е. Масуда) [254], «розвинене індустріальне суспільство (У. Мартін) [255], «електронно-цифрове суспільство» (Д. Тапскотт) [256].

Як бачимо, розвиток інформаційного суспільства має нелінійний характер та іншу специфіку, зокрема:

– взаємозалежність кількості та якості інформації;

– складність розрізнення достовірної та хибної (неправдивої, вигаданої) інформації;

– брак надійних критеріїв перевірки достовірності інформації;

– маніпулятивний вплив хибної інформації на індивідуальну та суспільну свідомість;

– стреотипне сприйняття інформації, хибні, фальшиві інформаційні цінності;

– переривчастість (атомізація) інформаційного середовища, яка зумовлює серйозні ризики у сфері інформаційної безпеки.

Ускладнення інформаційних відносин зумовлює виникнення різноманітних інформаційних посередників, котрі відіграють роль зв'язкових між окремим користувачем з його особистим простором та інформаційним полем у глобальному інформаційному середовищі. У такому полі інформаційної взаємодії, в якому змушена діяти людина, створюються інформаційні примари (фантоми), інформаційні артефакти та інформаційні сурогати. Спочатку ці інформаційні фантоми співіснують з реальністю, врешті-решт витісняючи останню, залишаючи натомість сурогатну квазіінформаційну завісу. Якщо людина не помічає цього, вона починає керуватися правилами цієї хибної реальності. Таким чином, можна стверджувати, що новостворене інформаційне суспільство сформувало й нову дійсність – віртуальну реальність.

Відтак, створення глобального інформаційного суспільства, нового світу, де усі соціальні процеси об'єднані в усеосяжні форми інформаційно-комунікативної взаємодії й інформаційного обміну спричинило те, що включення розрізнених до того елементів соціуму, різноманітних устроїв і способів господарювання в єдину загальну інформаційну картину світу, стало однією із фундаментальних цінностей цього світу й, відповідно, його інформаційної картини. Іншими словами, інтегративні концептуальні чинники перетворилися на атрибутивні цінності світу інформаційного суспільства. І в

цій іманентній системі цінностей всеохоплююча інформаційна взаємодія, якою охоплені відокремлені раніше форми соціальної комунікації, виступає як цілісна картина світу. Тому на вказаному етапі розвитку людства показником розвиненості, інноваційності, цивілізованості врешті-решт, стає включеність, інтегрованість у цілісний інформаційний світ.

Стосовно суспільства вказаний вище показник передбачає високий рівень розвиненості інформаційно-комунікативної інфраструктури, відповідних техніки й технологій, поширення сучасних цифрових технологій на всі сфери життєдіяльності соціуму. Зазначені вище рівні соціального розвитку не є суто технічними й технологічними. Аби вони такими стали, потрібні належні соціально-економічні умови – розвиток науки й інноваційного виробництва, високоякісна освіта, розвинена інфраструктура забезпечення вказаних процесів (медична, соціальна, правова та ін.). Утім, і виконання цих умов замало, позаяк втілення в життя цього цивілізаційного поступу неможливе без низки базових чинників: побудови правової держави з рівними для всіх правами й можливостями; вдосконалення усієї сукупності соціальних відносин, загальної культури суспільства, політичних, державних і громадських інституцій, які забезпечують вільний і всебічний розвиток особистості.

Що стосується особистості, то, крім високої освіченості й загальної культури, для її «вписування» в єдину інформаційну картину світу необхідні такі властивості, як інформаційна компетенція, комп’ютерна (цифрова) культура, спроможність і бажання кожної людини не бути лише пасивним «нейтроном» інформаційної взаємодії, а стати її активним, творчим суб’єктом, «електроном» інформаційної соціальності. До єдиної глобальної системи інформаційного світоустрою людина має увійти чинником вільного й творчого особистісного розвою як запоруки відповідного розвитку всієї світової спільноти.

Один із провідних науковців та дослідників інформаційного права О. Золотар серед пріоритетів належного рівня забезпечення інформаційної

безпеки людини називає «належний рівень інформаційної культури, тобто теоретичної та практичної підготовки особистості, за якого досягається захищеність і реалізація її життєво важливих інтересів та гармонійний розвиток в умовах інформаційного суспільства незалежно від наявності інформаційних загроз» [257, с. 77].

Саме вказані консолідуючі чинники, котрі стосуються не лише суспільства загалом, а й кожної людини, є незаперечними фундаментальними цінностями інформаційного суспільства як сучасного етапу цивілізаційного розвитку людства. При цьому більшість проблем щодо інформаційної безпеки особи й соціуму на етапі інформаційного суспільства розв'язується за допомогою саме цих незаперечних фундаментальних цінностей.

Ще одна базова властивість інформаційного світу – інноваційність. Специфікою інформаційної епохи є вибухове зростання нового знання. Адже сучасність вимагає, щоби здобуті наукою знання негайно втілювалися в техніці, технологіях, виходили продуктом на світові ринки, а базисом будь-якого знання є інформація.

В інформаційну епоху однією із найважливіших цінностей стає оволодіння інноваційними знанням і технологіями. Їх величезний потенціал здатен докорінно трансформувати економіки країн. Лавиноподібне поширення заснованих на інноваційному знанні інформаційних технологій, їх активне застосування в організації економіки, у виробництві та споживанні, фінансовій та інших сферах виводять відповідні знання в лідери в ринковій конкуренції.

Про те, що інновації є не просто популярним віянням сучасності, а однією із фундаментальних цінностей інформаційної епохи, може свідчити хоча б різке зростання попиту на високотехнологічну інноваційну продукцію. Знаннєва економіка базується на найпрогресивніших, найсучасніших, інноваційних досягненнях, а стрімке впровадження відповідних технологій сприяють тому, що найважливішими складовими сучасного ринкового продукту (товарів, послуг) стають знання й інноваційність.

У теперішній час економіка все більше тяжіє до сфери надання послуг, а не, як раніше, до товарного виробництва. Інформаційна епоха зумовлює зміщення пріоритетів від матеріальної товарної форми, фізичного існування засобів виробництва, капіталів, техніки тощо до інноваційно-технологічної, тобто інтелектуальної, розумової, знаннєвої, інформаційної. Позаяк, сучасна економіка все більше охоплює увесь світовий простір, долаючи географічні перешкоди й національні кордони, як зазначає багато вітчизняних і зарубіжних фахівців [258]. Відтак, економіка, заснована на знаннях, є передовсім економікою епохи інформаційної, економічної й культурної глобалізації.

Плюралізм як базова цінність інформаційної епохи означає рівне співіснування, багатоманітність поглядів, ідеалів, ідеологій, підходів до шляхів розвитку суспільства тощо. Його цінність полягає в урахуванні варіативності шляхів розвитку, соціального прогресу, соціальної динаміки.

Інформація, поняття якої наприкінці 1920-х років запровадив у науковий обіг американський дослідник Р. Хартлі як кількісний показник «відомостей, що поширюються технічними каналами зв’язку» [259], є безумовною цінністю інформаційного світу. Проте, сакральний зміст поняття «інформація» не розкрито до цих пір. Відома та загальноприйнята теорія Клода Шеннона [260], з урахуванням сучасного технологічного прогресу та перенасичення інформацією, характеризується формальним, чи навіть абстрактним трактуванням інформаційних взаємозв’язків. Основу такого твердження складає гіпотеза про те, що у теорії К. Шеннона сама цінність інформації для споживача не береться до уваги. Підтвердженням чого є й те, що сам дослідник назвав свою теорію «математична теорія зв’язку», відповідно до якої повідомлення – певні кодові пересилання передавача, а не сам зміст повідомлення. Сьогодні людство активно впроваджує концепції «екології інформації» та «інформаційної гігієни». Даний етап інформаційного розвитку людства продукує розвиток фази змістовного аналізу інформації, а не просто відповідного набору кодових значень. З упевненістю можна констатувати, що

людство перейшло в епоху, основною характеристикою якої є цінність інформації, яка енергетично збагачує та дає можливість реалізувати мету. Все інше буде на кшталт інформаційного шуму та марних (порожніх) даних.

У теперішній час термін «інформація» і в науці, й у широкому вжитку може набувати найрізноманітніших значень. За влучним висловом Т. Стоуньєра, інформаційне суспільство все ще не дійшло єдиної думки про те, що таке інформація [261]. Утім, не викликає сумнівів міждисциплінарний характер цього поняття, яке застосовується практично в усіх галузях сучасних природничих і соціальних, технічних і гуманітарних, теоретичних і прикладних наук.

З-поміж множини підходів до розуміння інформації в контексті її цінності для інформаційного суспільства можна виокремити три провідних. Це, по-перше, так званий антропно-комунікативний підхід, тобто тлумачення інформації у сфері спілкування як засобу загальнонаукового усвідомлення міжлюдських соціальних зв'язків і відносин. Другий, функціональний, підхід визначає інформацію як пов'язану з упорядкуванням взаємодій властивість самоорганізуючих систем. Нарешті, атрибутивний підхід розглядає інформацію як показник такої властивості усіх матеріальних систем, як гетерогенність розподілу матерії та енергії.

Як бачимо, за таких підходів до тлумачення інформації вже із самого її поняття випливає можливість порушень інформаційної (кібернетичної) безпеки, тобто інформаційних ризиків. Інформація, яка охоплює усі сфери життєдіяльності суспільства, створює умови інформаційної нерівності, коли розподіляється відповідно соціально-статусних, ресурсних та матеріальних чинників. А така нерівність значною мірою зумовлює виникнення інформаційних ризиків, порушення інформаційної безпеки. Це, зокрема, стосується негативних впливів окремих інформаційних ресурсів маніпулятивного характеру, вторгнення в особистісний інформаційний простір, кібернетичної злочинності та інших порушень інформаційних прав людини.

Таким чином, інформаційна безпека людини, суспільства й держави в усіх її аспектах є найважливішою світовою цінністю інформаційної епохи.

Наведені міркування стосовно інформаційної картини світу, застосування міждисциплінарної методології як підґрунтя вивчення проблем інформаційної безпеки втрачає сенс без з'ясування «локації» людини в цьому «живописі». Осягнення місця особи у глобальному інформаційному просторі сучасного суспільства пов'язане зі з'ясуванням сутності здатної до критичного мислення людини інформаційної епохи, яка включена у глобальні інформаційні комунікації, у філософському та соціальному сенсі.

Важливість такого осягнення важко переоцінити, позаяк це дає змогу виявити нові системні відносини, котрі виникають в інформаційну епоху у двоєдності людина – суспільство, відповідні нові властивості як людини, так і соціуму.

Беручи за основу викладений теоретичний дискурс, розглянемо безпосередньо критерії класифікації загроз безпеці особи в кіберпросторі.

Існує декілька критеріїв класифікації форм і видів загроз безпеці людину в глобальному кіберпросторі. Так, за *впливом на національну свідомість*, можна виокремити загрози, спрямовані на:

1) вплив на свідомість особи, її психологічний стан, психіку;

2) шкідливий для здоров'я людини вплив шляхом, наприклад, пропагування й поширення заборонених лікарських препаратів тощо;

3) заволодіння приватною інформацією особи для її подальшого протиправного використання;

4) пропагування у всесвітній мережі ідеології, радикалізму, тероризму і т.п.;

5) зазіхання на статеву свободу й відповідну недоторканність особи;

6) шахрайства у фінансовій сфері;

7) формування антисуспільних поведінкових зразків тощо.

Загрози кібербезпеці людини, які посягають на національні цінності – ще одна із найважливіших основ їхньої класифікації. З-поміж таких джерел можна виокремити наступні:

1) діяльність зловмисників і злочинних угруповань, спрямовану на викрадення приватної особистої інформації, персональних даних людей, заволодіння чужим майном за допомогою шахрайства у кіберпросторі;

2) терористичну діяльність за допомогою інформаційно-телекомунікаційних технологій різноманітних екстремістських організацій (етнічних, релігійних, націоналістичних тощо). Йдеться, зокрема, про інформаційно-психологічний вплив, особливо на молодь, формування відповідних настроїв;

3) діяльність зловмисників і злочинних угруповань, спрямовану на поширення у глобальному кіберпросторі порнографії, зокрема дитячої, пропозицію так званих інтимних послуг та інших різноманітних форм статевого насильства та збочень;

4) діяльність зловмисників і злочинних угруповань, спрямовану на протиправний обіг наркотиками й психотропними засобами, торгівлю забороненими для використання чи вільного обігу лікарськими препаратами, зброєю, людьми та їхніми органами чи тканинами тощо;

5) так би мовити, «аутозагрози», тобто небезпеку, що виходить від самих користувачів через їх власні помилки, недостатню технічну обізнаність, розуміння специфіки інформаційно-кібернетичної сфери тощо.

За *розташуванням джерела загрози* щодо об’єкта розрізняють загрози внутрішні та зовнішні. Внутрішні загрози виходять від самої людини, приміром, коли вона власноруч надає доступ до своєї приватної інформації необмеженому числу користувачів соціальних мереж. Прикладом зовнішніх стосовно об’єкта загроз можуть слугувати численні варіанти зламу ПЕОМ з метою заволодіння паролями, персональними та іншими даними тощо.

За такими критеріями, як *характер впливу, природа виникнення* виділяють умисні й ненавмисні загрози інформаційній безпеці людини.

Неумисні, випадкові загрози виникають, скажімо, через технічні розлади, тоді як умисні – це цілеспрямовані дії з метою створення небезпеки, завдання шкоди, котрі призводять до негативних для особи наслідків (наприклад, розповсюдження через Інтернет забороненої для оприлюднення інформації).

Для протидії подібним загрозам доцільним може бути створення Єдиної автоматизованої інформаційної системи доменних імен, покажчиків сторінок сайтів в інформаційно-телекомунікаційній мережі «Інтернет» і мережевих адрес, що дозволяло б ідентифікувати сайти в інформаційно-телекомунікаційній мережі «Інтернет», які містять інформацію, розповсюдження якої в Україні заборонене.

Окремою підставою класифікації загроз є *джерела загроз в Інтернеті* – усередині всесвітньої мережі, а саме:

– небезпечні сайти; зазначимо, що в Інтернеті існує низка пошукових сервісів, котрі містять інформацію стосовно рівня довіри до певних сайтів;

– шкідливе програмне забезпечення, спам-розсилання, фішингові сайти;

– шахрайські сайти, котрі «просуваються» задля отримання незаконного фінансового зиску (фіктивні інтернет-магазини, так звані псевдовірусники, фінансові піраміди тощо);

– інтернет-ресурси, спрямовані на індивідуальний інформаційно-психологічний вплив, передувсім на молодого, чи юного користувача; це, зокрема, численні, чати й форуми, котрі використовуються сексуальними збоченцями й маніяками, різноманітні порносайти, веб-сайти, де пропагується кіберсуїцид та узгоджені самогубства, тощо.

Класифікують *загрози* кібернетичній безпеці людини й *у межах окремих правових інститутів*. Так, в інституті персональних даних виокремлюють такі загрози:

– упровадження й використання операторами інформаційно-кібернетичних технологій отримання, накопичення й розповсюдження інформації, котра стосується суб’єктів приватної, персональної інформації, спрямування яких не відповідає проголошеній меті їх збирання;

– розроблення у вітчизняному законодавстві в інформаційно-кібернетичній сфері нормативно-правових актів, які містять положення, що суперечать Закону України «Про захист персональних даних»;

– збільшення кількості випадків протиправного оперування інформацією стосовно особливо уразливих аспектів особистих даних, як-от: персональні дані неповнолітніх, біометричні, медичні та інші види спеціальних категорій приватних даних тощо;

– спонукання довільного розповсюдження персональних даних у кіберпросторі користувачами соціальних мереж і т.п.

Варто також зазначити перманентне виникнення *новітніх загроз* кібернетичній безпеці людини, пов'язаних з розвитком інформаційно-кібернетичних технологій. Серед «новоспечених» небезпек, які можна віднести до цієї категорії, варто назвати: загрози конфіденційності персональних даних, спричинені активною рекламою онлайн-торгів RTB (Real-Time Bidding); загрози від специфічних файлів кукі (від англ. – пиріжок), які містять певне «досьє» на користувача; загрози у сфері створення та обігу віртуальної валюти Bitcoin тощо.

У цьому контексті слід особливу увагу приділити проблемі інформаційного впливу на особистість, з-поміж форм якого відзначимо цілеспрямовану дезінформацію, а також інформаційно-психологічні впливи – процес цілеспрямованого виробництва й розповсюдження інформаційного продукту, покликаного чинити вплив на людську психіку (приміром, погрози насилля або заклики до насильства, що спричиняє у людини непевність і побоювання за свою особисту безпеку).

Ми цілком погоджуємося з позицією доктора юридичних наук Є. Скулиша, який обґрунтував доцільність виокремлення інформаційно-психологічної безпеки людини у системі інформаційної безпеки як самостійного напряму. У розрізі даного вчений визначив наступні характерні чинники: «у зв'язку з переходом до інформаційно-комунікативного суспільства, збільшенням масштабів і ускладненням змісту та структури

інформаційних потоків та всього інформаційного середовища, багатократно посилюється його вплив на психіку людини, а темпи цього впливу стрімко зростають. Це визначає формування нових механізмів захисту людини від інформаційно-психологічних впливів, а суспільства – від глобальних інформаційних втручань; взаємодія психіки людини з інформаційним простором відрізняється якісною специфікою і не має відповідних аналогів серед інших типів структур (технічних, соціальних, соціотехнічних тощо); людина та її свідомість – центральна мета інформаційного впливу. Від окремих осіб, їхніх взаємозв'язків і взаємин залежить нормальне функціонування соціально-політичної системи» [262, с. 174].

Підкреслимо, що інформаційно-психологічні впливи можуть мати й позитивне, й негативне спрямування. Серед останніх можна навести брехливу, спотворену чи неповну інформацію, котра підміняє реальні події пропагандистськими вигадками, ідеологічними міфами. Це – так звані «інфологеми», які мають також здатність до самостійного примноження, розширеного самовідтворення.

Як зазначалося вище, виклики й загрози безпеці людини в інформаційній сфері виявляються, зокрема, усередині окремих правових інститутів. Наприклад, з-проміж новітніх викликів і загроз інтернет-банкінгу як складовій частині цифрової економіки можна назвати численні схеми «швидкого збагачення», фішинг, ризиковані інвестиції, «нігерійські листи», віртуальне працевлаштування, віртуальна медична допомога, мережеві банди, «мережеве жебракування», гарячі торговельні точки, ботнети тощо.

У межах теоретико-методологічного дослідження проблематики правового забезпечення кібернетичної безпеки людини неможливо оминути увагою питання таємниці приватного життя, особистих даних, у тому числі й дійового захисту персональних даних. Те, що загроза інформаційній безпеці у приватному й сімейному житті людини, при захисті її персональних даних зростає, не викликає сумнівів. Це зумовлене тим, що в зазначених сферах правові норми застосовуються здебільшого формально. Натомість, подальший

розвиток глобального інформаційного суспільства все більше актуалізує проблему захисту персональних даних, потребуючи пильної уваги як законотворців, так і правозастосовної практики.

Нагальність і важливість досліджуваних питань дає всі підстави стверджувати про необхідність систематизації галузевого законодавства і розроблення у межах останньої кодифікованого правового акта – *Інформаційного кодексу України*. Прогнозуючи структуру особливої частини майбутнього Інформаційного кодексу України, а саме інституту правового забезпечення кібернетичної безпеки, виділимо у його складі низку субінститутів – правового забезпечення кібернетичної безпеки людини, правового забезпечення кібернетичної безпеки суспільстві, правове забезпечення ікібернетичної безпеки держави. Тобто, на нашу думку, сукупність правових норм, які регулюють питання кібернетичної безпеки людини, створює самостійний правовий інститут, котрий в Інформаційному кодексі має посісти окреме місце у вигляді відповідного підрозділу. Проблематика гарантування інформаційних прав та інтересів, їх захисту, установлення режимів поширення інформації, визначення видів інформації, котра надається за згодою осіб, та інші питання також, на наш погляд, потребують окремої правової регламентації та наукового осмислення.

Відтак, пропонуємо до системи документів стратегічного планування включити Концепцію кібернетичної безпеки людини такого змісту (структури):

1. Загальні положення (обґрунтування актуальності).
2. Провідні принципи державної політики у сфері забезпечення кібернетичної безпеки особи.
3. Основні завдання й механізми реалізації державної політики у сфері забезпечення кібернетичної безпеки особи.
4. Прогнозовані результати реалізації Концепції. Цільові показники.

Вважаємо, що ухвалення й утілення положень цієї Концепції сприятиме формуванню позитивного кібернетичного простору, оптимізації

інформаційних відносин у суспільстві, підвищенню відповідальності держави за забезпечення законних інформаційних інтересів особи.

Прогнозованими результатами реалізації Концепції вбачаються:

– зведення до мінімуму шкідливих для людини інформаційно-безпекових чинників;

– підвищення рівня правової культури у сфері інформаційної безпеки особи;

– налагодження чіткої взаємодії різних державних інституцій, відомств у забезпеченні інформаційної безпеки особи, втіленні механізмів її реалізації тощо.

Змістовне наповнення пропонованої Концепції вбачаються таким:

1. Мета, завдання й механізми реалізації державної політики у сфері забезпечення кібернетичної безпеки особи.

Метою державної політики в зазначеній сфері є формування в Україні системи правового забезпечення кібернетичної безпеки особи, котра складається з нормативно-правової бази для правового регулювання відповідних інформаційних суспільних відносин, загальновизнаних принципів і міжнародно-правових норм, правозастосовної практики щодо реалізації суб'єктивних прав людини на захист від внутрішніх і зовнішніх загроз у кібернетичній сфері.

На сьогодні розвиток глобального інформаційного суспільства, ефективне правове забезпечення інформаційної безпеки особи гальмуються постійними трансформаціями викликів і загроз у цій сфері, тобто такими чинниками:

– підвищенням інтенсивності викликів і загроз, зростанням кількості правопорушень в кібернетичній сфері;

– ускладненням правових проблем ідентифікації й аутентифікації особи;

– недосконалістю інформаційно-телекомунікаційних технологій, можливістю технічних розладів і збоїв, уразливістю баз даних фізичних осіб у системах електронного врядування й судочинства;

– цифровою нерівністю;

– недосконалістю систем цифрової економіки.

У цьому контексті кібернетична безпека особи розуміється як стан її захищеності, котрий характеризується зведенням до мінімуму для людини ризиків у вигляді внутрішніх і зовнішніх інформаційних викликів і загроз в умовах глобального інформаційного суспільства, здатністю протистояти їм за допомогою культури інформаційної безпеки, формуванням і втіленням державної політики, спрямованої на створення належних умов для реалізації прав і свобод людини, а також забезпечення її безпеки в інформаційній сфері.

До інформаційних інтересів людини належать: реалізація її конституційних прав і свобод на доступ до інформації, на її використання з метою здійснення будь-якої діяльності, не забороненої законом, фізичного, інтелектуального й духовного розвитку; захист інформації, яка стосується сфери особистої безпеки.

Потребують удосконалення правові засоби й механізми забезпечення безпеки людини в кібернетичній сфері, серед яких: інструментарій ідентифікації й аутентифікації особи в кібернетичному просторі (засоби біометричної ідентифікації, захисту інформації, її цілісності й достовірності, захисту персональних даних та ін.). Належить також ужити дійових узгоджених організаційних, інформаційно-аналітичних, економічних, науково-технічних та інших заходів щодо прогнозування інформаційних загроз, запобігання їм, їх виявлення, стримування, відбиття, ліквідації наслідків у разі їхньої реалізації.

Нині найбільш нагальним убачається вдосконалення сучасних технологій на кшталт інноваційної універсальної платформи Blockchain, квантової криптографії, а також утілення в життя державної політики розвитку цифрової економіки, правового регулювання обігу криптовалюти тощо.

2. Принципи державної політики у сфері забезпечення кібернетичної безпеки особи.

У Концепції правового забезпечення кібернетичної безпеки особи

провідними принципами формування відповідної державної політики мають, на нашу думку, бути такі: визнання людини як головного й найуразливішого суб'єкта інформаційних відносин; відповідальності держави в інформаційній сфері; відповідності безпекових організаційно-правових заходів реальним і потенційним викликам і загрозам в інформаційній сфері; контролю за реалізацією інформаційної безпеки людини, зокрема шляхом залучення до участі в захисті інформаційних прав і свобод громадських організацій і об'єднань громадян, постійного моніторингу стану захищеності особи від внутрішніх і зовнішніх інформаційних викликів та загроз.

3. Пріоритети державної політики у сфері забезпечення кібернетичної безпеки особи.

Основними шляхами реалізації політики Української держави у сфері забезпечення кібернетичної безпеки особи вбачаються:

– удосконалення Закону України «Про основні засади забезпечення кібербезпеки України» в контексті захисту життєво важливих інтересів людини від внутрішніх і зовнішніх загроз в кібернетичному просторі;

– створення кібернетичного середовища, безпечного для користувачів;

– протидія інформаційно-психологічним впливам, розповсюдженню інформації з обмеженим доступом, даних, поширення яких заборонене в Україні, а також іншим небезпекам для людини в кібернетичному просторі;

– нормативне закріплення, в контексті реалізації принципу недоторканності приватного життя, в інформаційному законодавстві України (закони «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах» та ін.) правового механізму моніторингу стану захищеності особи від внутрішніх і зовнішніх загроз в інформаційному (кібернетичному) середовищі;

– урахування моніторингу інформаційної безпеки особи при поточному й перспективному плануванні діяльності Кабінету Міністрів України як постійного спостереження органів державного управління та місцевого самоврядування, громадських та інших організацій та об'єднань громадян за

станом захищеності інформаційної безпеки людини з метою виявлення джерел внутрішніх і зовнішніх загроз, аналіз правозастосування у цій сфері та вдосконалення на цій основі відповідної законотворчої діяльності;

– з метою здійснення організаційних функцій з моніторингу стану інформаційної безпеки особи, аналізу та інформування про реальні й потенційні та загрози ризики, підготовки систематичних доповідей про стан правового забезпечення інформаційної безпеки особи, розгляду скарг громадян щодо порушень їхніх інформаційних прав і вжиття належних заходів запровадити інститут Уповноваженого із захисту прав людини в інформаційній сфері при Президентові України.

4. Цільові показники реалізації Закону України «Про основні засади забезпечення кібербезпеки України».

Такими індикаторами ефективності втілення в життя положень Закону мають, на нашу думку, бути: ступінь загроз та ризиків кібербезпеці людини; рівень правопорушень проти особи у глобальному кібернетичному середовищі; рівень інформаційно-правової культури населення.

На підставі викладеного спробуємо запропонувати визначення поняття «кібернетична безпека людини», яке, на наш погляд, варто навести у вказаний Закон. Кібернетична безпека людини – такий стан її захищеності в умовах глобального кібернетичного суспільства, який характеризується: мінімізацією для людини ризиків, внутрішніх і зовнішніх викликів і загроз у кібер просторі, а також здатністю їм протидіяти; спроможністю держави й суспільства у процесі забезпечення кібернетичної безпеки людини гарантувати реалізацію її інформаційних прав і свобод.

Наведена дефініція випливає з виявлених у цьому дослідженні взаємних залежностей рівня забезпечення кібернетичної безпеки особи та результативністю реалізації її прав і свобод в інформаційній сфері, а також із його атрибутивних ознак, як статичних, так і динамічних.

Зазначимо, що, на нашу думку, з огляду на багатоаспектність поняття кібернетична безпека особи, яка зумовлена специфікою впливів внутрішніх і

зовнішніх інформаційних загроз, його не варто тлумачити розширено, виокремлюючи при цьому безпеку інформаційно-технічну, психологічну й ідеологічну. Адже врешті-решт усі ці іпостасі кібернетичної безпеки особи дуже тісно й часто нерозривно взаємозв'язані.

У сучасних умовах глобалізованого інформаційного суспільства у процесі регулювання інформаційних відносин слід неодмінно розуміти вагомість і враховувати розвиток правової свідомості як втілення ставлення кожного суб'єкта цих відносин, суспільства загалом до всіх інформаційно-правових проявів, формування усвідомленої оцінки правомірної та неправомірної поведінки. Відтак, вважаємо за потрібне підкреслити непересічне значення у сучасному суспільному житті правової свідомості, як загалом, так і стосовно досліджуваної нами проблематики інформаційної безпеки особи в глобальному інформаційному суспільстві при використанні глобального інформаційного (кібернетичного) простору.

Що стосується культури кібернетичної безпеки особи, то під нею, на наш погляд, слід розуміти сукупність певних знань, умінь і навичок в інформаційній сфері, а також належний рівень інформаційної правосвідомості. З-поміж указаних спеціальних знань, умінь і навичок назвімо насамперед такі, як спроможність реалізувати в інформаційному суспільстві свої законні інформаційні інтереси; усвідомлення перспектив і переваг від використання інформаційно-телекомунікаційних технологій; здатність критично оцінювати отримувану з різних джерел інформацію (її достовірність, актуальність, повноту, корисність тощо); можливість дієво протистояти реальним та потенційним викликам і загрозам в інформаційній сфері. Таким чином, культура інформаційної безпеки людини (тобто, спеціальні знання, уміння й навички) – це здатність особи виразно усвідомлювати свої інформаційні потреби, знаходити й оцінювати джерела інформації (їх достовірність, актуальність, повноту тощо), відшукувати, аналізувати, організовувати, тлумачити, узагальнювати інформацію, оцінювати продуктивність форм і засобів реалізації інформаційних потреб. Успішно протистояти усім викликам

і загрозам при використанні інформаційного (кібернетичного) середовища може лише людина, котра має високий рівень інформаційної культури.

Отже, для формування культури кібернетичної безпеки особи, необхідні, на нашу думку, розроблення, організація і здійснення відповідними державними органами і громадськими об'єднаннями заходів, спрямованих передусім на ті верстви інформаційного суспільств, які найбільш уразливі й найменш захищені від інформаційних викликів і загроз. Переконані, що ця проблематика потребує подальшого всебічного обговорення, пильної уваги наукової спільноти і широкої громадськості.

3.3. Порівняльно-правове дослідження правового регулювання кібербезпеки людини на міжнародному рівні

У цьому підрозділі проблематику кібернетичної безпеки людини розглянемо першочергово з позицій стабільності системи міжнародних відносин. При цьому слід наголосити на важливості розвитку кібернетичної безпеки на міжнародному рівні. Як засвідчив аналіз міжнародно-правових документів, дво- й багатосторонніх міжнародних угод, національних законодавств, проблеми правового забезпечення кібернетичної безпеки особи ще не отримали адекватної уваги. Нагальна потреба розроблення комплексних заходів для налагодження й удосконалення системи міжнародної кібернетичної безпеки, а також відповідного стратегічного партнерства зумовлена слабкою захищеністю людини в умовах мілітаризації глобального кібернетичного простору, розгортанням потужних інформаційних війн, значним поширенням комп'ютерної злочинності (особливо у фінансовій

сфері) та кібертероризму.

З огляду на особливості сучасного стану інформаційних прав і свобод людини убачається доцільним розроблення й ухвалення відповідної міжнародної угоди у сфері інформації прав, котра стане підґрунтям запровадження у національні законодавства міжнародних зобов'язань стосовно гарантування інформаційних прав і свобод, забезпечення кібернетичної безпеки особи, регулювання низки фундаментальних питань щодо, зокрема, захисту прав суб'єктів персональних даних (скажімо, про транскордонне передання таких даних). Крім того, важливим убачається впровадження ефективних механізмів забезпечення кібернетичної безпеки особи, створення з задля цього відповідних національних і міжнародних інституцій.

Відтак, досягнення завдань цього дослідження потребує уважного вивчення форм і механізмів співробітництва, дієвих правових інструментів протидії існуючим і потенційним інформаційно-безпековим викликам і загрозам, які передбачені чинними на сьогодні угодами про співпрацю у цій сфері.

Стабільність, стійкість міжнародного співробітництва у розв'язанні проблем кібернетичної безпеки відіграє важливу роль і в розвитку національного інформаційного законодавства.

Слід одразу підкреслити, що міжнародно-правовими нормами питання безпосереднього забезпечення безпеки особи в інформаційній сфері практично не регламентуються, позаяк її правосуб'єктність в міжнародному праві обмежена.

Натомість доцільність розгляду цієї проблематики зумовлена тим, що, з огляду на глобалізацію інформаційного (кібернетичного) простору, стабільність наявних у ньому відносин для стійкого існування та розвитку особистості в інформаційному суспільстві, питання міжнародної інформаційної безпеки становлять беззаперечний інтерес. Крім того, інформаційно-безпекові міжнародно-правові норми, як засвідчив проведений

аналіз, містять і регламентацію міжнародних аспектів забезпечення інформаційної безпеки людини.

Особливу небезпеку у сфері міжнародної кібербезпеки становлять загрози інформаційного впливу, зокрема таких його крайніх форм, здатних спричинити регіональні та світові конфлікти, руйнівний потенціал яких можна порівняти із дією «традиційних» засобів масового ураження – застосування інформаційної зброї, кібертероризм, інформаційні війни. Яскравим прикладом цього є те, що: анексія Російською Федерацією українського Криму, її агресія на Донбасі готувалися, супроводжувалися й тривають досі за допомогою широкомасштабної інформаційної війни проти України, руйнівним інформаційно-психологічним впливом на частину її населення. Відтак, на початку третього тисячоліття кібернетичний простір (поряд із землею, водою, повітрям і космосом) увійшов до сфер ведення воєнних дій, а головними об’єктами в інформаційних війнах є психологія ворожого війська й населення та інформаційна інфраструктура.

Варто зазначити, що світова спільнота ще не виробила єдиного підходу до проблематики міжнародної кібербезпеки, хоча відповідних нормативно-правових актів на сьогодні існує чимало. До них належать насамперед низка основоположних міжнародних документів щодо прав людини: Загальна декларація прав людини, міжнародні пакти про економічні, соціальні й культурні права, про громадянські й політичні права, Європейська конвенція про захист прав людини і основних свобод та інші. Саме ці документи закріпили основні загальносвітові стандарти прав і свобод людини.

Як одну зі складових права особи на кібербезпеку розглянемо детальніше інститут права на недоторканність приватного життя. Це поняття означає надання людині можливості регулювати, контролювати поширення інформації про себе, свою родину, житло тощо, перешкоджати зазіханням на її репутацію, честь і гідність, на несанкціоноване оприлюднення (розголошення) своїх персональних даних чи інших відомостей особистого характеру.

У міжнародно-правовому контексті недоторканність приватного життя є категорією «особистих прав, які надають змогу кожній людині стати на заваді розголошенню відомостей особистісного характеру про її життя, що оберігається від втручання держави і сторонніх осіб». Про можливі окремі обмеження цього права в рішеннях щодо застосування положень Європейської конвенції про захист прав людини і основних свобод зазначав Європейський суд з прав людини (ЄСПЛ): «*…приховане спостереження за поштою і зв'язком у разі надзвичайних умов є необхідним у демократичному суспільстві, але за наявності належних і ефективних гарантій*». Приміром, подібне втручання у приватне життя не суперечить Конвенції, коли воно має на меті запобігання конкретним, найнебезпечнішим злочинам або їхнє припинення (а не якихось дрібних правопорушень), або якщо воно застосовується до суворо обмеженого кола осіб тощо.

Утім на практиці декларування таких правил, на жаль, не може цілковито убезпечити від різноманітних вторгнень у приватну сферу людини. Наприклад, всесвітню увагу привернув Едвард Сноуден, американський програміст, котрий за контрактом працював на Агентство національної безпеки (АНБ) США. Він оприлюднив значний масив секретних матеріалів, із яких, зокрема, випливало, що американські спецслужби відстежували величезні потоки інформації в мережевому просторі багатьох, країн, у тому числі Європейського Союзу, встановивши необмежений доступ до серверів глобальних комунікаційних компаній. Так, АНБ і ФБР США перехоплювали трафіки таких інтернет-гігантів, як Microsoft, Apple, Facebook, Google між їхніми серверами й пересічними користувачами. При цьому без жодних судових дозволів аналітики спецслужб на свій розсуд могли обирати об'єкти для електронного стеження й таємного прослуховування. Деякі американські добровільно «зливали» спецслужбам дані про своїх користувачів, інших примушували до цього.

Як бачимо, навіть найбільш технологічно розвинені країни виявилися не спроможними відвернути подібне втручання. Тому назріла потреба

формування єдиного міжнародно-правового режиму забезпечення інформаційної (кібернетичної) безпеки.

Як і з переважної більшості міжнародно-правових питань, особливу роль у питаннях забезпечення права особи на кібербезпеку відіграє Організація Об'єднаних Націй – найбільш представницька міжнародна інституція. Зокрема, вже на другий рік свого існування організації, у 1946 році, в резолюції Генеральної Асамблеї ООН містилося важливе, на нашу думку, положення стосовно права особи на кібербезпеку, а саме: «…*свобода інформації є основним правом людини і являє собою критерії всіх видів свободи, захисту котрих Об'єднані Нації себе присвятили; ...свобода інформації, безперечно, вимагає від тих, хто користується її привілеями, бажання й уміння не зловживати ними. Основним принципом її є моральний обов'язок прагнути до виявлення об'єктивних чинників і до поширення інформації без злісних намірів*…» [263]. Питань кібербезпеки особи торкаються й наступні документи ООН.

Що стосується захисту персональних даних, то на міжнародному рівні це питання було регламентоване в 1981 році Конвенцією Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних (далі – Конвенція), яка містила низку відповідних вимог до держав-учасниць. Це, зокрема, приписи про те, що: громадянин має право знати про існування автоматизованих картотек; отримувати інформацію про наявність чи відсутність у цих картотеках даних на нього; отримувати особисто наявні в картотеках дані; у разі незаконності чи невідповідності цих даних вимогам Конвенції вимагати їх виправлення чи видалення, а в разі відмови в цьому – звертатися до вищщої інстанції. Крім того, в документі закріплювалися правила транскордонного передання персональних даних, гарантії прав щодо обробленння даних стосовно расового походження людини, її політичних переконань, здоров'я, сексуальної орієнтації та інших особливих категорій даних [264].

У ст. 6 Декларації ООН про права й обов'язки окремих осіб, груп і

органів суспільства заохочувати й захищати загальновизнані права людини й основні свободи закріплено, зокрема, й основоположні права, що стосуються забезпечення безпеки особи в інформаційній сфері:

– знати, розшукувати, здобувати, отримувати й розпоряджатися інформацією про всі права людини й основні свободи, в тому числі доступ до інформації про те, в який спосіб забезпечуються ці права і свободи у внутрішньому законодавстві, в судовій чи адміністративній системах;

– вільно оприлюднювати, передавати чи поширювати серед інших думки, інформацію і знання про всі права людини й основні свободи [265].

Що стосується безпосередньо проблем кібербезпеки людини, то початком їхнього усебічного обговорення й пошуку шляхів розв'язання на міжнародному рівні можна вважати міжнародну конференцію із глобального інформаційного суспільства (1996, ЮАР), де з-поміж інших розглядалися питання доступу особи до інформації, подолання нерівності в інформаційній сфері, інформаційно-психологічних впливів на людину.

Ухвалена 61-ю сесією Генасамблеї ООН (2005) резолюція 60/45 «Досягнення у сфері інформатизації й телекомунікації в контексті міжнародної безпеки» стала наступним важливим кроком у цьому напрямку, поклала початок формуванню принципово нового загальносвітового міжнародно-правового режиму, спрямованого на регулювання відносин у сфері інформації, інформаційно-телекомунікаційних технологій і методів їхнього застосування й використання [266].

У липні 2000 року в Японії провідні світові держави Великої вісімки підписали так звану Окінавську хартію глобального інформаційного суспільства (надалі – Хартія), де одним із головних напрямів розвитку цього суспільства визначено захист приватного життя під час оброблення особистих даних із одночасним забезпеченням вільного обігу інформації. У Хартії також зазначено, що інформаційно-телекомунікаційні технології є важливим чинником формування сучасного суспільства, а сутність соціальної трансформації, котра стимулюється інформаційно-комунікаційними

технологіями, полягає у її здатності сприяти людині й суспільству в застосуванні ідей і знань. При цьому головним завданням своїх учасників Хартія вбачає забезпечення кожному можливості користуватися перевагами глобального інформаційного суспільства, стійкість якого базується на вільному обміну інформацією і знаннями та іншими демократичними цінностями, які стимулюють розвиток людини.

Активна робота під егідою ООН щодо формування основ забезпечення права особи на кібербезпеку триває. Так, у 2001 році в Будапешті держави-учасники Ради Європи підписали Конвенцію про кіберзлочинність (CETS № 185). Положення цієї так званої Будапештської конвенції спрямовані на захист особистих даних, законних інтересів людей у використанні й розвитку інформаційних технологій, боротьбу зі злочинами в кібернетичному просторі, в ній уперше наведена класифікація таких злочинів. У Конвенції – єдиному в теперішній час обов'язковому регіональному міжнародному документі з питань кібербезпеки – зазначено, що вона є першою міжнародною угодою щодо злочинів, вчинених через Інтернет та інші комп'ютерні мережі, стосується мережевої безпеки, порушень авторських прав, кібернетичного шахрайства, дитячої порнографії та ін. Конвенцією також передбачені пошук комп'ютерних мереж, перехоплення даних та інші повноваження й процедури.

Будапештська конвенція встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву. Вона також доповнена Протоколом про «акти ксенофобського та расистського характеру, вчинених через комп'ютерні системи», й Директивною запискою [267].

Наша держава ратифікувала Будапештську конвенцію у 2005 році, проте на сьогодні не всі її положення інтегровані у вітчизняне законодавство, а повна їхню імплементація потребує істотних змін у Кримінальному процесуальному кодексі України.

До числа фундаментальних міжнародно-правових документів, котрий

регулює, зокрема, питання кібернетичної безпеки, належить прийнятий у 1992 році засадничий документ спеціалізованої установи ООН – Статут Міжнародного союзу електрозв'язку (МСЕ) [268], до якого приєдналися всі держави-члени ООН, в тому числі й Україна. Статут регулює комплекс питань міжнародної співпраці у сфері використання телекомунікацій, розвитку засобів та підвищення ефективності відповідних послуг, визначає чинники, котрі заважають функціонуванню існуючих телекомунікаційних мереж, тощо.

З метою оцінювання участі держав у галузі кібербезпеки на світовому рівні, підвищення поінформованості про важливість цих проблем та їх різні виміри МСЕ щороку оприлюднює так званий глобальний індекс кібербезпеки, котрий базується таких критеріях глобального прогресу у цій сфері: законодавчі заходи; технічні заходи; організаційні заходи; розбудова потенціалу; кооперація. Зазначимо, що обґрунтовані висновки МСЕ користуються широкою довірою.

Перша частина спільного законодавства ЄС про кібербезпеку – Директива щодо мережевої та інформаційної безпеки (Директива NIS) була ухвалена Європарламентом у 2016 році [269]. Правові заходи, передбачені Директивою, спрямовані на радикальне підвищення в Європейському Союзі загального рівня кібербезпеки (шляхом проведення відповідних операцій Групою реагування на інциденти, пов'язані з комп'ютерною безпекою, – CSIRT або CERT – та компетентним органом у галузі мереж та інформаційних систем), а також активізацію міжнародної співпраці й розвитку безпекової культури стосовно інформування відповідно до директивних вимог. Задля допомоги якнайшвидшій узгодженій реалізації державами-членами ЄС Директиви вона має додаток, де наведено найефективніший практичний досвід, пояснення та тлумачення, – так званий Інструментарій NIS (NIS Toolkit).

Ця Директива не є обов'язковою для України, котра поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у правозастосовній практиці, а деякі були частково впроваджені у вітчизняне

законодавство. Вбачається, що імплементацію Директиви NIS можна провести в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом. У теперішній час у Верховній Раді України зареєстровано законопроект, спрямований на приведення законодавства України у відповідність до Європейського. Це стосується і Директиви NIS (аналіз законопроекту наводиться у розділі Законодавчий рівень. Закон про кібербезпеку). Крім того, деякі вимоги Директиви вводить до розроблюваних законопроектів Державна служба спеціального зв'язку та захисту інформації України. Водночас її фахівці вважають, що при розробці загальних законів у сфері кібербезпеки відповідно до положень Директиви NIS буде вельми потрібною міжнародна допомога.

У виробленні єдиних підходів у сфері забезпечення кібернетичної безпеки як складової національної безпеки держав-учасниць значну роль відіграє Організація Північноатлантичного договору (НАТО). Цей напрям став одним із пріоритетних напрямів діяльності Альянсу з огляду на вразливість вказаної сфери, численність і різноманітність відповідних викликів і загроз [270, с. 42].

На Лісабонському саміті країн-членів НАТО (листопад 2010 року) за участі глав держав та урядів була прийнята нова Стратегічна концепція оборони та безпеки країн-членів блоку. У цьому документі загрози атак у кіберпросторі були фактично прирівняні до загроз із застосуванням війська, що, таким чином, передбачає можливість відсічі подібних масованих атак із застосуванням збройних сил держави, котра зазнала такого нападу. Позаяк останнім часом кібератаки стали чи не найсерйознішою загрозою безпеці, забезпечення кібернетичної безпеки країн-членів НАТО визначено другим за значущістю пріоритетом безпекової політики Альянсу. Водночас, співробітництво з партнерами щодо формування і вдосконалення кібербезпекової системи блоку визнано у Доктрині НАТО з кібербезпеки ключовим механізмом реалізації відповідних заходів [271].

Два роки потому вказані підходи були деталізовані Декларацією

Чиказького саміту (травень 2012 року) Ради НАТО, в п. 49 якої йдеться про налаштованість Альянсу на співробітництво з іноземними партнерами для забезпечення власної безпеки й організації адекватних відповідей на кібернетичні виклики й загрози [272]. А остаточне закріплення кіберпростору як арени можливого ведення бойових дій (поряд із землею, морем, повітрям і космосом) відбулося у документах Варшавського саміту країн-членів НАТО (липень 2016 року) [273].

Дії НАТО у сфері забезпечення кібернетичної безпеки мають два пріоритетні напрями. Це, насамперед, захист власних комп'ютерних мереж, рішення стосовно якого було ухвалено на саміті НАТО в Ньюпорті (Вельс, вересень 2014 року). Слід зазначити, що це завдання вбачається вельми непростим з огляду на дуже широку присутність суб'єктів блоку в мережах Інтернету. Адже для його виконання слід забезпечити захист усього комплексу інформаційно-комунікаційних систем, задіяних НАТО у своїх операціях і місіях, від численних загроз, що походять з кібернетичного простору.

Другий пріоритетний напрям – сприяння країнам-членам щодо вдосконалення сил і засобів захисту кібернетичного простору. Для цього застосовуються різні механізми, як-от дворічний план визначення колективних цілей кіберзахисту (приміром, розробка стратегії кіберзахисту), що їх мають підтримати всі учасники блоку. Шляхи й засоби реалізація цих узгоджених цілей систематично коригуються. Крім того, в межах численних освітніх установ НАТО (наприклад, школа в Обераммергау (ФРН), Кібернетична академія (Португалія), Талліннський кооперативний Центр передового досвіду з кіберзахисту (Естонія) та ін.) провадиться широкий спектр просвітницьких, навчальних і тренувальних заходів. Вказані заходи, спрямовані на посилення блоку за рахунок посилення кожного із членів, їхньої здатності до кіберзахисту, до узгодженого виконання завдання колективної оборони одне одного [274].

Нагальне завдання розбудови національної системи кібернетичної безпеки, спроможної ефективно протидіяти загрозам національній безпеці у

кібернетичній сфері, стоїть сьогодні й перед нашою державою. Дедалі частіше на кібернетичні атаки й злочини наражаються державні, фінансові установи, підприємства енергозабезпечення і транспорту та інших об'єктів критичної інфраструктури. І, як засвідчив аналіз стану кібербезпеки в Україні, ця складова національної безпеки має високий ступінь уразливості від кіберзагроз і залишається вельми слабкою.

Відповідно до укладених міжнародних угод у сфері кібербезпеки Україна співпрацює з іноземними державами, їхніми збройними силами, правоохоронними органами і спецслужбами, а також із багатьма міжнародними організаціями. У цьому контексті одним із пріоритетних напрямів міжнародного співробітництва у цій сфері вбачається активна діяльність України у структурах ООН, стратегічне партнерство з Організацією Північноатлантичного договору та Європейським Союзом.

Підсумовуючи дослідження цього підрозділу, відмітимо, що на сьогодні відсутній єдиний, загальний для всієї світової спільноти міжнародно-правовий документ щодо кібернетичної безпеки. Однак керівні принципи щодо методів підвищення рівня безпеки в кібернетичному просторі містять Конвенція ООН проти транснаціональної організованої злочинності (2000 рік) та Статут Міжнародного союзу електрозв'язку (1992 рік), Доповідь ООН про кібербезпеку (2015 рік).

Єдиним регіональним обов'язковим в юридичному сенсі документом є Будапештська конвенція про кіберзлочинність (2001 рік). Наша держава є учасником цієї конвенції, а тому більшість її норм матеріального права імплементувала в національне законодавство. Водночас, на нашу думку, задля ефективної реалізації всіх положень Будапештської конвенції слід удосконалити кібербезпековий понятійно-термінологічний апарат Кримінального процесуального кодексу України.

Директива NIS не є обов'язковою для України, котра поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у правозастосовній практиці, а деякі були частково впроваджені у вітчизняне

законодавство. Вбачається, що імплементацію Директиви NIS можна провести в межаї механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом.

Висновки до розділу 3

Серед пріоритетних напрямів цього розділу визначено здійснити системний аналіз правового регулювання кібербезпеки людини, розробити критерії класифікації загроз безпеці людини у кіберпросторі, провести порівняльно-правове дослідження правового забезпечення кібербезпеки людини на міжнародному рівні. За результатами реалізації визначених завдань нами отримані такі основні висновки:

1. У межах дослідження правових засад кібербезпеки людини *інформаційну дієздатність* як складову інформаційної правосуб'єктності визначено як спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав, брати на себе певні правові обов'язки, а також нести юридичну відповідальність у разі неправомірної поведінки.

На основі теоретичного аналізу правової природи відносин у сфері забезпечення кібернетичної безпеки людини, комплексно досліджено усі її складові – суб'єкт (людина у глобальному інформаційному просторі, котра потребує належного правового забезпечення своєї безпеки при користуванні кібернетичним простором), об'єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов'язків усіх учасників зазначених суспільних відносин).

Удосконалено зміст поняття «*кібернетична безпека людини*», яке запропоновано розуміти як стан її захищеності, який визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й

інформаційного суспільства забезпечувати її інформаційну безпеку.

2. Відмічено, що найбільш уразливим суб'єктом інформаційних правовідносин є людина. Зумовлено це постійним виникненням нових викликів і загроз кібербезпеці людини, пов'язаних з недосконалістю інформаційно-телекомунікаційних технологій, інформаційно-психологічними впливами, використанням інформації для досягнення геополітичних, терористичних та інших протиправних, руйнівних цілей. Відтак, в умовах глобального інформаційного суспільства особистість у процесі задоволення своїх потреб найбільш яскраво виявляє свою соціальну складову, і, з огляду на нові безпекові виклики й загрози, змушена на основі культури інформаційної безпеки виробляти відповідні заходи протидії.

Визначено основні критерії класифікації загроз кібербезпеці людини. Зокрема:

- мета, до якої прагне джерело загрози;
- джерело загрози кібербезпеці людини;
- розташуванням джерела загрози;
- характер впливу, природа виникнення.

3. Всебічне дослідження новітніх викликів і загроз кібербезпеки в умовах транскордонності у глобальному інформаційному суспільстві, а також небезпечних тенденцій у цій сфері дало змогу виокремити критерії їх можливої класифікації: джерело загрози (виклику), залежність від джерела загрози, розташування джерела загрози стосовно об'єкта, характер впливу. На цій основі, з метою вдосконалення вітчизняної системи правового забезпечення кібернетичної безпеки людини, запропонована авторська класифікація видів відповідних викликів і загроз. Зокрема, з огляду на значущість соціальних мереж, визначено джерела загроз в Інтернеті, а саме: сайти, котрі становлять небезпеку для особистості (мають на меті вплив на свідомість індивіда, рекламовані задля отримання зиску та ін.); спам, тотальне розсилання реклами та іншої інформації без бажання користувача тощо.

Крім того, вивчення сучасних інформаційно-телекомунікаційних

технологій дало змогу виявити специфічну групу загроз, пов’язаних з цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin та інших), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie та ін.). У теперішній час найбільш нагальним вбачається вирішення проблем, пов’язаних із розвитком новітніх технологій (на кшталт універсальної інноваційної платформи Blockchain), удосконалення систем ідентифікації й аутентифікації особи в кібернетичному просторі тощо.

4. Спираючись на проведене системне наукове дослідження, визначено напрями розробки Концепції кібернетичної безпеки людини, її можливі структуру та зміст, а також потребу долучення до її складу документів стратегічного планування України. Запропоноване структурно-змістовне наповнення вказаної Концепції містить головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення кібербезпеки особи. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави у цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість Концепції.

Доцільність розробки Концепції кібернетичної безпеки людини зумовлена, на нашу думку, необхідністю вдосконалення національного законодавства про кібернетичну безпеку в сенсі закріплення поняття кібернетична безпека людини, правового забезпечення кібернетичної безпеки людини, формування системи забезпечення безпеки особи в інформаційній сфері як сукупності відповідних сил і засобів.

5. За результатами проведеного у даному дослідженні системмного аналізу норм права, котрі стосуються забезпечення кібербезпеки людини, що вони містяться не лише в інформаційному, а практично в усіх галузях законодавства – конституційному, цивільному, адміністративному, виборчому, трудовому, фінансовому, банківському, податковому,

процесуальному (кримінальне й цивільне) та ін. На основі такого застереження зроблено висновок, що інститут правового забезпечення кібербезпеки людини має міжгалузевий комплексний характер і становить сукупність юридичних норм, котрі регулюють групу однорідних суспільних відносин стосовно забезпечення кібернетичної безпеки людини у процесі реалізації нею своїх прав та законних інтересів – матеріальних, духовних, соціальних, політичних, культурних, пізнавальних, екологічних та інших. Водночас в умовах глобального інформаційного суспільства для правового забезпечення кібернетичної безпеки людини базисними є норми інформаційного права, що, власне, і виступає показником її галузевої належності.

Основні результати розділу викладено в працях автора: [275-280].

РОЗДІЛ IV
ПРАВОВА ЗАХИЩЕНІСТЬ СУСПІЛЬСТВА У КОНТЕКСТІ ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ ТРАНСФОРМАЦІЙ У КІБЕРПРОСТОРІ

4.1. Аналіз концепцій інформаційного суспільства

Один із визначальних феноменів сучасності – формування інформаційного суспільства, спричинене бурхливим розвитком інформаційних технологій, впровадженням їх у всі сфери життєдіяльності людства, зумовлює потребу належного упорядкування нових суспільних відносин, вироблення форм і засобів впливу на їхніх учасників, відповідних механізмів тощо.

В інформаційному, або постіндустріальному суспільстві, формування якого означає по суті перехід світової спільноти на новий етап свого цивілізаційного розвитку, особливої вагомості й першорядної загальнолюдської цінності набуває інформація. Формування інформаційного суспільства й відповідних суспільних відносин (зокрема, їхнього правового регулювання) пов’язують зі зміною ціннісних пріоритетів – від матеріальних благ (виробництво матеріальних продуктів, енергії, видобуток сировини тощо в індустріальному суспільстві) до інформації: провідною тенденцією прогресу нового інформаційного суспільства стає розвиток інтелектуально-інформаційних ресурсів, наукового знання, їхнє перетворення на цінність, важливий продукт.

Позаяк цей феномен, пов’язані з його розвитком трансформаційні соціальні зрушення позначаються абсолютно на всіх сферах буття соціуму, дослідженням широкого кола проблем, пов’язаних з інформаційним суспільством, займаються філософія, соціологія, політологія, правознавство, економічна наука, менеджмент, а також кібернетика та багато інших наук.

У науковому обігу поняття інформаційного суспільства з’явилося за історичними мірками нещодавно стараннями насамперед економістів і програмістів, філософів і соціологів, політологів і політиків. Дещо пізніше це поняття увійшло до кола наукових і професійних інтересів правників, котрі привнесли у його тлумачення юридичні аспекти. Сьогодні це поняття відбиває сутність та об’єктивні тенденції чергового витка цивілізаційного розвитку людства, пов’язаного з виникненням інформаційно-телекомунікаційних технологій, а відтак нових суспільних потреб, відповідного способу життя тощо.

Ззастосовуване поняття «інформаційне» стосовно сучасного суспільства замінило собою цілу низку термінів на його позначення, яке засноване на знаннях – «the knowledgeable society») [281], конвенціональне [282] тощо. Своєю чергою, М. Кастельс пропонував користуватися в таких випадках терміном «інформаціональне суспільство». Дослідник уважав, що інформація, інформування в сенсі передання певного знання завжди відігравали важливу роль, тоді як для відображення певної атрибутивної властивості особливої форми соціальної організації більше підходить термін «інформаціональний». Зазначена властивість полягає в тому, що в теперішній історичний проміжок усі способи транслювання інформації перетворилися на підстави економіки, структурування суспільства та здійснення владних повноважень [253].

Розвиток інформаційного суспільства має нелінійний характер та іншу специфіку, зокрема:

– взаємозалежність кількості та якості інформації;

– складність розрізнення достовірної та хибної (неправдивої, вигаданої) інформації;

– брак надійних критерії перевірки достовірності інформації;

– маніпулятивний вплив хибної інформації на індивідуальну та суспільну свідомість;

– стреотипне сприйняття інформації, хибні, фальшиві інформаційні цінності;

– переривчастість (атомізація) інформаційного середовища, яка зумовлює серйозні ризики у сфері інформаційної безпеки.

Ускладнення інформаційних відносин зумовлює виникнення різноманітних інформаційних посередників, котрі відіграють роль зв'язкових між окремим користувачем з його особистим простором та інформаційним полем у глобальному інформаційному середовищі. У такому полі інформаційної взаємодії, в якому змушена діяти людина, створюються інформаційні примари (фантоми), інформаційні артефакти та інформаційні сурогати. Спочатку ці інформаційні фантоми співіснують з реальністю, врешті-решт витісняючи останню, залишаючи натомість сурогатну квазіінформаційну завісу. Якщо людина не помічає цього, вона починає керуватися правилами цієї хибної реальності.

Генезис поняття «інформаційного суспільства» та розуміння сутності самого феномену пов'язані передовсім з теоріями індустріального й постіндустріального суспільства. Теоретики постіндустріального суспільства у 60-і – 80-і роки XX століття стверджували що центр суспільної ваги переміщується від промисловості (виробничої сфери, в основі якої лежать земля, праця й капітал) до інформації, зростання її значення та важливості, її поширення і забезпечення доступу до неї, пріоритетного розвитку технологічних, інфраструктурних та економічних аспектів, інформаційно-комунікаційних технологій.

У праці «Прийдешнє постіндустріальне суспільство» (1973) Д. Белл навів такі головні ознаки вказаного суспільства:

1) примат економіки обслуговування над економікою виробництва;

2) вихід на головні ролі науково-технічних фахівців;

3) теоретичні знання як головне джерело інновацій;

4) менеджмент технічного прогресу;

5) «інтелектуальні технології» (лінійне програмування, теорія рішень, інформаційні теорії тощо, пов’язані з комп’ютерними технологіями) [283]. Засновник теорії постіндустріального суспільства у 1970 роках зазначав, що «інформаційне суспільство підкреслює не просто становище розвитку для постіндустріального суспільства, а домінанту роль інформації в соціальній структурі [284, с. 52].

У теперішній час не існує єдиної загальновизнаної концепції постіндустріального суспільства, проте аналіз праць багатьох дослідників дозволяє виявити певні спільні погляди. Так, практично усі вони погоджуються з такою періодизацією розвитку людства: суспільство доіндустріальне, індустріальне й постіндустріальне [285-289]. При цьому головним відмінними рисами останнього періоду від попередніх називаються: інформація стає провідним виробничим ресурсом замість сировини й енергії; пріоритет у виробничій діяльності переміщується з видобутку й вироблення на оброблення; на зміну попереднім праце- та капіталомістким виробничим методам і процесам приходять технології, засновані на науці.

Крім того, у розвитку постіндустріального суспільства підкреслюється провідна роль знань і технологій. І, нарешті, більшість дослідників погоджуються, що сучасний період суспільного розвитку є перехідним.

До кінця 1970-х років сформувалася думка, що знання й інформація стають безпосередньою й головною виробничою силою сучасної світової системи господарювання, позаяк технологічний розвиток утілюється в самостійному існуванні цих феноменів.

Сама концепція суспільства, котра спирається на інформаційні технології, започаткована у 1960-1970-х роках працями Д. Белла, Е. Тоффлера, Й. Масуди, Р. Дарендорфа й А. Турена в межах теорії постіндустріального суспільства у спробах поєднати технологічні й соціальні аспекти. Тоді ж з’явився й відповідний термін – «інформаційне суспільство», запроваджений

для точнішого визначення стану сучасного етапу еволюції людства завдяки розвитку знань, передовсім у сфері комп'ютерних і телекомунікаційних технологій.

Згадуваний вище знаний японський соціолог Й. Масуда ототожнював поняття постіндустріального й інформаційного суспільства [290]. А його американський колега Е. Тоффлер, вважаючи, що знання є базою вдосконалення технологій, писав: «…нові машини й техніка стають не лише продукцією, а й джерелом новітніх творчих ідей» [291]. Е. Тоффлеру також належить визначення принципів функціонування індустріального суспільства, від яких відмовляється суспільство постіндустріальне (інформаційне): типізація, концентрація, централізація, синхронізація, спеціалізація, максимізація [292].

Як зазначав у праці «Інформаційне суспільство як суспільство постіндустріальне» Й. Масуда, на відміну від матеріального виробництва в індустріальному суспільстві в суспільстві інформаційному на пріоритет належить виробництву знання й інформації. Соціальні зв'язки, потрібні для суспільного розвитку, формуються у процесі масового виробництва інформації, а відтак значно зростає роль комунікативної діяльності й соціального управління. Зникає примат речей, їх вироблення, а натомість відбувається масове виробництво знань. Таким чином, кожен член соціуму реалізує свої здібності, виробляючи нове знання й інформацію за допомогою комп'ютерних й інформаційно-телекомунікаційних технологій [290]. Крім того, зважаючи на те, що інформація за своєю сутністю є транскордонною, Й. Масуда атрибутивною складовою переходу до інформаційного суспільства вважає загальні глобалізаційні процеси.

Відомий американський фахівець, один із засновників інформаційного моделювання Дж. Мартін визначив інформаційне суспільство як інтегральне поняття, котре всебічно охоплює питання функціонування соціальної системи, головною ознакою якої є впровадження інформаційних технологій у наукову, економічну, виробничу, соціальну, освітню та інші сфери життєдіяльності

[293, с. 31]. У такому суспільстві, доводить дослідник, якість життя та перспективи економічного й соціального прогресу зумовлює саме інформація, рівень її застосування.

Як бачимо, питання так званого постіндустріального суспільства перебували в центрі уваги провідних світових дослідників – філософів, соціологів, культурологів та ін., котрі доводили, що глобальні соціальні зрушення відбуваються через зміни пріоритетів від сфери виробництва до сфери послуг і споживання. У контексті цих досліджень, об'єктивно пов'язаних із розвитком інформаційних технологій, формується концепція інформаційного суспільства, адепти котрої вважають, що неодмінною умовою будь-якої соціальної взаємодії виступає інформація. Тобто, на думку цих дослідників, діалектика розвитку зумовила перехід кількісних змін в інформаційній сфері у формування інформаційного суспільства – нового типу соціального світоустрою. Простіше кажучи: сучасне суспільство є інформаційним, позаяк у теперішній час кардинально зросли обсяги інформації, яка в ньому циркулює. При цьому варто зазначити, що процес інформатизації суспільства триває, впливаючи на спосіб життя людей і відповідне формування нових правовідносин.

Результати аналізу й узагальнення чималої кількості концепцій розвитку інформаційного суспільства дає підстави виокремити провідні з-поміж них: технологічну, економічну, зайнятості, просторову й культурологічну.

Підґрунтям *технологічної* концепції є інформаційно-технологічні інновації, що з кінця 1970-х років почали масово входити в науково-технічний і побутовий вжиток. Тому прихильники цієї концепції і вважають головним рушієм формування інформаційного суспільства нові технології як найпомітнішу ознаку сучасності. Йдеться передовсім про мережеву й персональну комп'ютеризацію, розвиток кабельного й супутникового телебачення, онлайнових інформаційних послуг, текстових редакторів, компактних носіїв значних обсягів інформації та інших нових виробничих і офісних комп'ютерних технологій. Основний сенс концепції в тому, що

соціальні трансформації відбувається в результаті впливу на суспільство величезних обсягів технологічних новацій. «Нові технології, - відмічає британський соціолог Френк Вебстер, - одна з найпомітніших ознак народження інформаційного суспільства» [294].

Натомість *економічна* концепція розвитку інформаційного суспільства на передній план висуває економічні аспекти інформаційної діяльності: економіка стає інформаційною, коли у валовому національному продукті превалює відповідна частка. А якщо інформаційна складова стає провідною в господарській діяльності, то й усе суспільство можна вважати інформаційним.

Близькою до економічної є концепція *зайнятості населення*, в основі якої лежать два головні критерії – кількість працездатного населення, зайнятого у галузі інформаційних технологій, а також вплив цієї сфери на всю економіку (валовий внутрішній продукт) і частка застосування у промисловості та сфері послуг штучного інтелекту.

Своєю чергою, географічним принципом послуговується *просторова* концепція, яка водночас базується на економіці й соціології. Головним чинником її прибічники вважають інформаційні мережі, котрі мають значний вплив на часово-просторову організацію, оскільки з’єднують різні місця й об’єкти. Варто зазначити, що завдяки нинішній широкій популярності соціальних інформаційних мереж просторова концепція інформаційного суспільства набуває все більше прихильників.

Так, значного поширення набула практика визначення базисної точки, центру інформаційних мереж, котрі можуть поєднувати рідні об’єкти (точки) – від окремого офісу чи підприємства до країни, регіону ба навіть усього світу. У цьому сенсі можна вести мову про національне, міжнародне і глобальне «провідникове суспільство», яке створює «кільцеву інформаційну мережу» в кожному помешканні, торговельному чи навчальному закладі та навіть для кожної людини в будь якому місті, котра має ноутбук чи електронний гаджет з відповідним налаштуванням.

Нарешті, *культурологічна* концепція розвитку інформаційного

суспільства спирається на найбільш зрозумілий критерій, позаяк ні в кого не виникає сумнівів у надзвичайному зростанні інформаційного чинника у повсякденному житті. Водночас культурологічні показники значно важче підлягають вимірюванню.

Таким чином, сьогодні людина існує в інформаційно навантаженому суспільстві, а вплив цього чинника значно складніший і глибший, ніж може здатися. Йдеться про те, що інформаційне середовище проникає в людину, перетворюється на її складову, навіть коли сама людина воліє не реагувати на впливи кібернетичного простору, котрий її оточує.

Підтримуємо позицію тих науковців, які виокремлюють ще одну концепцію інформаційного суспільства – *суспільство знань*. Ця концепція не є новою для нашого часу, проте її найбільший прояв відбувся саме із розвитком інформаційно-комунікаційних технологій у 21 ст. У 1993 р. з'явилася праця одного з найбільш впливових теоретиків менеджменту 20 століття Пітера Друкера «Постекономічне суспільство» [295], перший розділ якої дослідник назвав «Від капіталізму до суспільства знань». До речі, сам вчений називав себе «соціальним екологом».

Цікавою з цього приводу є позиція ЮНЕСКО, у Всесвітній доповіді якої «До суспільств знання» у 2005 році [296], зазначалося, що «суспільство знань відрізняється від інформаційного суспільства, оскільки інформаційне суспільство ґрунтується на понятті технології, а суспільство знань має ширші соціальні, етичні та політичні параметри». Абсолютно вірний на наш погляд підхід з єдиною поправкою: якщо в основі інформаційного суспільства завжди покладено інформацію та технології її оброблення, поширення, перетворення та передачі, то в основі суспільства знань – завжди процес перетворення інформації в знання.

Варто також, на нашу думку, акцентувати увагу, що існуючі форми та способи комунікацій, характерні для суспільства знань, здійснюються задля задоволення потреб, реалізації інтересів і цінностей особи й суспільства, а не заради інформаційної взаємодії як такої. Саме це, вважаємо, і є ціннісним

самопізнанням під час аналізу інформаційної картини світу. Саме в цьому полягає сутність аксіологічного підходу до вивчення інформаційної сфери – процесів, взаємодії, обміну, продукції, послуг тощо, які ми розглядали к попередніх розділах нашої роботи.

При формуванні інформаційної картини світу ціннісними міркуваннями неодмінно охоплюється широке коло явищ і проблем, амплітуда оціночних суджень щодо яких може бути вельми значною, аж до протилежних. Це стосується, скажімо, оцінювання беззаперечної користі чи абсолютної шкоди чого-небудь, кібербезпеки чи кіберризиків і загроз тощо.

Отже, розвиток суспільства знань – це не лише матеріалізація технологічних досягнень в інформаційній сфері, а передовсім прогрес самої соціальної структури людської спільноти, котра прагне до все повнішої задоволення своїх потреб у цій царині. А втім, розбудова інформаційного суспільства ще більшою мірою зумовлена еволюцією людини як носія соціальних цінностей, розвитком творчих потенцій особи, її здатності до критичного мислення, зростанням індивідуалізації, обсягів особистих та громадянських прав і свобод, демократичних основ організації суспільного життя, формуванням інформаційної культури. Важливим аспектом у розвитку суспільства знань є наявність кіберпатріотизму, під яким ми розуміємо набуту суспільством систему характеристик, що постійно розвивається в процесі комунікацій як через вплив різних інституцій громадянського суспільства, ЗМІ та ін., є усвідомленням суспільством своєї приналежності до нації, високим духовно-моральним ставлення громадянин до своєї Батьківщини, яке виявляється в активній і цілеспрямованій діяльності з пропаганди національних інтересів, відстоювання їх у кіберпросторі та високим рівне інформаційної культури. Невід’ємним елементом кіберпатріотизму є національна самосвідомість, під якою ми розуміємо глибоке усвідомлення суспільством своєї приналежності до української нації.

Із соціально-економічного погляду передумовами прогресу суспільства знань є вільний розвиток індивідуально-творчої конкуренції, коли з-поміж

соціально спрямованих технологій обираються найкращі та найефективніші. З огляду на примат вільної творчості до числа атрибутивних передумов удосконалення інформаційного суспільства слід віднести також соціальне забезпечення, медицину, освіту, культуру, тобто ті галузі, котрі забезпечують поступальний і безпечний розвиток особистості, життєдіяльність людини.

Соціально-політичними засадами розвитку суспільства знань є безперечно, перманентна демократизація політичного ладу, формування громадянського суспільства, толерантність і плюралізм, пріоритет прав і свобод людини.

Без втілення наведених вище цінностей як атрибутів суспільства знань та інформаційної картини світу недосяжним є формування нового типу соціуму, котрий ґрунтується на глобальних інформаційних комунікаціях (взаємодії та обміні). Відображенням аксіологічного підходу саме і є наведений аспект розгляду, який виходить із засадничих особистісних і соціальних цінностей. І як слушно зауважують О.П. Дзюбань та С.Б. Жданенко усе суспільство стає системою освіти, протягом усього життя людина повинна отримувати нову освіту [297, с. 64].

Інновації є не просто популярним віянням сучасності, а однією із фундаментальних цінностей інформаційної епохи, може свідчити хоча б різке зростання попиту на високотехнологічну інноваційну продукцію. Знаннєва економіка базується на найпрогресивніших, найсучасніших, інноваційних досягненнях, а стрімке впровадження відповідних технологій сприяють тому, що найважливішими складовими сучасного ринкового продукту (товарів, послуг) стають знання й інноваційність.

У теперішній час економіка все більше тяжіє до сфери надання послуг, а не, як раніше, до товарного виробництва. Інформаційна епоха зумовлює зміщення пріоритетів від матеріальної товарної форми, фізичного існування засобів виробництва, капіталів, техніки тощо до інноваційно-технологічної, тобто інтелектуальної, розумової, знаннєвої, інформаційної. Мало того, сучасна економіка все більше охоплює увесь світовий простір, долаючи

географічні перешкоди й національні кордони, як зазначає багато вітчизняних і зарубіжних фахівців [258]. Відтак, економіка, заснована на знаннях, є передовсім економікою епохи інформаційної, економічної й культурної глобалізації.

Розв'язання проблеми забезпечення глобальної кібербезпеки лежить у площині створення умов захищеності особи як суб'єкта глобального інформаційного суспільства від внутрішніх і зовнішніх загроз. Тому вбачається за доцільне детальніше дослідити специфіку інформаційного суспільства в контексті створення належних умов для реалізації людиною усіх своїх прав і законних інтересів, усебічного особистісного розвитку.

У науковий обіг термін «глобалізація», котрий сьогодні невіддільний від «інформаційного суспільства», запровадив у 1985 році американський соціолог Р. Робертсон [298-299]. А об'єктивно світові глобалізаційні процеси, котрі характеризуються створенням єдиного інформаційного простору при високому рівні реального інформаційного обміну, почали проявлятися у 1970-80-х роках [300-301].

У теперішній час спостерігаємо підвищення дискретності глобального розвитку, загальної конкурентної боротьби з активним застосуванням політичних, економічних, військових, а також інформаційних важелів, нерівномірне поширення благ, створюваних завдяки глобалізаційним процесам, та певних їх негативних наслідків.

Сутність феномену глобалізації полягає у становленні загальносвітових відносин і зв'язків, універсалізації, що охоплює усі сфери життєдіяльності. Цей процес стосується усього людства без винятку й об'єктивно зумовлений опосередкуванням глобального простору загальним світовим господарством, екологічними проблемами, всесвітніми інформаційними комунікаціями тощо. Зрозуміло, що в контексті становлення інформаційного суспільства визначальним є розвиток глобальних комунікацій, котрий своєю чергою спричиняє виникнення нових проблем загальносвітового масштабу.

Як бачимо, провідна суспільна тенденція сучасності – глобалізація

сприяє загальному інформаційному інтегруванню в усіх сферах людської життєдіяльності. Відтак, глобалізаційна суспільна динаміка вбачається надзвичайно важливим гуманітарним і цивілізаційним феноменом, котрий об'єктивує інформаційну взаємозалежність сучасних і наступних людських поколінь незалежно від раси, релігійних, політичних чи інших переконань. Таким чином, глобалізація інформаційного суспільства є великомасштабним, багатоманітним і водночас суперечливим феноменом зростання уніфікаційних процесів у соціальній, економічній, політичній, правовій та інших глобальних системах.

Зазначені тенденції потребують належного законодавчого забезпечення. Це зумовлено, зокрема тим, що глобалізаційні процеси сучасного етапу розвитку інформаційного суспільства активно стимулюються прогресом інформаційно-комунікаційних технологій, що, своєю чергою, означає виникнення зростаючого кібернетичного трафіку. Завдяки розширенню технологій і засобів впливу безперервно вдосконалюються канали інформаційних комунікацій, а виробники інформаційного продукту активно користаються цими можливостями для впливу на людей, а не лише для того, щоби зробити інформацію доступною для кожного члена суспільства. При цьому жорстка конкуренція в кіберпросторі зумовлює не лише інтенсифікацію інформаційних потоків, а і їхній наступальний характер стосовно споживача. Тобто, такі потоки, впливаючи на його особистість, формують суспільну думку, імідж різних суспільних об'єктів і феноменів, підбурюючи людину до реакції у відповідь.

Сукупність персональної інформації стає в сучасному глобалізованому інформаційному світі чи не найважливішою властивістю людини. Така інформація неминуче накопичується й фіксується в кіберпросторі, може викривлятися, доповнюватися фейковими даними, спотворюватися, що завдає шкоди людині в сенсі порушення її репутації, конфіденційності тощо. Відтак особа втрачає персональну захищеність у глобальному кіберсередовищі, котре не має не тільки державних, культурних, мовних кордонів, а й часто-густо будь

яких морально-етичних обмежень. І для захисту вказаного атрибуту особи самих лише технічних та програмних засобів замало.

Як бачимо, перехід у віртуальне кібернетичне середовище все більшої й більшої частини міжособистісних комунікацій, а також зв'язків особи із суспільством та державою значно підвищує вразливість людини у глобалізованому світі. Оскільки динаміка глобалізаційних інформаційно-комунікативних процесів характеризується значною інтенсивністю й великою швидкістю поширення і зворотної реакції ретельного наукового дослідження потребують вдосконалення правові аспекти забезпечення кібербезпеки в умовах інформаційного суспільства. Усе це зумовлює зростання потреби світової спільноти своєчасно отримувати об'єктивну, достовірну інформацію щодо соціально-економічних, політико-правових та інших процесів. Ця обставина вбачається однією з атрибутивних особливостей широкомасштабного впровадження інформаційно-комунікаційних систем у контексті сучасних процесів глобалізації. Тому величезного значення набуває правове забезпечення кібернетичної безпеки, котре істотно впливає на стан правових і політичних систем усіх світових держав, у тому числі й на процес розвитку інформаційного суспільства у світі.

Залученість будь-якої держави до глобалізаційних процесів передбачає, насамперед, чітку інституціоналізацію відповідної державної інформаційної політики, її стратегічної мети, а саме: розвиток відкритого інформаційного, кібернетичного простору, зокрема за рахунок інтеграції у відповідний світовий простір; еволюцію інформаційного суспільства; вдосконалення національних законодавств у сфері інформації та інформаційно-комунікаційних технологій, кібербезпеки на основі світових тенденцій і міжнародно-правових актів. Таким чином, сучасні глобалізаційні процеси надзвичайно актуалізують проблеми забезпечення інформаційної, кібернетичної безпеки як на міжнародному, так і внутрішньодержавному рівнях.

Спираючись на викладене стосовно інформаційного суспільства,

спробуємо виокремити його ключові ознаки. Це, по-перше, наявність високорозвинених інформаційних технологій, їх значну поширеність серед населення, у бізнесових колах, в державних і самоврядних органах. По-друге, це отримання пересічними громадянами та іншими суб'єктами суспільства очевидних переваг від застосування новітніх інформаційних технологій, а саме: вільного й рівноправного доступу до інформаційних ресурсів і кібернетичних технологій; розвитку інформаційно-телекомунікаційних систем, баз даних, мереж тощо; упровадження інноваційних технологій, зокрема, підвищення за рахунок цього ефективності роботи органів державного управління й місцевого самоврядування при неодмінному забезпеченні інформаційної, кібернетичної безпеки особи, суспільства й держави.

Сьогодні питання правової регламентації низки проблем, пов'язаних з використанням кіберпростору, мережі Інтернет, дискутуються не лише науковою спільнотою й політиками, а й широкою громадськістю. Це, зокрема: «право бути забутим», або право на «цифрове забуття»; право на недоторканність приватного життя, збереження персональних даних та багато інших.

Спробуємо з'ясувати сучасний стан справ із забезпеченням кібернетичної безпеки, сприятливого кіберпростору в умовах функціонування глобального інтернет-середовища й відповідних комунікацій.

У цьому контексті слід зазначити, що однозначної відповіді на ключове питання стосовно того, що таке Інтернет, немає й до сьогодні. Утім, можна виокремити такі його головні ознаки, зумовлені специфікою кіберпростору:

- транскордонність;

- анонімність у віртуальному просторі;

- можливість уникнути контролю й правової відповідальності шляхом, зокрема, обходу режимів, визначених національними законодавствами, та судової юрисдикції своєї країни (приміром, використання зон .com, .net, .org, .ag, .sc та інших найбільш вільних інтернет-зон);

- ієрархічність і зональна структуризація. Мережа Інтернет являє собою просторове утворення з ієрархією різних суб'єктів: структур реєстрації доменних імен й асиметрично розподілених багатьох посередників – інформаційних, торговельних, інтернет-провайдерів та інших, котрі забезпечують користувачам (споживачам інформації) можливість доступу до інформаційних ресурсів мережі;

- динамізм розвитку, постійне зростання й удосконалення діалоговості та взаємодії;

- наявність величезної кількості електронних з'єднань і комунікацій, розширення інтерактивних інформаційних зв'язків (наприклад, мережева угода).

Що стосується регуляторів поведінки учасників мережі, себто відносин, що виникають у кібернетичному інтернет-просторі, то правники виокремлюють такі їх типи: прямі законодавчі; соціальні (корпоративні) норми; ринкові й конкурентні закони; технічні й технологічні норми. А з огляду на те, що законодавець зі своїми правовими приписами не встигає за стрімким розвитком власне Інтернету й міжсуб'єктних відносин у мережі, то регулювання переважної частини вказаних відносин відбувається за так званими «інтернет-звичаями» – усталеними діловими традиціями.

У деяких країнах тривають дискусії стосовно доцільності прийняття національних законів про Інтернет, обґрунтовуючи це певною специфікою відносин, що складаються в мережі. До цих особливостей належать, зокрема, такі:

- специфічний суб'єктний склад – відносини в мережі можуть виникати між особливими суб'єктами, такими як розробники мереж, провайдери, оператори зв'язку, міжнародні структури, які опікуються розвитком інтернет-протоколів, та інші;

- діяльність суб'єктів відносин в Інтернеті може регламентуватися різними національними нормами, позаяк і самі ці суб'єкти можуть перебувати в різних країнах;

- без застосування інформаційно-комунікаційних технологій і мереж неможливі відносини в Інтернеті, які виникають з приводу інформації, котра в ньому циркулює, тобто мають інформаційну сутність. Відтак, об'єктом таких відносин є не будь-яка інформація, а лише та, що обробляється, розміщується чи зберігається у кібернетичному віртуальному просторі;

- на сучасному етапі суспільного, державного й технологічного розвитку інтернет-відносини виникають у сфері автоматизації управління різноманітними інформаційними системами, зокрема такою складною кібернетичною системою, якою є всесвітня мережа Інтернет.

Оскільки Інтернет у купі із сукупністю ПЕОМ створює технологічну основу реалізації міжнародної концепції всесвітнього інформаційного суспільства, то при формуванні системи правового регулювання відповідних суспільних відносин слід враховувати низку важливих обставин, зокрема:

- Інтернет є сукупністю мереж різного географічного розташування, а тому не має будь-якого власника;

- оскільки маршрутизатори інтернет-мереж не мають єдиного зовнішнього управління, Інтернет неможливо повністю вимкнути;

- Інтернет став загальнолюдським надбанням;

- Інтернет надає користувачам широкі можливості, котрі можуть бути використані зацікавленими особами як на благо, так і з протиправною метою;

- мережа Інтернет – це насамперед загальний засіб відкритого зберігання та розповсюдження інформації, вільного й рівноправного доступу до неї, з огляду на що нещодавно виникли такі поняття, як «електронна демократія», «інтернет-демократія» («e-democracy», «Internet democracy» [302]);

- аналогічно до телефонних комунікацій Інтернет може зв'язати кожен комп'ютер з будь-яким іншим, підключеним до мережі. Інтернет-сайти поширюють інформацію індивідуально, з ініціативи користувача, на кшталт телефонного автовідповідача;

- інформація в кіберпросторі Інтернету поширюється за тим же

принципом, що й чутки у людському середовищі: якщо вона викликає значний інтерес – розповсюджується швидко серед широкого кола суб'єктів, коли ж інформація мало кому цікава, то й поширення її мінімальне й повільне.

Мережу Інтернет складають мільйони комп'ютерів індивідуальних користувачів, корпоративних, урядових, наукових та приватних мереж. Упровадження так званого протоколу IP (Internet Protocol) і принципу маршрутизації пакетів даних уможливило об'єднання мереж різної будови та розміщення. У цьому разі протокол – це своєрідна єдина комп'ютерна «мова», алгоритм, правила передачі даних між вузлами комп'ютерної мережі, котрі під час роботи в мережі використовуються комп'ютерами для обміну даними, аби «розуміти» один одного. Найпопулярнішим з-поміж значного числа кількості інтернет-протоколів які використовуються в мережі, таких як Arcnet, ATM, BGP, DNS, EIGRP, Ethernet, Frame relay, FTP, HDLC, HTTP, HTTPS, ICMP, IGMP, IMAP, IP, IS-IS, L2TP, LDAP, OSPF, POP3, PPP, RIP, SLIP, SMTP, SNMP, SSH, SSL, TLS, TCP, Telnet, Token ring, UDP, XMPP та інших [303]), є протокол передачі гіпертексту, який використовується для пересилання з одного комп'ютера на інший веб-сторінок – HTTP (Hyper Text Transfer Protocol). Саме він є базовим для так званого «вебу», або «www» («World Wide Web» – «всесвітня павутина»). Цим терміном зазвичай позначають розподільну систему, котра надає користувачам мережі доступ до розташованого на різних комп'ютерах, підключених до Інтернету, аудіовізуального контенту. Звісно, вказаний протокол є лише однією із багатьох аналогічних розподільних систем.

У зв'язку із глобалізацією інформаційного використання кібернетичного простору, у формуванні відповідної міждержавної інфраструктури виникає чимало нових складних проблем у сфері забезпечення безпеки людини, суспільства й держави. Переважну більшість із них можливо розв'язати винятково шляхом удосконалення відповідних міжнародного й національних законодавств, ефективного міжнародного співробітництва для ліквідації безпекових викликів і загроз у кіберпросторі, налагодження дійового

контролю за їхніми джерелами.

Серед основних сучасних кібервикликів і кіберзагроз глобальному інформаційному суспільству слід, на нашу думку, назвати такі: деструктивний вплив на різних суб'єктів (пропаганда); економічна свобода; зіткнення культур; правозастосовні проблеми в умовах кібернетичної транскордонності; надмірна соціальна мобільність, інформаційне відчуження, сугестія, зомбування.

Спробуємо стисло охарактеризувати окремі із цих загроз.

Зіткнення культур. Одним із очевидних результатів широких комунікаційних взаємин представників різних етносів і культур, активного поширення уніфікованих масових культурних стандартів є зближення світосприйняття людьми різних континентів, рас і національностей, їх відхід від давніх традицій своїх народів, втрата ними своєї унікальної ідентичності. Крім очевидних позитивних аспектів такого зіткнення культур, воно призводить до загострення конфліктів на етнічному, релігійному та іншому ґрунті, до виникнення різноманітних радикально настроєних угруповань, провокує прояви агресії і створює можливості керування ними у глобальному інформаційному, кібернетичному просторі. Сприяючи швидкій інтеграції, взаємному проникненню різних культур, інформаційні можливості кібернетичного простору зумовлюють також загострення у такому змішаному світі суперечностей і конфліктів. Народи менш розвинутих країн відчувають загрозу своїй ідентичності від представників більш «просунутих» держав, що створює ґрунт для проявів фундаменталізму й екстремізму, зростання соціально-політичного напруження.

Крім того, надмір інформації у кіберпросторі, значна частина якої дуже сумнівної якості, а то й відвертий спам і фейки, серйозно впливає на ефективність традиційних механізмів комунікації органів публічної влади із громадянами. Йдеться насамперед про виборчий процес, засоби масової інформації, система зв'язків із громадськістю (т. зв. public relations) тощо. Щоб державне управління не втратило дієвість, потрібно вживати до нових форм і

методів керування соціально-економічними, політичними та іншими процесами, створювати нові або кардинально реформувати старі управлінські структури.

Створення нової глобальної ідентичності, котре веде до зникнення унікальності окремих народів, етносів і груп, зумовлює виникнення нових, ще більш гострих глобальних суперечностей і конфліктів. Адже далеко не всі люди можуть спокійно сприйняти нові глобальні цивілізаційні цінності (в основі яких об’єктивно лежить превалювання певної нації), пустивши в непам’ять традиційні цінності власного народу. Саме це призводить до виникнення великих, розгалужених агресивних утворень терористичного спрямування. І незалежно від кількості, щільності та географії проживання своїх прихильників ці угруповання використовують кіберпростір для просування, пропаганди своїх ідей та координування зловмисних дій.

Особливий вплив глобалізаційні процеси мають на молодь, на формування у неї відповідних цінностей, життєвих настанов і принципів, які можуть суперечити культурним засадам і традиціям їхніх народів, порушувати зв'язок поколінь. Відтак, розбіжності окремих культур, їх особливостей і традицій спричиняють негативне ставлення, несприйняття інших культур взагалі, нетерпимість до їх представників. Домінуючим стає запит на подолання усіх існуючих перешкод, відмову від традиційних національних цінностей і підвалин, загальне змішування й інтеграцію.

Економічна свобода. Яскравим прикладом може слугувати виникнення так званих цифрових валют – електронних грошей, випуск яких не здійснюється жодним банком і не має правових регуляторів. Це створює передумови зростання тіньової економіки, котра не контролюється державними фінансовими органами. Під час будь-яких розрахунків між економічними суб’єктами таку цифрову валюту неможливо відкликати, вона не контрольована, а тому не підлягає вилученню чи блокуванню. За таких умов відсутності регуляторних механізмів унеможливлюється облік підозрілих фінансових операцій. Відтак, виникають умови, які сьогодні часто вже

реалізуються, для «відмивання» грошей, боротьби з владними структурами держав, підтримки тероризму в різних регіонах світу за допомогою цифрових валют.

Як бачимо, головну загрозу при використанні таких валют становить відсутність правового регулювання цього процесу, контролю за ним, що приваблює до них як окремих зловмисників, так і організовану злочинність.

Сучасні потенції транскордонного використання кіберпростору нівелюють можливості національних законодавств, державного контролю й економічного впливу. У такій ситуації концентруються як потужні можливості так і серйозні деструктивні ризики, котрі здатні завдати значної шкоди для реалізації законних інтересів людини в глобальному інформаційному світі. Про це свідчить низка проблем, таких як:

ідентифікації;

спотворення результатів електронного голосування;

технологічні негаразди під час створення систем електронного врядування й електронної демократії;

недостовірності баз даних; незахищеності конфіденційної інформації та персональних даних у процесі надання державних адміністративних послуг;

зловмисного використання вказаних даних під час здійснення електронного судочинства; поширення шкідливого, незаконного контенту, котрий становить загрозу для життя і здоров’я людини й дезорієнтує її;

оприлюднення електронними засобами масової інформації відомостей, які паплюжать честь і гідність людини;

викрадення інформації, що використовується у фінансово-банківських установах (інтернет-банкінг);

втрата інформації через зловмисні кібератаки під час користування інтернет-мережею тощо.

Реальні загрози глобальному інформаційному суспільству й кожній людині несуть:

мілітаризація кіберпростору,

розв’язування широкомасштабних інформаційних війн,

поширення екстремістських і маніпулятивних матеріалів,

деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо.

Убачається, що в таких умовах успішне розв’язання вказаних глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об’єднаних плідних зусиль усього світового співтовариства.

4.2. Правовий чинник у попередженні кіберзагроз сучасному українському суспільству

Немає жодних сумнівів, що дія інформаційних технологій, користування кіберпростором не мають становити небезпеку для людини, суспільства й держави. Проте громіздкий, неповороткий законотворчий механізм хронічно не встигає за стрімким розвитком цієї сфери, а тому вона залишається практично поза правовим полем. Відтак, вагомим фактором, котрий знижує ефективність використання кібернетичного простору, функціонування в інформаційному середовищі, вбачається, окрім одвічного людського чинника, відсутність належної нормативно-правової бази.

Тотальна інформатизація, створення глобальних інформаційно-телекомунікаційних мереж торкнулися всіх сфер людської життєдіяльності. Але насамперед, на нашу думку, відповідні юридичні лакуни викликали проблеми у таких галузях як комп’ютерні правопорушення, захист таємниці, власність, фінанси і банківська справа, контрактне право, авторське право, безпека даних, транскордонні інформаційні потоки, безпека даних, захист особистої інформації й персональних даних та ін.

Комп’ютерні технології дають змогу оперувати величезними обсягами різноманітної інформації, отримувати, передавати, зберігати не лише текстово-графічні матеріали, а й аудіо- й відеодані, причому з будь-якого цифрового пристрою, підключеного до мережі, й практично миттєво. Тому оформлення цього феномену в нові юридичні межі вбачається нагальним завданням державної політики.

Як засвідчила суспільно-політична й державно-управлінська практика, при розробці правової регламентації функціонування вказаної сфери слід орієнтуватися на довготермінову перспективу. Низька ефективність усталених юридичних інструментів у регулюванні актуальних суспільних відносин, особливо у сферах, де найбільше застосовуються новітні інформаційні технології, зводить нанівець спроби влити молоде вино нової культури у старі міхи існуючого правопорядку. Так, радикальних змін зазнають такі, здавалося б, довершені правові галузі, як конституційне, авторське, патентне, контрактне право. Оскільки раніше не існувало юридичних норм стосовно злочинів, здійснюваних за допомогою високих технологій, серйозних змін зазнає кримінальне і кримінальне процесуальне право. І цей перелік можна продовжувати.

Результати аналізу практики правового регулювання сфери кібернетичної безпеки дає підстави виокремити дві групи проблем, котрі, вважаємо, потребують невідкладного й кардинального розв’язання. Це, по-перше, питання виконання відповідного законодавства. Так, більшість фахівці відзначають, що недосконалим є саме це законодавство, зокрема щодо кваліфікації комп’ютерних злочинів і призначення покарання, а також труднощі у його застосуванні [304-307].

По-друге, це питання, що стосуються узгодження національного законодавства й міжнародно-правовими нормами з відповідними стандартами правозастосування. Транскордонність і транснаціональність глобальної мережі серйозно утруднює реалізацію приписів національного законодавства й контроль за його дотриманням, спричиняє юрисдикційні суперечності при

розв’язанні багатьох питань – технологічних, технічних, економічних, культурологічних та інших, які виникають при використанні кіберпростору. Саме функціонування Інтернету зумовлює кардинальні зміни в міждержавних стосунках, потребує переведення співпраці держав і міжнародних структур на більш високий, якісно новий рівень.

Таким чином, нові реалії інформаційного суспільства зумовлюють виникнення перед світовою спільнотою сукупності проблем і завдань, розв’язання яких лежить у міжнародно-правовій площині. Варто при цьому зазначити, що всі ці питання тісно переплетені та взаємозалежні. Приміром, на міжнародну правозастосовну практику негативно впливають недосконаліть національного законодавства, неузгодженість його норм з міжнародними. Водночас національне правове регулювання наштовхується на певні міжнародно-правові обмеження.

Характерно, що до потреби правового регулювання використання кіберпростору останнім часом усе більше схиляються навіть ті адепти Інтернету, котрі раніше палко обстоювали його вільності. У цьому контексті нерідко йдеться про певне специфічне регулювання, виходячи з особливостей Інтернету й кіберсередовища загалом. У дискусіях з цього приводу з’явився термін «інтернет-контроль», який передбачає такі рівні: доступ до електронної мережі; операторність (функціональність) мережі; діяльність у кіберпросторі [308-310].

На нашу думку, проблеми, якими покликаний опікуватися вказаний контроль, стосуються здебільшого соціальної й морально-етичної сфер. Це, скажімо, комп’ютерні шахрайства й крадіжки, спостереження (зокрема, й за приватним життям), пропаганда расизму, ксенофобії, практичні рекомендації щодо створення вибухівки, зброї та набоїв, інформація, котра ганьбить людську честь і гідність, суспільну мораль тощо. Зазначимо також, що ухвалення рішення стосовно особливого контролю за використанням кіберпростору знаменує собою усвідомлення суспільством потреби державно-правового регулювання суспільних відносин, які виникають у сфері

застосування інформаційно-комунікаційних технологій.

Слід торкнутися ще однієї важливої проблеми. Керовані комп'ютерною технікою автоматизовані кібернетичні системи стають сьогодні повноцінними суб'єктами інформаційної взаємодії. Можна стверджувати, що нинішній світоустрій утворено саме за допомогою розумних машин, штучного інтелекту. Відтак, серйозну небезпеку може становити можливість шляхом віддаленого управління через вказаних суб'єктів делегувати певні повноваження, реалізовувати, чи навіть їх перекручувати та спотворювати. Тому сьогодні в умовах тотального поширення інформаційно-телекомунікаційних технологій, використання кіберпростору часом важко визначити справжнє джерело управління й контролю – людина це чи машина й виявити при цьому якісь відмінності. «*...нові машини двадцятого століття,* – писала ще кількадесят років тому одна із засновниць так званого кіберфемінізму, професорка Каліфорнійського університету Донна Харауей, – *зробили неоднозначним розмежування природного і штучного розуму й тіла... Потенції наших машин усе зростають, натомість ми самі лишаємося страхітливо інертними*» [311].

З огляду на це, аналізуючи проблеми використання кіберпростору, роботу глобальної електронної мережі, котра є своєрідною технологічною картою, вважаємо за доцільне особливу увагу приділити можливостям кіберсистем, мікрочіпів, гібридів, нанотехнологій. У глобальному інформаційному суспільстві впровадження таких недержавних суб'єктів в інформаційну взаємодію, в управлінські процеси, в життєдіяльність «цифрової» людини й соціуму вбачається неминучим. Мало того, цілком імовірно, що сама держава й громадянське суспільство як такі втратять свою актуальність, позаяк штучний інтелект і подібні кіборги непомітно, поволі, але ефективно переберуть до своїх рук управління. Тому актуальність проблем щодо влади, впливу, контролю в контексті використання кіберсередовища не викликає сумнівів, а особливо правовий чинник, який має стати надійним регулятором подібних процесів.

Отже, на нашу думку, глобальне проникнення Інтернету в усі сфери життєдіяльності аж ніяк не означає, що держава втрачає здатність контролювати суспільство, що відбувається зумовлена інформаційними технологіями трансформація влади, її глобалізація у віртуальному просторі. Навпаки, як і в «реалі», у кіберпросторі, окрім комп'ютерних технологій, національні закони, традиції та звичаї не менш важливі. Саме на спроможність впливати та стежити за дотриманням законів у глобальному просторі спираються зорієнтовані на державу підходи до розв'язання багатьох зазначених вище питань. На обстоювання інтересів людини й суспільства, забезпечення їхньої кібернетичної безпеки спрямоване осягнення процесу управління цифровим середовищем, котре передбачає триєдність: незалежність – дисципліна – право [312].

Важливим напрямом, галуззю законодавства у сфері безпеки стає боротьба зі здійснюваними за допомогою глобальної мережі Інтернет кібернетичними злочинами, котрі завдають серйозної шкоди, але вельми непросто встановити навіть сам факт їх скоєння. Традиційні кримінологічні й криміналістичні підходи, засоби й методи практично безсилі у віртуальному світі, котрий живе за своїми власними законами і правилами. Тому отримати хоча б орієнтовну статистику кіберзлочинів не уявляється можливим, позаяк відсутні будь-які свідчення.

Відтак, слід зазначити, що стосовно визначення складу кібернетичних (комп'ютерних) злочинів фахівці ще й до цього часу не мають одностайності. І це не дивно, адже приписи класичного законодавства, наприклад, щодо власності, котра має бути матеріальною (відчутною, речовинною) й може бути викрадена, змінивши при цьому володільця, втрачають усілякий сенс, коли йдеться про, скажімо, бази даних, програмне забезпечення тощо. Так, шведські правники частіше використовують термін «комп'ютерні зловживання», визначаючи його як інцидент, пов'язаний з комп'ютерними технологіями, коли потерпілий зазнає чи може зазнати шкоди, а зловмисник має зиск або може його отримати.

Ознаки комп'ютерних злочинів можуть збігатися з кваліфікаційними ознаками таких «традиційних» їх видів, як викрадення власності, фінансові злочини, вандалізм та ін. Виникає також питання стосовно розміру шкоди, що при визначенні покарання дає змогу розрізняти тяжкість злочину. Низку складних для розв'язання питань під час провадження справ про кіберзлочини викликає правозастосування чинного законодавства у сфері розкрадань, комерційної таємниці, порушення авторського і суміжних прав, конфіденційності, фальшування документів тощо, яке застосовується для визначення покарання. Так, якщо власник інформації ігнорує безпекові заходи щодо захисту комерційної таємниці чи конфіденційної інформації, то в разі звинувачення у її викраденні може виникнути питання про так зване «незахищене розкриття», котре унеможливлює притягнення до відповідальності.

Ще одним непростим для кваліфікації та визначення складу злочину є несанкціонований доступ до баз секретної інформації, коли інформація не копіювалася, не змінювалася й не використовувалася. Це, приміром, бажання «хакера» продемонструвати свої «видатні» здібності зламувати будь-який захист. Цілком можливо, що при кваліфікації злочину й визначенні покарання відповідь буде знайдена у площині ретельного аналізу кримінально караної «комп'ютерної поведінки». Ще раз підкреслимо, що при визначенні покарання за різні види кібернетичних (комп'ютерних) злочинів, у тому числі й згаданий вище несанкціонований доступ, питання стосовно матеріальності, «речовинності» об'єкта викрадення та ознак володіння ним (які в разі «традиційних» крадіжок є істотними) не розглядаються.

У цьому контексті корисним убачається звернутися до міжнародного законодавства, виокремивши окремі особливості кваліфікації розглядуваних нами злочинів.

Так, із середини 1980-х років правозастосовна практика США поділяє комп'ютерні делікти на злочини проти інтелектуальної власності та несанкціоноване використання інформаційних технологій [313]. Відповідно

до федерального закону Австралійського Союзу несанкціонований доступ до комп'ютерів, насамперед тих, що задіяні у галузях зв'язку й транспорту, вважається кримінальним злочином. Два різновиди комп'ютерних злочинів передбачає законодавство КНР, а саме: поширення неліцензійних програм й умисне зараження системи комп'ютерним вірусом. Низку нормативно-правових актів, спрямованих на запобігання комп'ютерним злочинам і боротьбу з ними, ухвалено у Гонконзі. До кримінально караних правопорушень ці документи відносять злам комп'ютерної системи з корисливою метою чи для заподіяння шкоди, а також несанкціоноване проникнення в ЕОМ через інформаційно-комунікаційні мережі.

Як бачимо, національні кримінальні законодавства у сфері кібернетичної злочинності мають істотні відмінності як у кваліфікації подібних злочинів, так і в питаннях відповідальності за їхнє скоєння. При цьому, зрозуміло, мета й завдання щодо боротьби з комп'ютерними злочинами, проблеми, які виникають у зв'язку з ними, є ідентичними в кожній країні. У тому числі й проблема реалізації в глобальному інформаційному середовищі власної нормативно-правової бази. Ще більші законодавчі ускладнення виникають у країнах з федеративним устроєм, позаяк закони, чинні на певній території, втрачають свою силу у випадку транскордонних інформаційних потоків у кіберпросторі.

Тому не дивно, що на шляху розв'язання зазначених проблем міжнародно-правового регулювання використання кібепрпростору й функціонування Інтернету багато фахівців визнає за доцільне налагодити загальне технічне координування, запровадити універсальну стандартизацію в цій сфері. Дійшовши висновку, що глобальна мережа є передовсім утворенням технічним, дослідники запропонували новий підхід до керування. Зокрема, професор права Стенфордського університету (США) Лоуренс Лессіг вважає, що специфічною правовою базою – регулятором вільної поведінки користувачів Інтернету має бути архітектоніка мережі, котру складають технічні протоколи і програмне забезпечення, що виступають певними

правилами контролю [314, с. 61]. Саме архітектоніка, будова Інтернету зумовлює характер й особливості майбутньої мережі і, відповідно, свобод, гарантованих людині при користуванні нею.

Важливо також, що оформлені як комунікаційні протоколи технічні характеристики підвищують ефективність інформаційно-комп'ютерної комунікації та знижують її вартість. Скажімо, низка оцінювальних специфікацій і стандартів, які розкривають понятєвий апарат, регламентують основні технічні аспекти та пропонують низку безпекових заходів стосовно функціонування комп'ютерних систем тощо, зробили вагомий внесок у створення науково-методологічного підґрунтя у сфері інформаційної та кібернетичної безпеки . Утім технічними аспектами зовсім не вичерпується кібербезпекова проблематика, тим паче, як засвідчила практика, стандартизовані комп'ютерні системи більш уразливі до зловмисних проникнень.

У цьому контексті дослідники правових аспектів глобалізаційних процесів називають низку актуальних питань, які потребують свого розв'язання, Так, Т. Фрейліх ставить, зокрема, питання про суб'єктність інтернет-контролера контенту, програмного забезпечення тощо, які надходять із різних країн, про можливість адекватного реагування країнами на сучасні виклики і загрози в кібернетичному просторі, обмеженнями своїми державними кордонами й національними юрисдикціями [315]. Звідси випливають й похідні проблеми щодо, приміром: належності змісту інтернет-контенту до юрисдикції держави, котра його створила, чи країни-отримувача інформації, компетентісних меж стосовно інформації, «спільної» для декількох країн, тощо.

Отже, сучасна наукова думка більшим пріоритетом вважає питання узгодження використання кіберпростору з міжнародно-правовими нормами поряд із дослідженням інших численних проблем правового регулювання у сфері інформаційних технологій. Цікавим у цьому сенсі є праця П. Маєра, у якій науковець, дослідивши наявні міжнародно-правові обмеження, виділив

ключові напрями розв'язання згаданих вище питань. Це, зокрема, формування загальних принципів діяльності, загальне міжнародне договірне право, загальні міжнародні та міждержавні угоди у сфері користування кіберпростором, координування діяльності всесвітньої мережі Інтернет тощо [316].

Важко не погодитися з дослідником, що протидіяти безлічі конкретних актуальних безпекових викликів і загроз у кібернетичному просторі (кіберзлочинність, загрози критичній інфраструктурі країн тощо) можна значно ефективніше на основі вироблення й дотримання загальних принципів регуляторної діяльності в глобальному інформаційному середовищі. Так, підтриманню положень міжнародних конвенцій про права і основні свободи людини в інформаційну епоху вельми вагомо може посприяти застосування норм договірного права. Основою вироблення міжнародного інструментарію вдосконалення роботи у сфері передання інформації та іншої взаємодії у кіберпросторі можуть стати міжнародні та міждержавні угоди, договори міжнародних спілок. Доцільним убачається також вироблення й ухвалення компетенції різноманітних міжнародних структур щодо координування широкого спектру питань: функціонування ринків телекомунікаційного обладнання, розроблення технічних стандартів, інтернет-адміністрування та ін.

Експертка ЮНЕСКО із Нової Зеландії Е. Лонгворт, підтримуючи ідею укладення вказаної міжнародної угоди, вважає, що вона має передбачати основні положення правового режиму й порядку врегулювання спірних питань у міжнародних судових установах. Дослідниця також пише про необхідність створення розгалуженої децентралізованої структури керування глобальною мережею Інтернет для продовження конструктивного міжнародного діалогу із зазначених питань, що потребує значних спільних зусиль усіх членів світової спільноти. Приєднуються до цієї думки й американські правники, професори Гарвардського й Колумбійського університетів Джек Голдсміт і Тім У, котрі впевнені, що ефективне

децентралізоване керування значно краще стимулює свободу, самовизначення й різноманіття [317]. Наводячи за взірець договір про міжнародні води Антарктики, особливі перспективи Елізабет Лонгворт убачає в реалізації ідеї міжнародного інформаційного, кібернетичного простору. Своєю чергою, застосувати положення про навколоземний простір задля розв'язання юридичних проблем кібернетичного простору, мережі Інтернет пропонує Е. М. Бальсано [318].

Як бачимо, ідея міжнародної співпраці задля вироблення загальних принципів правового регулювання використання кіберпростору, укладання відповідних угод складна й багатоаспектна, вона потребує ретельного дослідження й опрацювання. Утім є всі підстави вважати, що вона буде реалізована.

Крім того, потребу застосування в указаній сфері міжнародних правових актів і міждержавних угод можна, на нашу думку, обґрунтувати потребою уникнення прийняття різними країнами національних норм і законів, які конфліктують між собою, а також необхідністю вироблення універсальних підходів та єдиних стандартів щодо нормативно-правових актів, котрі стосуються інформаційно-телекомунікаційних технологій, користування кіберпростором, мережею Інтернет.

Наявна на сьогодні практика державного регулювання Інтернету, як показали результати комплексного дослідження перспектив його застосування, потребує серйозного подальшого наукового пошуку. Вважаємо, що віднайти дійові форми та методи регулювання соціальних відносин, що виникають при використанні кіберпростору, можна лише на шляху всебічного вивчення проблеми, у тому числі культурних, етичних, морально-психологічних та інших її складових. Таким чином, украй нагальним завдання сучасного суспільства в умовах перманентного підвищення національних і міжнародних безпекових вимог убачається дотримання прийнятих положень. Прикладом застосування суто технічних рішень щодо розв'язання досліджуваних проблем може слугувати наведена нижче ситуація.

Як зазначалося, розвиток глобальних інтернет-технологій відкриває транскордонні можливості для кібернетичних зловмисників. І якщо в певній країні відсутня правова відповідальність за комп'ютерні делікти, то вона має всі підстави відмовити у сприянні розслідуванню подібних злочинів. Задля унормування питань міжнародного співробітництва у боротьбі з кіберзлочинами, створення правого поля кіберпростору Рада Європи в листопаді 2001 року ухвалила Конвенцію про злочинність у сфері комп'ютерної інформації (ETS № 185) [319]. Усі правопорушення у цьому середовищі вказаний документ класифікував на чотири групи, а для їхнього запобігання та припинення на країни-підписанти покладалися певні зобов'язання.

Щоправда, деякі громадські організації, зокрема, американські, британські, іспанські та ін., звернули увагу, що окремі приписи цього міжнародно-правового акта суперечать положенням Європейської конвенції про захист прав людини. У їхній заяві йшлося, що контролем за приватним життям і приватними комунікаціями слід вважати фіксацію й перехоплення інтернет-провайдерами за допомогою технічних засобів інформації в інтересах правоохоронних органів [320].

Упевнені, що в галузі правого регулювання суспільних відносин, які виникають у зв'язку з користуванням кіберпростором, і надалі виникатимуть питання, які потребуватимуть широкого обговорення і зваженого, делікатного вирішення.

На сьогодні фахівці намагаються визначити оптимальні напрями застосування загальних принципів чинної нормативної бази у сфері інформаційних технологій і використання кіберпростору з погляду узгодження національних і міжнародного законодавств з відповідних питань . На нашу думку, до найбільш нагальних для розв'язання у цьому контексті є питання забезпечення безпеки й таємниці даних, а також визнання прав на них.

Варто зазначити, що саме безпеці інформації зазвичай приділяється найбільша увага порівняно із, скажімо, її доступністю. Про це свідчить і вся

світова практика захисту даних. Так, приміром, у Франції Закон про архіви був ухвалений ще в 1760 році, у 1957 році – Закон про таємну статистику, а в 1978 році – Закон про інформацію, записах і свободах, де вперше у світовій законодавчій практиці йшлося власне про інформацію. У Великій Британії перший подібний документ – Офіційний таємний акт – набув чинності у 1911 році.

Водночас, і це теж переконливо доводить історичний досвід, тотальне зосередження інформаційних баз даних у руках держави, брак, а то й повна відсутність суспільного контролю за ними призводять до посилення адміністративних важелів влади бюрократії й технократії. З огляду на це в багатьох країнах свобода інформації є одним із пріоритетів державної інформаційної політики. Законодавство Швеції, наприклад, передбачає вільний доступ громадян до інформації (документації), котра циркулює в центральних та муніципальних органах влади та має суспільне значення [313].

Ефективне розв'язання розглядуваного нами питання таємниці даних лежить у площині формування загальних правових принципів збереження конфіденційності інформації. У цьому контексті поняття «таємниця даних» можна витлумачити як здатність особи контролювати використання інформації, яка її стосується. Цю проблему, як уже зазначалося, серйозно загострили бурхливий розвиток комп'ютерних систем і мереж, застосування інформаційно-телекомунікаційних технологій для оброблення персональних даних. Сьогодні особливо актуально звучить відомий постулат: «*Хто володіє інформацією, той володіє світом*». Тобто, той, хто володіє інформацією про людину, має над нею владу. Відтак, право на недоторканність, конфіденційність особистих даних стає в ряд основних прав людини.

У добу глобальної інформатизації, поширенням Інтернету навіть такі країни Сходу, як, приміром, Китай, Таїланд, Японія та інші, попри свої багатовікові традиції у стосунках держава – особа, що спираються на релігійні догмати, змінюють своє ставлення (й відповідну нормативно-правову базу про охорону даних) до питань приватної, персональної інформації. Так, у 1990-х

роках, з розвитком всесвітньої мережі законодавча база КНР щодо безпеки даних поповнилася такими правовими принципами, «запозиченими» у західної цивілізації: поваги; інформованої згоди; балансу (між недоторканністю приватного життя й безпекою суспільства), а також принципом соціальної ректифікації, тобто очищення [321].

Окремого закону щодо захисту персональних даних немає в Таїланді. Проте і в цій країні планується запровадження цифрових посвідчень особи людини. З цього приводу професор філософії Університету Чулалонгкорна (Бангкок) Сорадж Хонгладаром у контексті конфіденційності персональних даних наголосив, що заперечення буддизмом індивідуального «Я» аж ніяк не означає, що він відмовляється від приватного життя [322].

Вельми складні трансформаційні процеси дискретної самоідентифікації особи відбуваються у суспільній свідомості Японії. Як писав директор Інституту інформації та медіаетики Цукубського університету Макото Накада, нині кожен японець існує в системі трьох світів, які впливають на генезис його особистості. Перший із них (сакаї) – світ сучасних західних цивілізаційних цінностей; другий (секен) – традиційний національний світогляд; третій – порочний світ зла з усіма об’єктивними й суб’єктивними негараздами, що він несе [323].

Таким чином, поступово усвідомлюючи потребу захисту персональних даних в епоху інформаційного суспільства, світогляд Сходу, який кардинально відрізняється від західного егоцентризму, приєднується до системи глобальної інформаційної комунікації.

Сьогодні різноманітні дані про людину потрапляють і циркулюють у складних розгалужених мережах, принципи функціонування й потенціал яких розуміє вельми незначне коло фахівців. Тому пересічна людина, довіряючи інформацію про себе, сподівається на державу, на правовий захист своїх законних інтересів, на те, що всі суб’єкти інформаційних відносин належним чином оперують персональними даними, що їх не буде використано на шкоду особі. В умовах поширення автоматизованих систем питання захисту таємниці

даних набуває особливої ваги. Адже надзвичайні потужності, швидкості й можливості сучасних інформаційно-телекомунікаційних технологій, їхня відносна дешевизна, сприяючи створенню величезних за обсягом баз даних, систем запису, значно полегшують доступ до особистої інформації, роблять її вразливою до зловмисних зазіхань. Сучасні цифрові технології дозволяють маніпулювати цими даними у непередбачуваний спосіб, отримувати до них доступ особам чи структурам, які не мають на це права і можуть їх використовувати зі своєю, не завжди безпечною, метою, відмітною від первісного призначення.

Отже, безпеку й таємницю даних неможливо роз'єднати. То ж створення оптимального співвідношення між правом особи на захист від зловживань її персональними даними й небезпекою несанкціонованого доступу до конфіденційної інформації є, на нашу думку, важливим аспектом інформаційної політики всіх держав у сучасних умовах.

З огляду на викладені вище обставини в багатьох країнах розробляються й ухвалюються нормативні документи щодо захисту конфіденційної інформації, зокрема фінансово-банківської таємниці. Так, принципам збереження конфіденційності відомостей стосовно клієнтури присвячений закон США про модернізацію фінансового обслуговування (так званий закон Грема – Лінча – Блайлі). У 1996 році безпекові стандарти конфіденційності, цілісності й доступності даних про здоров'я людей затверджено також законом Сполучених Штатів Америки про підзвітність документації щодо страхування здоров'я.

Убачається за доцільне з метою підвищення дієвості інформаційно-безпекових заходів сформулювати основні загальні принципи, які мають ураховуватися у законотворчості та правозастосовній практиці усіх держав, котрі прагнуть до формування правової бази регулювання інформаційних відносин (збирання, оброблення, поширення, доступ, конфіденційність, захист тощо). Це, по-перше, забезпечення інтересів особи, суб'єкта персональних відомостей, а саме:

– інформування особи про характер та обсяг її персональних даних, котрі потрапляють у систему, про суб'єктів, мету, спосіб, час і тривалість їх використання;

– оперування персональними даними з обов'язковим урахуванням прав і основних свобод людини й виключно у визначених законом межах і цілях;

– користування лише тим обсягом персональних відомостей, який потрібен для конкретної дозволеної мети;

– забезпечення повноти, достовірності й часової відповідності наявних в інформаційних системах даних;

– забезпечення права людини знайомитися з наявними в інформаційних системах даними, котрі їх безпосередньо стосуються;

– забезпечення права суб'єктів персональних відомостей вносити виправлення у дані про себе інформаційних системах.

По-друге, це забезпечення інтересів суспільства й держави, а саме:

– законодавче закріплення умов і порядку доступу до відомостей конфіденційного, приватного й персонального характеру;

– запобігання несанкціонованому втручанню, видозміні чи спотворенню інформації у відповідних базах даних;

– раціональна цінова політика щодо інформаційних послуг і доступу до інформації.

Уважаємо, що з-поміж прав людини у контексті конфіденційності відомостей можна виокремити такі основні: на контроль, на інформування, на коректне використання, на перевірку й на зміну (виправлення) даних.

Виходячи із цього, є всі підстави стверджувати, що розв'язання проблем збереження й безпеки даних, розширення цифрових комунікацій лежить у площині розвитку відповідної нормативно-правової бази, що передбачає, зокрема, дотримання певних стислих приписів:

– дотримання високих режимів утаємничення щодо чітко визначених категорій відомостей;

– оперування даними виключно із законною метою, передбаченою

законодавством країни походження чи використання інформації;

– забезпечення безпеки важливих даних достатніми й доцільними правовими й технічними засобами.

Ще одним важливим аспектом забезпечення належного безпекового контролю є питання правоналежності даних. Визнання цього права означає насамперед дотримання норм авторського і суміжних прав, дозвільних документів та обмежень щодо окремих категорій відомостей з метою створення оптимальних умов для ефективного користування інформацією, в тому числі в кіберпросторі. Класичне авторське, патентне право та інше законодавство про інтелектуальну власність захищало здебільшого не власне зміст відомостей, а передовсім носія інформації. В епоху цифрових технологій, які позбавляють інформацію свого фізичного втілення, ситуація докорінно змінилася. Нині будь-хто може подивитися фільм чи прочитати книжку без відвідин кінотеатру чи книгарні з бібліотекою. «Торгівля інформацією містить внутрішню суперечність. Покупцеві, котрий дізнався про те, що він купує, тепер не потрібно придбавати цю інформацію, позаяк він нею вже володіє. З іншого боку, попри те, що створення і придбання інформації може бути вельми витратним, відтворювати її можна доволі дешево». Відтак, у галузі виробництва інформаційного продукту однією із найскладніших, як із правового, так і з морально-етичного поглядів, є проблема захисту інтелектуальної власності, котра залишається нагальною для сучасного суспільства загалом.

Законодавство про захист авторських прав в інформаційній сфері має свою специфіку для різних країн і правових систем, про що засвідчив аналіз усталених підходів до питань власності взагалі й інтелектуальної власності зокрема. Приміром, забезпечення насамперед моральних прав автора, нерозривності ланцюга автор як особистість – авторська праця – репутація лежить в основі європейської традиції. Натомість у Британії й США ключовим у цьому сенсі є поняття «майно» й, відповідно, «майнові права». Тому предметом захисту авторського права в цих країнах є «оригінальні авторські

твори, втілені в будь-яких матеріальних засобах (UCC, 1952 р.). В азійському ж регіоні процес репродукування програмного продукту розглядається переважно як авторське бажання перевершити конкурента. Подібні морально-етичні погляди на різні аспекти інформаційної комунікації відбиваються у національних законодавствах країн цієї групи.

У теперішній час правознавці, зокрема теоретики інформаційної безпеки, відзначають такі найбільш уразливі ланки в існуючій системі захисту інтелектуальної власності. Це, по-перше, те, що наявне на сьогодні відповідне законодавство можна застосовувати до нинішніх реалій у сфері інформаційних відносин і використовувати кіберпростір хіба що за аналогією. По-друге, захист права на інтелектуальну власність практично унеможливлює постійний розвиток нових і вдосконалення наявних технологій відтворення інформації, як, скажімо, різноманітні варіанти цифрових записів, котрі, за логікою, мають підлягати захисту нормами авторського права. Утім у цьому разі йдеться не про захист ідей та контроль за розповсюдженням зазначеного продукту. Відтак, ефективний правовий захист у таких випадках убачається в застосуванні таких інструментів, як ліцензування, лізинг тощо, поряд із приписами авторського і суміжних прав.

Важливе місце у забезпеченні права інтелектуальної власності посідає закон про втрату конфіденційності (у країнах, де діють правові норми щодо захисту таємниці інформації). Його приписи, крім широкого масиву традиційного інформаційного продукту (креслення, формули, списки споживачів, фінансові відомості, виробничі та комерційні секрети тощо), стосуються такої категорії, як особиста таємниця (листування, різні папери, прямі, записані або пересказані перемови тощо). Варто також зазначити, що там, де обіг конфіденційної інформації регулюється законодавчо, здебільшого вважається недоцільними ретельна деталізація й регламентація поводження з численними видами державної, фінансової, комерційної, приватної та іншої інформації. Натомість перевага надається створенню міцної й водночас гнучкої правової основи, яка охоплює всі види відповідних суспільних

відносин. Зазвичай, указаний закон про втрату конфіденційності сполучається із запровадженням безпекових правил. Головне, на наш погляд, не забувати при цьому про захист приватного життя людини від, приміром, зловживань, шахрайств чи збитків, а не лише піклуватися про різні сфери національної безпеки.

Отже, вважаємо, що з метою забезпечення принаймні мінімально необхідного захисту від злочинів, пов'язаних з кіберсферою та використанням кіберпростору, ефективного правозастосування у цій галузі кожна країна має прийняти низку законодавчих актів, котрі передбачали б такі аспекти:

– узгоджені з міжнародними технічними стандартами приписи стосовно цілісності й безпеки даних;

– правові гарантії захисту в разі потреби законних інтересів користувачів за допомогою відповідного юридичного інструментарію;

– регулювання транскордонних інформаційних потоків, а також гарантії захисту у цій сфері національних інтересів.

Звісно, проблему поширення кіберзлочинності як негативного «додатку» до переваг інформаційної доби і як складової загальнокримінальної ситуації самим лише прийняттям відповідного законодавства розв'язати неможливо. У цій справі потрібен комплексний підхід, постійний державний контроль і відстеження потенційних ризиків від випадкових або умисних загроз для інформаційних систем, їхніх уразливих місць. Сукупність заходів, спрямованих на мінімізацію вказаних ризиків, має включати: визначення чинників уразливості в інформаційній сфері й кіберпросторі; доцільний контроль; запобігання неправильному використанню інформації, зловживанням, правопорушенням і злочинам у цій галузі. Натомість, для ефективного запобігання та виявлення комп'ютерних деліктів, протидії їм відповідна безпекова система має ґрунтуватися на тих самих організаційних принципах і застосовувати аналогічні алгоритми функціонування, досягаючи максимально можливого рівня системних програмних засобів і технологій, що й сучасні операційні середовища й оболонки.

Убачається, що задля налагодження дієвої системи інформаційної, кібернетичної безпеки в сучасному інформаційному суспільстві слід розробити й послідовно втілювати в життя комплекс заходів у таких двох напрямах: по-перше, формування негативної суспільної думки щодо правопорушень у кіберпросторі та інформаційній сфері загалом, унормування, чітке визначення відповідальності за кожен із видів вказаних правопорушень; по-друге, вжиття заходів із координування зусиль щодо підвищення рівня освіченості й поінформованості громадянського суспільства у сфері інформаційної та кібернетичної безпеки.

На наш погляд, реалізація зазначених заходів, спрямованих передусім на запобігання різноманітним правопорушенням в інформаційному й, зокрема, кібернетичному середовищах може стати визначальним чинником у справі забезпечення безпеки в цій сфері.

При цьому слід розуміти, що йдеться не про повну й остаточну перемогу над кіберзлочинністю, чого, мабуть, досягти нереально. Говорити можна вести лише про мінімізацію, обмеження ризиків. А для контролю над цими ризиками міжнародній спільноті належить сформувати надійну правову систему та ефективні механізми, що потребує від кожного користувача достатньо високого рівня знань та умінь. Для усвідомлення реальних проблем й оволодіння методів протидії кіберзлочинності суспільство має виробити відповідні творчі підходи. Варто, напевне, ще раз наголосити, що йдеться про розв’язання вказаних проблем уразливості інформаційних систем не лише за допомогою технічних засобів, а і шляхом формування відповідних морально-етичних передумов та нормативно-правової бази.

Французький філософ і теоретик культури XX століття, визначний представник французького структуралізму Мішель Фуко свого часу писав, що держава не має сутності, вона не є універсальною. Держава як така не є автономним джерелом влади, вона є ніщо інше, як ефект, абрис, рухомий перетин одвічного процесу формування Державного [324]. Ця глибока за змістом сентенція підтверджує ключову роль морально-етичної

відповідальності, необхідність для інформаційного суспільства створювати у процесі використання кіберпростору й інформаційних технологій, а також соціальної комунікації у глобальному середовищі відповідний інструментарій саморегулювання. Такої ж думки дотримувався й К. Маркс, коли говорив, що моральну силу неможливо створити самими лише статтями закону.

У контексті вдосконалення безпекового інформаційного законодавства громадські організації, освітні заклади, комерційні структури мусять активізувати свою діяльність у цій сфері шляхом прийняття й утілення в життя статутів, кодексів професійної поведінки й етики. Адже належний формат регулювання кібернетичного середовища, з погляду Л. Лессіга, сформує саме кодекс як зведення норм і правил [325]. А на більш конкретизоване викладення наявної в інформаційній сфері регламентації, а також втілення можливості сприяти ефективнішій самореалізації користувача в кіберсередовищі спрямовані насамперед морально-етичні кодекси.

Початок створення поведінкових морально-етичних кодексів був покладений із синтезом набутого досвіду, зіставленого з усталеними в суспільстві нормами моралі, визначенням загальних принципів і правил міжособистісних комунікацій у певній сфері діяльності. Сам термін «кодекс» (лат. codex, спочатку – стовбур, колода, згодом – скріплені дерев'яні таблички для письма, книга) означає:

1) єдиний законодавчий акт, який систематизує певну галузь права;

2) сукупність приписів, норм, переконань.

Ґенеза кодексів пов'язана з релігійними канонами і своїм корінням сягає глибокої давнини. У спільнотах, об'єднаних за професійною ознакою, вони виражалися у певних морально-етичних нормах і правилах, які, ґрунтуючись на загальних для суспільства моральних цінностях, відбивали специфіку конкретної професійної діяльності. Найдавніші зразки таких правил поведінки фахівців певної галузі, де в межах трудової діяльності етичні вимоги поєднуються із правовими приписами, зустрічаємо у спадщині Стародавнього Єгипту. Класикою подібних документів стало зведення морально-етичних

принципів і норм поведінки медичних працівників, назване за ім'ям давньогрецького лікаря 5–4 ст. до н. е. «Клятвою Гіппократа», де медицина ототожнюється з мудрістю, а той, хто нею володіє, – з божеством. Гордість за належність до цього фаху, повагу суспільства до особливого статусу лікаря викликають слова клятви про презирство до корисливості, пороків і забобонів, про скромність, совість і віру у високі ідеали [326]. Не дарма і сьогодні лікарі в багатьох країнах, розпочинаючи свою професійну діяльність, складають цю величну присягу.

Формуванню багатьох професійно-етичних вимог і відповідних статутів посприяв розподіл праці, який відбувався у середньовіччі. Зумовлювався цей процес потребою додаткового регламентування поведінки фахівця з урахуванням особливостей його професійного середовища й характеру діяльності. Адже, віддзеркалюючи сутність фаху в сукупності цінностей та ідеалів, які притаманні професійній моралі й унормовують професійну поведінку, спрямовану на підвищення продуктивності праці й поліпшення результатів виробництва, професійна етика є моральним регулятором міжособистісних професійних стосунків.

Варто зазначити, що засади професійної етики складають моральні взірці та ідеали, притаманні колективістській психології. Відмінності різногалузевих етичних кодексів зумовлена особливостями певних видів і сфер людської діяльності, таких як і державна служба, промислове виробництво, юриспруденція, медицина, освіта, військова служба, правоохоронна діяльність, журналістика тощо. Кодекси професійної етики виконують такі важливі функції, як регулювання поведінки фахівців та формування уявлення про їхню відповідальність перед суспільством, яка втілюється у якості та гідності професійної діяльності.

Водночас надметою теорії соціальної відповідальності є синтез громадянського обов'язку перед суспільством та основних прав і свобод людини – свободи особистості, слова, мас-медіа тощо. Ця ліберальна концепція стосується практично усе розмаїття суспільних інформаційних

інституцій, а тому коло її застосування якнайширше. Знаний англійський фахівець у галузі медіа та комунікацій Деніс Маквейл у зміст основних принципів теорії соціальної відповідальності закладає такі чинники, як високі професійні зразки об'єктивності та чесності, зумовлені турботою про народне благо і прагненням досягти та зберегти оптимальну рівновагу різноманітних поглядів в умовах плюралістичного громадянського суспільства, щоби запобігти будь-якому насильству або ж можливості принизити, образити групи меншин за якоюсь ознакою [327]. Таким чином, актуалізація теорії соціальної відповідальності свідчить, на нашу думку, про те, що однією з атрибутивних ознак сучасного демократичного правового суспільства стає морально-етичне регулювання процесів, які відбуваються в інформаційній сфері та використання кіберпростору.

Як бачимо, професійний кодекс фахівця – це насамперед своєрідний алгоритм соціалізації, основним завданням якого є прищеплення морально-етичних стандартів у певній галузі. На думку професорки Центру прикладної етики Вірджинського університету (США) Дебори Джонсон, головною функцією етичного кодексу є оформлення колективної мудрості представників певного фаху [328].

Убачається, що у професійних морально-етичних кодексах названих вище категорій спільнот поряд із специфічними поведінковими настановами стосовно, скажімо, захисту даних, формування фахової репутації тощо мають міститися й морально-етичні норми щодо прав і свобод людини, її честі й гідності та інших загальнолюдських цінностей. У кінцевому результаті морально-етичний кодекс має увібрати в себе все те, що покоління представників певного фаху вважали найважливішим у своїй роботі, їхній багаторічний досвід, а також стати узгодженим втіленням загального професійного набутку.

Утім до використання інформаційних технологій і кіберпростору нині причетні далеко не лише ІТ-професіонали. Завдяки своїй універсальності, відносній простоті у використанні та фінансовій доступності всесвітня

інформаційна мережа, кіберпростір створили благодатний ґрунт для виникнення різноманітних соціокультурних утворень, інтернет-спільнот (приміром, блогерів, хакерів і т.п.), котрі сформували свою систему цінностей і поведінкових норм, певну субкультуру. Сьогодні вони вже досягли такого рівня розвитку, коли можна говорити про «кодифікацію» зазначених зразків і неписаних правил у певні зведення морально-етичного регулювання діяльності членів цих спільнот.

Із часом, з розвитком комп'ютерних технологій, у професійних спільнотах виникає потреба в морально-етичних регуляторах їхнього створення й застосування. Проникнення інформаційних технологій практично в усі сфери життєдіяльності не лише спричинило загальні суспільні перетворення, зумовивши виникнення нових професій, зростання числа зайнятих в ІТ-сфері, а й істотно вплинуло на світосприйняття, систему інтересів і пріоритетів людини, котрі визначають її поведінку, спосіб дії та механізми прийняття рішень. Видозмінюються також ціннісні орієнтири, пов'язані із трудовою діяльністю, системою стосунків «людина – машина». Про це свідчить, зокрема, прийняття стандартів професійної відповідальності фахівців у переважній більшості спеціалізованих структур у сфері інформаційних технологій.

Наприкінці 20 століття морально-етичне регулювання у професійній ІТ-сфері виходить за межі цього середовища, показником чого стало включення до базових програм низки освітніх закладів відповідних нормативів і положень. Тобто, формування інформаційного суспільства, викликане розвитком комп'ютерних технологій, зумовило потребу поширення професійної ІТ-етики на широкий користувацький загал, насамперед таких понять, як «моральне регулювання» й «відповідальність».

Відтак, стрімкий розвиток «корпоративної» теорії комп'ютерної етики перетворив її на інформаційну етику – нову, велику й затребувану наукову галузь, котру сьогодні пропонують відносити до соціальної етики. Механізми правового й організаційного закріплення соціальної етики базуються, зокрема,

на засадничому положенні, що практика індивідуума в соціумі здійснюється в контексті моральних цінностей. Убачається, що це повною мірою відповідає принципам інформаційної етики.

Американські дослідники Т. Фрейліх та Р. Рубін вважають, що шляхами досягнення дійового управління інформаційною взаємодію є національне й міжнародне правове регулювання, а також самоконтроль [329]. Під останнім учені розуміють прийняття морально-етичних кодексів та елементарне дотримання правил мережевого етикету. Позаяк, про що йшлося вище, інертний державний законотворчий механізм не встигає реагувати на безліч питань, пов'язаних з користуванням глобальним інформаційним простором, виникає нагальна потреба морального суспільного саморегулювання. Саме про це говорить мудра сентенція: *де не набирає чинності закон, там його замінює мораль*.

Ми цілком погоджуємося з думкою професора М. Кириченка у тому, що інформаційна етика як складник ідеології інформаційного суспільства базується на таких ключових характеристиках, що становлять сутність етичних і моральних теорій та цінностей, завдяки яким укріплюється людська гідність [330, с. 52].

Інформаційна етика регулює своїми засобами соціальні відносини стосовно користування кіберпростором. Тому передусім вона має визначитися і поняттям кібернетичного простору: це «середовище» чи «місце». Якщо кіберпростір – це фізичне місце, то в етичному контексті для визначення прав, обов'язків та відповідальності користувачів всесвітньої мережі Інтернет слід сформувати відповідний кодекс (скажімо, кодекс доброчесності власників, володільців і користувачів відкритих інформаційних систем, зокрема й інтернет-спільноти). Примітно, що зразки таких об'єднань у межах певної інформаційної області вже відомі. Це, приміром, канадський Кодекс поведінки в Інтернеті, французька Хартія Інтернет та ін. До числа загальних приписів у цій галузі належать такі основні принципи (закріплені також у праві Євросоюзу), як свобода думки, захист людської гідності, приватності тощо.

Подібний підхід бачимо й у «Принципі забезпечення доступності інформації», або, як його ще називають, «Біллі про право інформації в епоху інформації», схваленому 1990 року Національною комісією США з бібліотек та інформаційної науки.

З огляду на викладене, вважаємо, що своєрідною «інформаційною конституцією» в нашій країні має стати закон «Про основні засади забезпечення кібербезпеки України». Він має не лише закладати головні принципи технократичного поступу та правового забезпечення користування кібернетичним простором і кібербезпеки, а й установити морально-етичні критерії, зразки функціонування інформаційного, кібернетичного середовища соціуму й держави. Ключовим його предметом мають стати загальнолюдські моральні цілі й завдання інформатизації та кібербезпеки, спрямовані на створення належного рівня інформаційної життєдіяльності кожного громадянина країни як потенційного члена глобального інформаційного світового співтовариства.

Оскільки між усталеними етичними принципами, закріпленими в національних і міжнародному законодавствах, і реальністю інтернет-середовища існує чималий розрив, на практиці важливо застосовувати й дотримуватися чітких і точних правил, директив і приписів. У зв’язку з цим світова наукова спільнота одностайна в тому, що потрібен динамічний, гнучкий міжнародний інструмент на кшталт етичного кодексу Інтернету з відкритими принципами для сприяння майбутньому прогресу й новим форматам.

Унікальний феномен інтернет-середовища потребує відповідного універсального механізму й інструментарію регулювання специфічних процесів, що в ньому відбуваються. Тому згаданий вище етичний кодекс Інтернету має, на нашу думку, чітко та зрозуміло формулювати приписи, але при цьому зважати на такі особливості, як, приміром, індивідуальна власність чи так звані «горизонтальні ефекти» , котрі характерні для мережі, але вельми сумнівні із загальноправової точки зору.

Яскравим свідченням світового визнання того, що повсюдне активне впровадження інформаційних технологій спричиняє кардинальні соціальні трансформації, стала розробка ЮНЕСКО (Організація Об'єднаних Націй з питань освіти, науки і культури – UNESCO, United Nations Educational, Scientific and Cultural Organization) розробила Етичний кодекс інформаційного суспільства. Цей документ, створений з метою регулювання суспільних відносин, зокрема і при користуванні кіберпростором, проголошує, що інформаційне суспільство має ґрунтуватися на загальноприйнятих цінностях; усі зацікавлені суб'єкти діють в інтересах суспільного блага і сприяють запобіганню зловмисному використанню інформаційних технологій [331-332].

Утім, попри нагальність і важливість такого міжнародного документа, проєкт зазначеного кодексу був визнаний «неспроможним розв'язати реальні проблеми» через охоплення ним завеликої кількості аспектів життєдіяльності інформаційного суспільства й надто загального змісту його рекомендацій.

Отже, з огляду на бурхливий розвиток інформаційних технологій, посилення впливу їхнього використання на життя сучасного соціуму, роль етичних кодексів невпинно зростає. Зумовлено це насамперед збільшенням чисельності прийнятих норм, правил, статутів тощо, спрямованих на регулювання суспільних інформаційних відносин при користуванні кіберпростором. Головним їхнім завданням убачається виконання в сучасному інформаційному суспільстві морально-регулятивної та рефлексивної функцій.

Водночас, фахівці відзначають певну обмеженість, нечіткість, брак конкретики та інші подібні вади чинних етичних кодексів. Це зайвий раз підтверджує потребу виховання, закріплення морально-етичних принципів у свідомості кожного індивідуума, груп, спільнот, соціуму загалом. Позбавитися вказаних недоліків, підвищити дієвість прийнятих моральних норм можна, на наш погляд, якщо дотримуватися при їхньому формуванні певних вимог. По-перше, їхній зміст має підкріплювати правові норми й засадничі принципи, сприяти їх втіленню в життя. По-друге, до створення

кодексів, формулювання морально-етичних зобов'язань, які, власне, й утворюють зведення морально-етичних правил, слід залучати науковців, фахівців-практиків, усіх зацікавлених осіб та широку громадськість. По-третє, викладені в цих документах принципи, настанови і приписи мають бути чіткими, зрозумілими та прагматичними.

Практична спрямованість інформаційної етики проявляється в регуляторних незмінних, константних моральних настановах відповідних етичних кодексів. При цьому критеріями оцінювання людської поведінки є універсальні морально-етичні уявлення, котрі є фундаментом загальновизнаних моральних принципів. У свою чергу, дієвість втілення прийнятих правил соціальної взаємодій в інформаційному, кібернетичному середовищі залежить від рівня самосвідомості індивідуума, ставлення морально-етичного налаштування суспільства, жорсткості соціального реагування за порушення моральних приписів. Таким чином, виникає потреба подальшого вдосконалення морально-етичних кодексів, наукової розробки функцій інформаційної етики, котра є одним із наріжних каменів такого соціального явища, як інформаційна безпека.

Підбиваючи підсумки проведеного дослідження, зазначимо, що правове забезпечення кібернетичного середовища нами розглядається також як об'єкт морально-правового регулювання. Сутність останнього полягає в налагодженні суспільних відносин, врегулювання яких базується на нормах права та моралі. Із цією метою держава, як основний регулятор, виконує такі основні завдання:

1) удосконалення чинних, розроблення та впровадження в законодавство нових правових норм, які відповідають сучасним потребам людини, суспільства й держави і спрямовані на правове регулювання використання кіберпростору, узгодження національного й міжнародного інформаційного законодавств тощо;

2) утвердження й упорядкування доцільних суспільних відносин у сфері державного управління інформаційним середовищем, зокрема питань захисту

таємниці даних, інтелектуальної власності, авторського права тощо, шляхом упровадження морально-етичних і правових норм;

3) захист передбачених законодавством відносин у процесі користування інформаційними технологіями, кіберпростором, у тому числі визначення відповідальності за їхнє порушення;

4) регулювання суспільних відносин, пов'язаних з еволюцією інформаційного суспільства, шляхом формування суспільної думки, створення морально-етичних кодексів тощо;

5) участь у міжнародних проєктаж, з метою налагодження жієвої співпраці для попередження кіберзагроз на глобальному рівні.

Різке зростання технічних можливостей, повсюдне впровадження комп'ютерних технологій зумовило суспільну потребу в надійному функціонуванні кіберпростору, для чого необхідне швидке розв'язання проблеми ефективного нормативно-правового регулювання. Подальшого наукового дослідження й удосконалення потребує правозастосовна практика у сфері інформаційної, кібернетичної безпеки, котра базується на відповідних законах, актах, угодах та інших регламентуючих документах. При цьому важливим убачається всебічне, комплексне дослідження, котре би враховувало необхідність досягти оптимального балансу технічних, соціокультурних, морально-етичних та інших чинників.

Істотно доповнити інструментарій координування нормативного регулювання інформаційного, кібернетичного простору, підвищити його ефективність мають саморегуляторні технології сучасного суспільства, представлені морально-етичними кодексами.

Відтак, на наше переконання, реалізація вказаних заходів дозволить закріпити у суспільній свідомості сукупність морально-правових прав і обов'язків, виробити почуття поваги до норм соціального співжиття, а також відповідальності за їх дотримання.

Таким чином, є всі підстави стверджувати, що на сучасному етапі розвитку суспільство потребує (в межах прийнятої моделі кібернетичної

безпеки) розроблення державної соціальної стратегії застосування інформаційних технологій та використання кіберпростору, котра би вказувала на головні пріоритети прогресивного розвитку суспільства і закладала базис для створення механізму координування соціальних норм.

4.3. Теоретико-правове підґрунтя системи соціального регулювання в інформаційному суспільстві

Як доведено всією історією людства, безпека є атрибутом його нормального існування. При цьому постійно зростає гуманістична спрямованість процесу її забезпечення. У контексті сьогодення це дасть змогу створити безпечні умови використання суспільством інформаційних технологій та кіберпростору, запобігаючи та знешкоджуючи виклики та загрози інформаційного характеру.

Успішне створення умов безпечного функціонування в кібернетичному просторі потребує значних зусиль і ретельної попередньої підготовки. Результати аналізу можливостей наявних технологій та їхніх майбутніх потенцій доводять, що вкрай важливо, аби новітні цифрові технології не втратили соціальний зміст і не набули антигуманістичної спрямованості. Варто також наголосити, що вектор нових інформаційних технологій визначається не стільки їхніми розробниками, скільки самим суспільством, де формується відповідне соціальне середовище – гуманістичне чи з префіксом анти.

Для розвитку людської цивілізації, її виживання неабиякої вагомості набуває оцінювання технічних «інфо-кібер-технологічних» новацій та прогноз

щодо їхнього використання. Зрозуміло, що володіння правдивою інформацією стосовно можливих напрямів застосування комп'ютерних технологій істотно сприяє убезпеченню від можливих різноманітних шкідливих наслідків. Натомість «гарантом» майбутніх негараздів (аварій, катастроф тощо) є нерозуміння наслідків застосування вказаних технологій, отримання неповної, недостовірної, спотвореної чи хибної інформації. При цьому, як відмічають фахівці з кібербезпеки «кіберзагрози еволюціонують в прискореному темпі, вони стають досконалішими, краще організованими і транснаціональними» [333]. Тобто, головним дороговказом на шляху розвитку системи інформаційних технологій має стати прийдешнє людства. Тому, на наше переконання, структура глобальної світової безпекової системи обов'язково зазнає позитивних змін з огляду на зміщення в гуманістичний бік пріоритетів у змісті кібернетичної безпеки.

Відтак, забезпечення якнайширшого різноманіття в інформаційних мережах правомірного контенту в контексті захисту основних людських прав і свобод – це задоволення передусім саме тих інформаційних потреб, які відповідають інтересам прогресу світової цивілізації. Тобто, коли йдеться про інформаційно-телекомунікаційні технології, які спрямовані на повагу до загальнолюдських цінностей, якраз і передбачається, що винятково на прогресивний поступ спрямовуватиметься оволодіння соціумом знанням та інформацією за допомогою технологій.

Забезпечення загального рівного доступу до інформації та відповідних технологій передбачає насамперед розширення соціальної бази кібернетичної безпеки, що сприятиме оптимізації всіх рівнів функціонування – особистісного, суспільного й державного. У цьому зацікавлене громадянське суспільство, котре проголошує рівні можливості, в тому числі й стосовно участі в інформаційних комунікаціях, для усіх своїх членів. Таке розширення соціальної бази інформаційної безпеки означає водночас ріст кількості її суб'єктів. Тож виникає важливе завдання підвищення рівня інформаційної культури, освіченості вказаних соціальних суб'єктів й суспільства загалом. Це

рівною мірою стосується і професійної діяльності в галузі інформаційно-телекомунікаційних технологій, і взагалі будь-якої діяльності в інформаційній сфері, котра охоплює всіх суб'єктів інформаційних відносин при використанні кіберпростору, оскільки безпеку соціуму визначає, врешті-решт, саме рівень головної передумови формування соціально-економічного, наукового, культурного й духовного потенціалу – людського ресурсу. Тому, виходячи з наведених резонів, визначальними чинниками забезпечення надважливої складової національної безпеки – інформаційної та кібернетичної безпеки вбачаються наука й освіта.

Зростання в кібербезпеці ролі соціальної складової зумовлює, на наш погляд, потребу запровадження принципово нового виду захисних інформаційно-безпекових заходів – соціальних. Якісною новизною вказаний вид захисту кібербезпеки людини, суспільства й держави зобов'язаний складній, багаторівневій системі механізмів і поведінкових форм, сукупність котрих цю безпеку забезпечити.

Задля успішного розв'язання проблем забезпечення кібернетичної безпеки потрібне, на нашу думку, впровадження комплексу заходів, а саме:

– проведення активного наукового пошуку в межах розвитку інформаційної етики – нової галузі етичного знання, котра перебуває на етапі свого становлення;

– освітні та виховні заходи;

– всебічна популяризація в суспільній свідомості способів, моделей і форм морально-етичної поведінки у глобальному кіберсередовищі із застосуванням при цьому найсучасніших цифрових технологій, із залученням усіх можливих ЗМІ та активною участю державних структур.

Спробуємо на підставі виокремлених нами трьох рівнів соціальних заходів кібербезпеки: – макро-, мезо- та мікрорівень – сформулювати їхній зміст й головні напрями функціонування та розвитку:

– на *макрорівні* (охоплює все суспільство) вказані заходи реалізуються шляхом організації, упорядкування, регулювання інформаційних потоків та

поширення засобів і способів, певної послідовності оцінювання й оброблення інформації, а також застосування інформаційних технологій у процесі соціальної взаємодії, як міжособистісної, так і масової. Суб'єктами захисту інформаційної безпеки на цьому рівні є суспільство й держава. Здійснюють цю функцію вони за допомогою відповідних соціальних інституцій, діяльність яких спрямована, зокрема, на поширення і пропагування соціальних норм, культурних і суспільних цінностей, традицій, формування системи освіти та морально-правового регулювання, створення сприятливого соціокультурного середовища тощо;

– на середньому – *мезорівні* (суспільні організації та групи) соціальні захисні заходи втілюються шляхом використання й розповсюдження джерел інформації, а також особливих, притаманних конкретним організаціям і соціальним спільнотам, способів соціальної взаємодії, оцінювання й переопрацювання інформації. Безпосередніми суб'єктами захисту інформаційної безпеки на цьому рівні є різноманітні політичні, громадські, виробничі, релігійні та інші організації й соціальні структури. З-поміж засобів здійснення ними зазначеної функції варто виокремити прийняті в цих групах морально-етичні норми та правила, певні приписи, що регламентують процеси інформаційної взаємодії та безпечного користування інформаційними технологіями та кіберпростором.

На *мікрорівні* (індивідуальному) соціальні інформаційно-захисні заходи здійснюються під час розвитку й навчання людини шляхом формування певної системи регуляції чи сукупності інструментів та алгоритмів, котрі визначають її поведінку в кібернетичному середовищі.

Розглянемо детальніше технології, що застосовуються, виходячи зі змісту та структури соціальних заходів забезпечення інформаційної безпеки.

На макрорівні у межах відповідної державної політики належить, на нашу думку, здійснити насамперед такі кроки: сформувати концепцію правового забезпечення інформаційної та кібернетичної безпеки; організувати та активно провадити просвітницькі заходи щодо прав та обов'язків при

користуванні інформаційними технологіями і кіберсередовищем, популяризувати основні принципи інформаційної кібербезпеки; створити міцний науково-методологічний фундамент у сфері інформаційної та кібернетичної безпеки.

Зазначимо, що проблеми кібернетичної безпеки із суто спеціальних перетворилися на соціальні, тобто перейшли у сферу захисту прав людини. Очевидно, що виконувати інформаційно-захисні функції, гарантувати дотримання прав особи й суспільства в цій сфері має передувсім держава за допомогою законодавства. Вважаємо, що задля захисту прав людини й суспільства у боротьбі зі правопорушеннями у кібернетичному просторі, комп'ютерними злочинами потрібна не лише уніфікація відповідного національного законодавства, а й вироблення єдиних підходів на міжнародному рівні, об'єднання зусиль усієї світової спільноти щодо регулювання процесів користування глобальним кіберпростором. Значення комплексних наукових досліджень, які б зважено враховували технічні, культурні, морально-етичні та інші аспекти, в успішному здійсненні вказаних заходів важко переоцінити.

Водночас державна політика правового забезпечення кібернетичної безпеки має спрямовуватися на мобілізацію системи освіти, засобів масової інформації на популяризацію, пропагування морально-етичного поводження в кіберпросторі, глобальній електронній мережі, формування в суспільній свідомості відповідних поведінкових моделей, котрі мають створити базис системи кібернетичної безпеки.

У руслі аналізованих вище питань кібербезпеки приєднуємося до позиції американського професора філософії Т.В. Байнума, котрий у контексті розв'язання сучасних проблем застосування новітніх технологій визначає певні рівні, ступені поширення етичних знань [334].

Методологічні засади інформаційної етики закладені працями Норберта Вінера, де, зокрема, піднімаються такі фундаментальні питання, як захист базових цінностей Homo sapiens – життя, здоров'я, свободи, безпеки,

можливості набувати знання та їх застосовувати. Виходячи з цього, досліджувати та розв'язувати проблеми, які виникають у процесі застосування інформаційних технологій та кібернетичного простору, слід на двох рівнях.

На першому – базовому – рівні до всіх суб'єктів спільноти доводиться істина про соціальні й морально-етичні наслідки використання інформаційних технологій та кіберпростору. Робиться це шляхом якнайширшого інформування суспільства стосовно проблематики, пов'язаної із створенням і застосуванням новітніх технологій, популяризації та пропаганди відповідної поведінки. На цьому рівні інформаційної етики одну з головних ролей відіграють засоби масової інформації. Стосовно проблем сфери інформаційної безпеки, відповідних прав і обов'язків її суб'єктів постійно, в міру зростання впливу новітніх технологій, має сповіщати населення система розповсюдження інформації. Широкий загал має чітко усвідомлювати, які переваги й водночас загрози несе поширення інформаційних технологій та використання кіберпростору. На наш погляд, позитивним результат такої діяльності на першому рівні популяризації інформаційної етики та інформаційної безпеки можна вважати тоді, коли зростатиме кількість соціальних суб'єктів інформаційних відносин, котрі будуть спроможні попередньо оцінювати поведінку інших суб'єктів цих стосунків, виявляти та розпізнавати соціальні й морально-етичні проблеми, що при цьому виникають, будучи при цьому пересічними громадянами, не фахівцями у дотичних сферах – кібернетики, інформаційних технологій, філософії, соціології, правознавства та ін.

Другий рівень інформаційної етики – теоретичний. Тут до аналізу соціально-етичних проблем суспільства, пов'язаних з використанням інформаційних технологій і кібернетичного простору, поєднується теоретичний пошук. На наше переконання, оскільки теоретична інформаційна етика дає змогу фахівцеві розглядати морально-етичні ситуації, що виникають, використовуючи для наукового пошуку та всебічного аналізу нагальних проблем філософський, соціологічний, юридичний та інший

дослідницький інструментарій, дисципліна «теорія інформаційної етики» має увійти в навчальні плани вищї освіти.

Вказані рівні поширення морально-етичного знання тісно взаємопов'язані й не мають чіткого розмежування. Об'єднує їх спільна надмета – захист загальнолюдських цінностей, прав і свобод людини та громадянина. Відтак, кожен соціальний суб'єкт і, відповідно, суспільство загалом мають усвідомити всі можливі наслідки – позитивні й негативні – користування інформаційними технологіями й кібернетичним простором. Тому ІТ-фахівці, державні, політичні й громадські діячі, аби їхня діяльність була ефективною, мусять володіти знаннями й навичками, які б відповідали принаймні другому рівню інформаційної етики. Водночас завданням наукової спільноти у своїх дослідженнях є подальше розкриття соціального й морально-етичного впливу інформаційно-телекомунікаційних технологій та використання кіберпростору.

З огляду на це одним із пріоритетів державної політики у сфері правового забезпечення кібернетичної безпеки має стати сприяння й усебічна підтримка наукового пошуку, пов'язаного з розробкою та впровадженням новітніх цифрових технологій, аналітичних і прогностичних досліджень у цій галузі [335]. При цьому, як убачається, вказані дослідження, котрі базуються на положеннях інформаційної етики, мають спрямовуватися на синтез набутого досвіду, моделювання теоретичних концепцій, напрацювання рекомендацій щодо налагодження оптимальної системи інформаційної та кібернетичної безпеки, а також на прогнозування можливих негараздів від використання комп'ютерних технологій, їхнє запобігання, нейтралізацію та знешкодження.

Важливим чинником розробки наукового підґрунтя кібернетичної безпеки є також:

– розроблення освітніх методик у цій галузі та механізмів формування під час освітнього процесу інформаційної культури;

– сприяння розробці та розповсюдженню наукових, науково-

популярних, навчальних, методичних, довідкових та інших матеріалів стосовно питань інформаційної та кібернетичної безпеки, культури та етики особи й суспільства;

– підготовка й підвищення кваліфікації педагогічних працівників з метою налагодження в системі вищої, спеціальної та середньої освіти високопрофесійного навчального процесу для підготовки високопрофесійних кадрів системи забезпечення інформаційної та кібернетичної безпеки.

Водночас, роль державних інститутів у забезпеченні процесів інформаційної взаємодії полягає насамперед в особливому сприянні, патронаті цієї сфери, але аж ніяк не жорстким контролем кожної її галузі чи стадії. Для реалізації своїх відповідних функцій державні структури мають виконувати такі завдання: формувати, проголошувати, популяризувати морально-етичні принципи, на яких базується інформаційне суспільства, а також надавати їм юридичної форми; здійснювати моніторинг і контроль за їхнім утіленням й дотриманням; вживати відкритих і прозорих регулятивних заходів у разі відсутності підтримки вказаних принципів або зловживань з боку окремих суб’єктів.

Крім того, держава повинна втілювати вказані морально-етичні регулятивні норми, прищеплювати повагу до них як до взірця етичного застосування інформаційних технологій і користування кіберпростором. У результаті впровадження інформаційної етики має посприяти утвердженню в свідомості суспільства тих принципів, на яких воно має будуватися на інформаційному етапі свого розвитку. У свою чергу, ці принципи мають екстраполюватися на сферу захисту прав і свобод людини.

При цьому, як уже побіжно зазначалося, створювати оптимальне з морально-етичного погляду інформаційне середовище слід не тільки, ба навіть не стільки шляхом блокування й покарання порушників, скільки, й передувсім, формування виховних зразків, розробка і впровадження методів і засобів, спрямованих на осягнення населенням морально-етичних цінностей, прищеплення поваги до них, а також до самоаналізу й самовдосконалення.

Надметою усіх цих заходів є досягнення в інформаційному, кібернетичному середовищі морально-етичної саморегуляції та заснованого на спільних інтересах і соціальній відповідальності самоконтролю.

Що стосується мезорівня забезпечення інформаційної безпеки, то він передбачає розроблення й запровадження безпекових заходів на рівні груп, колективів, об'єднань. Формування цих захисних механізмів спирається на солідаризацію індивіда з певною конкретною спільнотою. Головною метою вказаних заходів є вироблення в людини спроможності під час користування інформаційними технологіями та кіберпростором керуватися тими поглядами, нормами, критеріями, котрі прийняті в певному професійному середовищі чи соціальній групі.

Спробуємо виокремити ті різновиди соціальних спільнот у сфері застосування інформаційних технологій і використання кіберпростору, які, на наш погляд, мають потребу в морально-етичному регулюванні.

Перший тип – це професіонали, IT-спеціалісти, для яких ця галузь є сферою фахової діяльності. Сюди слід віднести й колективи, бізнес-інтереси котрих пов'язані з інформаційним, кібернетичним середовищем, а також віртуальних викладачів, бібліотечних працівників та деяких інших. До другого типу належать усі категорії індивідуальних й колективних користувачів. Спільноти третього типу складають засоби масової інформації. Нарешті, четвертий тип складається з тих, хто займається регулюванням контенту в інформаційному, кібернетичному просторі. Через брак правових важелів впливу для цієї категорії засобом забезпечення прозорості в роботі пошукових механізмів покликані слугувати морально-етичні кодекси.

Слід зазначити, що питання морально-етичного регулювання професійної діяльності вже доволі давно перебувають серед пріоритетів у середовищі IT-фахівців. Так, вагомий внесок у справу підвищення професіоналізму й морально-етичного становлення комп'ютерних спеціалістів, прищеплення професійної відповідальності зробили етичні кодекси Інституту інженерів електротехніки та радіоелектроніки (IEEE, 1990

р.) [336] та Асоціації виробників обчислювальної техніки (ACM, 1992 р.) [337]. Положення, закріплені в цих документах, свідчать про те, що фахівці прагнуть не лише керуватися загальноприйнятими в соціумі морально-етичними нормами, а й дотримуватися засадничих принципів інформаційної та кібернетичної безпеки, таких як таємниця відомостей, конфіденційність, доступність і достовірність інформації тощо.

Варто також додати, що на сьогодні все більше актуалізується питання професійної відповідальності, що зумовлено підвищенням вимог до фахового рівня спеціалістів в умовах розвитку інформаційного суспільства й зростання уваги до інформаційної та кібернетичної безпеки.

Ще у 2003 році Р. Броді увів до наукового обігу таке поняття, як «інформаційна наївність» IT-професіоналів, доводячи кардинальну відмінність змісту слів «знати про» та «знати». Визначив він це поняття як «стан, який не може бути більшим, ніж реалізація процесу, пов'язаного з виробленням артефактів» [338]. Дещо розширюючи семантику «наївності» (щось безпосередньо просте, викликане життєвою недосвідченістю), додамо сюди брак професійних знань та умінь, а також невисокий рівень компетентності.

Вважаємо, що протидія такій професійній ваді полягає в активному застосуванні у професійній інформаційній, кібернетичній сфері морально-етичних кодексів, покликаних запобігати можливим негативним проявам, формувати високу фахову компетентність, ретельність і відповідальність. Про це йшлося в попередньому підрозділі.

Стосовно третьої категорії користувачів, діяльність яких в інформаційній сфері та кіберпросторі потребує регулювання, то слід підкреслити що формування професійної журналістської етики, працівників засобів масової інформації має давні традиції, тісно пов'язані із загальними світовими процесами демократизації й гуманізації. Нині це – загальновизнані у професійному середовищі принципи міжнародної журналістської етики, котрих необхідно дотримуватися в роботі, правдивості й об'єктивності,

безкорисливості, поваги до гідності людини, до її приватності, виражати суспільні інтереси, загальнолюдські цінності, висвітлювати усе розмаїття культур та поглядів, а також діяти відповідно до норм інформаційної безпеки.

Нинішні досягнення інформаційно-телекомунікаційних технологій, охоплення ними усіх сфер людської життєдіяльності створюють для засобів масової інформації величезні потенції впливу на суспільну свідомість. Тому дуже важливо, щоб професійні журналісти всіх ЗМІ інтерполювали на глобальні інформаційні мережі та кіберпростір високі норми свого корпоративного етичного кодексу.

Нарешті, спільнота провайдерів інтернет-контенту – ще одна категорія, діяльність котрої через відсутність, як зазначалося, її правового регламентування, потребує обов'язкового, на наше переконання, запровадження морально-етичних кодексів. Питання, які слід передбачати в такому документі, повинні, на наш погляд, стосуватися, зокрема, підпорядкованості пошукових інтернет-служб, критеріїв блокування й поширення інтернет-контенту, гарантій їхньої етичної роботи та ін. Сюди варто віднести також питання відповідальності «регулювальників» всесвітньої мережі за ретранслювання в кіберпросторі незаконного, забороненого, шкідливого, небезпечного чи неетичного контенту.

У цьому контексті показовим убачається приклад, коли всесвітньо відома компанія Google визнала, що під час панорамної зйомки вулиць населених пунктів для картографічного сервісу Street View її співробітники порушували вимоги недоторканності приватного життя. Фотографуючи міста, «гугломобілі» водночас «збирали персональні дані громадян у незашифрованих мережах Wi-Fi протягом кількох років. Ця інформація містила логіни, паролі, листи електронної пошти. У подібних порушеннях була також викрита компанія «Яндекс» [339].

Отже, убачається цілком очевидним, що інтернет-посередники мусять сповіщати про принципи, форми й методи своєї діяльності, гарантуючи при цьому дотримання конфіденційності довіреної їм інформації. Відтак, потреба

обговорення й формування відповідного морально-етичного кодексу є вельми нагальною.

Окремі зразки таких зведень уже є. Це, наприклад, кодекс практики для виробників баз і банків даних, запропонований Європейською асоціацією з інформаційних послуг (EUSIDIC). У цьому документі «червоною ниткою» проводиться ідея дотримання повноти, достовірності, доступності, конфіденційності та інших принципів інформаційної безпеки. Його положення спрямовані на забезпечення відкритості інформаційних потоків з обов'язковим урахуванням вимог захисту персональних даних та законних інтересів усіх суб'єктів відносин, пов'язаних із виробництвом, зберіганням і переданням інформації [340]. Упевнені, що міцним фундаментом професійної діяльності спільнот інтернет-провайдерів саме й мають стати принципи справедливості, відкритості, достовірності й конфіденційності.

Розглядаючи це питання, доцільним вважаємо привернути також увагу дослідників і громадськості до діяльності інтернет-серверів діалогових та азартних ігор, а саме до морально-етичних аспектів їхньої роботи. Запровадження навіть елементарних правил у сферу надання цих та подібних послуг може, на нашу думку, серйозно посприяти психологічному захисту користувачів, насамперед дітей і підлітків, зменшити кількість психосоціальних розладів.

Регулювання питань свободи слова й доступу до інформації відповідно до Конвенції про права людини пов'язане в демократичному суспільстві з обов'язками та відповідальністю. У нинішніх умовах виникає питання щодо пристосування цих регуляторів до кіберсередовища або ж створення спеціального документа, котрий регламентував би інтернет-відносини. І проблему цю аж ніяк не можна назвати простою. Виникає запитання, чи є такими ж неприпустимими у віртуальному просторі ті категорії інформації, які вважаються незаконними або неприйнятними в реальному житті, або ж специфіка глобальної мережі припускає існування особливих її форм, котрі потребують окремої регламентації.

До певної міри розв’язати ці проблеми має, на нашу думку, інформаційна етика, зокрема і шляхом унормування функцій інтернет-посередників, позаяк відповідальність за наслідки діяльності останніх не передбачена європейським законодавством. Наведені вище приклади далеко не вичерпують перелік недоліків у роботі інтернет-провайдерів, а тому слід, вважаємо, розробити додаткові гарантії забезпечення її прозорості.

Цілком приєднуємось до професора Кентського університету Томаса Фрейліха, котрий одним із способів ефективного регулювання інформаційної взаємодії називав самоконтроль [341]. У контексті цього дослідження варто згадати і про технічні способи його здійснення, а саме: застосування фільтраційних програм, функцій модераторів, розроблення технічних регламентів як програмного забезпечення для рейтингових і фільтраційних операцій.

Зауважимо, що сучасна практика напрацювала поки що небагато зразків саморегулювання та спільного регулювання кінцевих користувачів. Одним із таких прикладів, щоправда вельми примітних і позитивних, спільного регулювання мережевого контенту може слугувати загальнодоступна, відкрита, багатомовна універсальна інтернет-енциклопедія, широко відома як Вікіпедія (Wikipedia). До створення її контенту, перевірки фактажу, редагування тощо залучається практично уся громадянська інформаційна спільнота. Як джерело найрізноманітнішої інформації це віртуальне видання набуло величезної популярності у користувачів всесвітньої мережі, попри те, що з огляду на свою специфіку воно не належить до наукових.

Правовідносини між розробниками цього інтернет-ресурсу, його численними авторами та користувачами регулюються зведенням офіційних правил Вікіпедії. Усі суб’єкти, пов’язані з ресурсом, відповідно до цього своєрідного кодексу не повинні допускати образ, зневажання, агресії та погроз, авторської багатоликості. Автори беруть на себе зобов’язання дотримуватися неупередженості, нейтралітету у своїх матеріалах, не оприлюднювати у статтях енциклопедії оригінальних досліджень, посилатися

на джерела інформації, що ними подається. Категорично заборонено використання анонімних проксі-серверів, а в разі інших порушень порядок відновлюється за допомогою перемов. Так звані «Правові основи» переліку передбачають умови, що запобігають порушенню авторського права.

Як бачимо, запроваджені творцями Вікіпедії регулятивні заходи не лише сприяли підвищенню морально-етичної поінформованості інтернет-спільноти, а й зумовили загалом конструктивні, довірчі відносини між її учасниками.

Ще одним прикладом саморегулювання в технічному сенсі є проект (котрий нині успішно функціонує) «Створення інтернет-контенту» (Internet Content Generated) у межах якого передбачено генерування специфічного демократичного кіберсередовища (Internet Democracy Generated). Ці віртуальні утворення дають змогу користувачам у пошуках альтернативного управлінського інтернет-інструментарію дискутувати на предмет моделей створення, розвитку й розповсюдження інформації. Приміром, моніторити інтернет-середовище для виявлення порушень правових та морально-етичних приписів можна сьогодні за допомогою платформи «Creative Commons» [342] та інших подібних моделей, що виникають стихійно.

Таким чином, на мезорівні при організації суспільних заходів слід застосовувати методи й засоби створення відповідної соціальної атмосфери, духу здорового корпоративизму. Крім того, необхідно уможливити ідентифікацію індивіда з конкретною соціальною спільнотою, прищепити почуття гордості за причетність до неї. Ці заходи мають також передбачати формування усередині вказаних соціальних утворень професійні та інші морально-етичні приписи й настанови, котрі визначають умови функціонування в інформаційному, кібернетичному середовищі та безпечного використання відповідних технологій.

Здійснюючи свою функцію духовного регулятора поряд із традиційними правовими і моральними приписами та традиціями, інформаційна етика є важливим чинником формування морально-інформаційного середовища сучасного соціуму, у тому числі й окремих спільнот, груп, колективів,

індивідуумів.

Уявляється, що морально-етичний кодекс має бути такою собі точкою тяжіння, доцентрові сили якої зумовлюють досягнення системою того кінцевого стану, котрого вона прагне досягти. Приміром, наслідком усвідомлення вагомості морально-етичного регулювання на рівні спільнот є актуалізація прагнення до вивчення принципів інформаційної етики, до сприяння її правового та організаційного закріплення, а також, відповідно, вдосконалення етичних кодексів у сфері використання інформаційних технологій та кіберпростору.

Вважаємо, підвалини ефективного функціонування системи кібернетичної безпеки закладаються ще на етапі проєктування новітніх інформаційних технологій у науково-дослідницьких лабораторіях, послідовною, цілеспрямованою, професійно відповідальною роботою їхнього персоналу з обов'язковим урахуванням соціальних і морально-етичних наслідків застосування таких новацій. Завершальний користувач як кінцева ланка вказаної послідовності має чітко розуміти основні засади функціонування конкретних інформаційних технологій та користування кіберпростором.

Запорукою успіху в цій справі, на наше переконання, має стати освітня і просвітницька діяльність за активного й дієвого державного сприяння. Для продуктивної інформаційної взаємодії конче потрібна належна освіченість користувачів та їхня поінформованість щодо відповідних прав та обов'язків. Провідною ідеєю сучасної інформаційно-технологічної освіти є гуманізм, усвідомлення того, що головною метою розвитку суспільства є людина, її фізичне, інтелектуальне, духовне і психологічне зростання, котре визначає її потреби, пріоритети, інтереси й, урешті-решт, сенс життя.

Тобто, змінюючи свідомість окремого індивіда, освіта до певної міри модифікує суспільну свідомість також. Тому освіта, і в цьому її неминуща цінність, є важливим атрибутом набуття суспільством свого нового стану, де відбувається формування нової якості свідомості, як індивідуальної, групової,

так і суспільної загалом.

В інформаційному суспільстві особлива роль освіти полягає в навчанні не лише використання інформаційних технологій і кіберпростору, а й громадянських та морально-етичних засад життєдіяльності. Освітня система як суспільна інституція з формування «людини соціальної» має істотно посприяти втіленню завдання прищеплення суб'єктам інформаційних відносин розуміння й потреби дотримуватися норм інформаційної етики, а також виховання в них навиків їхнього застосування.

Крім того, на систему освіти покладається завдання, щоб всі суб'єкти суспільних відносин були поінформовані стосовно основ чинного законодавства, їхніх прав та обов'язків, проблем, з якими стикається інформаційне суспільство та шляхів їх подолання. Відтак, у процесі навчання, виховання та всебічного розвитку особистості однією із головних освітніх функцій убачається інформування, пояснення правових і морально-етичних аспектів забезпечення кібернетичної безпеки на індивідуальному рівні.

Система освіти для формування повноцінного інформаційного суспільства має домагатися, щоб кожен його член усвідомив свою роль у загальному інформаційно-безпековому процесі, був спроможним розуміти характер впливу технологій на життєдіяльність суспільства, зіставляти свою поведінку із загальноприйнятими морально-етичними цінностями. Актуальність цих тверджень підтверджується положеннями згадуваного проєкту «Етичний кодекс інформаційного суспільства» ЮНЕСКО, де правове регулювання й самоконтроль називаються запорукою належного регулювання інформаційної взаємодії [343].

Отже, на мікрорівні (індивідуальному) соціальних інформаційно-безпекових заходів передбачається формування у кожного індивіда (у тому числі із застосуванням спеціалізованих форм підготовки, тренінгів за спеціальними методиками тощо) під час використання ним інформаційних технологій і кіберпростору, участі в інформаційних відносинах особистісних настанов, моделей поведінки, сукупність яких і складає систему морально-

етичних спонук людини, котрі регулюють її діяльність в інформаційному, кібернетичному середовищі.

На соціальні заходи забезпечення інформаційної безпеки перших двох із проаналізованих рівнів впливають переважно зовнішні чинники, діяльність соціальних інституцій та інших сторонніх суб'єктів тощо. Натомість успіх «мікрорівневих» заходів зумовлюється насамперед діями безпосередньо самої людини.

Важливою умовою створення дієвої системи кібербезпеки загалом та інформаційно-психологічної безпеки кожної людини зокрема є суб'єктивний чинник – рівень усвідомлення особою наявних викликів і загроз, її бажання існувати в безпечному інформаційному й кібернетичному середовищі. Кожен має особисто прагнути оволодіти інформаційно-безпековими навичками, бажати навчитися забезпечувати в доступний йому спосіб інформаційну безпеку. Тобто, соціальна активність кожного індивіда полягає передусім, на нашу думку, в усвідомленні власних прав та обов'язків, у втіленні засад інформаційної етики як підґрунтя кібернетичної безпеки.

Таким чином, соціальні інформаційно-безпекові заходи – це ухвалена й підтримувана особою, колективом, суспільством і державою багаторівнева система технологій, спрямована на створення специфічного механізму регуляції, котрий визначає відповідну морально-етичну поведінку людини у процесі користування інформаційними технологіями і кіберпростором та взаємодії в цьому середовищі. Вказані заходи стверджують і зміцнюють усталені правові приписи й морально-етичні настанови щодо кібербезпеки. Поза тим, вони є суспільним рушієм популяризації загальнонаукової теорії кібербезпеки, котра в теперішній час формується в рамках світової наукової думки. Крім того, вони зумовлюють гуманістичну спрямованість зазначеної ідеї, а це має призвести до кардинального прогресу в розумінні сутності та особливостей феномену інформаційної, та кібернетичної безпеки.

Трансформації, які сталися у світобаченні людини на зламі тисячоліть, зумовили різке зростання вагомості ціннісної складової у глобальній

безпековій системі. Це об’єктивно підтверджує постулат, що будь-яка теорія безпеки сприймається суспільством лише тоді, коли вона має гуманістичну спрямованість, відповідає інтересам людини, поважає її права і свободи, в тому числі й інформаційні. Сучасна безпекова наука вбирає у себе все більше складових – соціальних, економічних, політичних, психологічних та багато інших. Це надає їй значно більшої динамічності, гнучкості, здатності відповідати конкретним викликам конкретного історичного періоду.

Сучасний стан формування загальної теорії кібербезпеки характеризується намаганням врахувати останні фундаментальні напрацювання у вказаній галузі та розв’язати чималу кількість проблемних питань. Останні, як убачається, зумовлені низкою об’єктивних та суб’єктивних чинників.

Це, по-перше, складний, комплексний характер зазначених проблем, розв’язання яких потребує інтегрованих зусиль різних наукових галузей. По-друге, з-поміж чинників, які впливають на стан кібербезпеки, є дуже багато суб’єктивних. По-третє, це величезне розмаїття джерел і причин викликів і загроз інформаційній безпеці.

Результатом розвитку загальної теорії кібербезпеки має стати науково-теоретичне утворення, відповідно зорієнтоване у предметному і проблемному сенсі. Проте не слід вважати її певною інтегрованою концепцією, котра вивчає усі аспекти інформаційної безпеки, які є предметом вивчення різних наукових галузей. Убачається, що штучне об’єднання цих численних і різнопланових аспектів не лише недоцільне, а й узагалі неможливе.

Утім для чіткого з’ясування місця загальнонаукової теорії кібернетичної безпеки, яка перебуває на етапі формування, потрібно виявити її взаємозв’язок з іншими спеціальними безпековими теоріями, а також із технічними, природничими й суспільними науками, позаяк питання інформаційної безпеки, як зазначалося вище, розглядаються, прямо чи опосередковано, усіма науковими галузями. Таким чином, можемо стверджувати, що, методологічно підтримуючи усі дослідження безпекової проблематики в усіх наукових

галузях, загальнонаукова теорія кібербезпеки пов’язана з кожною із них. При цьому слід підкреслити, що йдеться про універсальний цілісний феномен, котрий розкриває основні засади забезпечення інформаційної безпеки у різних сферах життєдіяльності.

Теорія кібернетичної безпеки з погляду свого теоретичного статусу є зорієнтована на розгляд комплексних наукових проблем, які є суміжними для різних наук. Це, звісно, зближує нову теорію із подібними. Вона уявляється таким напрямом наукового пошуку, котрий яскраво унаочнює умовність поділу на наукові галузі, єдність і цілісність усесвіту, оскільки на системній основі забезпечує перетин прикладних дисциплін. Себто теорія інформаційної та кібернетичної безпеки об’єднує прикладні моменти різних наук для вивчення сутності, змісту, форм, засобів і методів її забезпечення, перетворюється на методологічну базу та початковий пункт подальших розробок окремих, спеціалізованих інформаційно-безпекових концепцій.

Підбиваючи певні підсумки, зазначимо, що мінімізація викликів і загроз в кібернетичному просторі, створення безпечних умов життєдіяльності в інформаційному суспільстві потребують значних зусиль від усіх суб’єктів відповідних відносин. У цьому контексті потреба запровадження соціальних заходів забезпечення кібернетичної безпеки як принципово нової форми захисту цієї сфери якраз і зумовлена зростанням ролі в ній соціальної складової. Із цією метою розроблений комплекс освітніх та виховних заходів, проводиться широка інформаційно-пропагандистська кампанія за активної участі, зокрема, державних інститутів із залученням якнайширшого числа усіх категорій засобів масової інформації та новітніх технологій для популяризації в суспільній свідомості зразків, форм і способів моральної поведінки у глобальному інформаційному та кібернетичному просторі. Ключовою складовою цієї кампанії вбачається розгортання наукового пошуку в межах інформаційної етики – галузі етичної науки, котра проходить етап свого становлення й розвитку. Саме її основні результати мають складати базис правового забезпечення кібербезпеки України.

Соціальні інформаційно-безпекові заходи утворюють складну, багаторівневу систему, спрямовану на забезпечення кібернетичної безпеки на трьох рівнях: макро- (усе суспільство), мезо- (соціальні спільноти, організації тощо) та мікро- (індивідууми).

Головними суб'єктами захисту на першому рівні є суспільство й держава, задля забезпечення безпеки котрих у межах реалізації відповідної державної політики належить насамперед сформувати несуперечливу концепцію правового забезпечення кібербезпеки, усебічно популяризувати, за активної державної підтримки та участі, основні положення кібернетичної безпеки, права й обов'язки у цій сфері, створити міцні теоретичні, методологічні засади у сфері кібернетичної безпеки.

На другому, середньому, або мезорівні технологіями захисту його суб'єктів (соціальні групи, громадські, релігійні та інші організації чи об'єднання, професійно-виробничі структури тощо) є усталені та прийняті в різноманітних соціальних чи професійних спільнотах морально-етичні норми та правила безпечного користування інформаційними технологіями і кіберпростором, приписи та процедури взаємодії в указаній сфері.

На індивідуальному або мікрорівні соціальних інформаційно-безпекових заходів вони втілюються шляхом просвіти, навчання й виховання індивидів задля формування в їхній свідомості системи правових і морально-етичних регуляторів, відповідних алгоритмів та інструментів, котрі визначають їхню поведінку при використанні інформаційних технологій та кіберпростору.

Узагальнюючи аналіз соціальних інформаційно-безпекових заходів, зазначимо, що це – багаторівневий технологічний комплекс, який ухвалений державою і підтримується особою, колективом, групою та суспільством, спрямований на формування в суспільній свідомості специфічного механізму регулювання моральної поведінки людей у процесі користування інформаційними технологіями та кіберпростором, дотримання морально-етичних вимог в інформаційних соціальних відносинах.

У цій праці визначаються також місце в системі наукового знання загальної теорії кібербезпеки, котра консолідує всі частини інформаційно-пізнавального цілого в системі інформаційної безпеки, а також специфіка її розвитку й головні завдання. Надзвичайна вагомість захисту суспільства від інформаційно-кібернетичних викликів і загроз зумовлює потребу формування загальної теорії кібернетичної безпеки, передовсім її соціально-філософських засад. Водночас, розглянуті вище соціальні інформаційно-безпекових заходи стануть запорукою поширення й затвердження в суспільстві, в рамках новостворюваної загальнонаукової теорії інформаційної та кібернетичної безпеки, відповідної соціально-філософської концепції.

Висновки до розділу 4

Пріоритетними напрямами наукових досліджень цього розділу були: аналіз основних концепцій інформаційного суспільства, визначення ролі правовового чинника у попередженні кіберзагроз сучасному українському суспільстві, дослідження соціального аспекту в механізмах забезпечення кібербезпеки суспільства. На основі цього отримано наступні висновки:

1. За результатами аналізу основних концепцій інформаційного суспільства, обгрунтовано пріоритет розвитку суспільства на сучасному етапі - захист прав і свобод людини має бути головним пріоритетом у застосуванні інформаційних технологій і використанні кіберпростору. На цій теоретичній основі виокремлено низку кібервикликів і кіберзагроз глобальному інформаційному суспільству: деструктивний вплив на різних суб’єктів (пропаганда); економічна свобода; зіткнення культур; правозастосовні проблеми в умовах кібернетичної транскордонності; надмірна соціальна мобільність, інформаційне відчуження, сугестія, зомбування.

2. Констатовано, що на сферу прав і свобод людини безпосередньо впливає висока оперативність новацій у сфері інформаційних технологій й

використання кіберпростору, зокрема це й технології інтернету речеу, штучного інтелекту, нано технологій, інформаційно-комунікаційних технологій тощо. Відтак, набуває неабиякої вагомості проблема наслідків їхнього застосування, актуалізується потреба, аналізувати і враховувати ці обставини, налаштовуючи, зокрема, новітні технології на дотримання загальнолюдських цінностей. У цьому контексті здатність прогнозувати і впливати на вказані процеси доводить інформаційна етика. Дослідження тенденцій розвитку й використання інформаційно-телекомунікаційних технологій та кіберпростору дає підстави стверджувати, що одним із головних напрямів відповідної державної політики інформаційне суспільство має забезпечити організацію й усебічне сприяння науковому пошуку в цій сфері, глибокому аналізу та надійному передбаченню результатів розроблення, впровадження і застосування новітніх технологій. Останні мають набути соціального змісту і спрямовуватися на досягнення винятково гуманістичних цілей.

3. Обгрунтовано та підтверджено, що реальні загрози глобальному інформаційному суспільству й кожній людині несуть мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо. Доведена гіпотеза, що в таких умовах успішне розв'язання вказаних глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об'єднаних плідних зусиль усього світового співтовариства.

4. На основі аналізу практики правового регулювання запобігання кіберзагрозам сучасному українському суспільстві, визначено низку актуальних проблем сьогодення, котрі, потребують невідкладного й кардинального розв'язання: 1) дотримання відповідного законодавства, зокрема у частині кваліфікації комп'ютерних злочинів і призначення покарання, а також труднощі у його застосуванні. 2) узгодження

національного законодавства з міжнародно-правовими нормами й відповідними стандартами правозастосування. Транскордонність і транснаціональність глобальної мережі серйозно утруднює реалізацію приписів національного законодавства й контроль за його дотриманням, спричиняє юрисдикційні суперечності при розв'язанні багатьох питань – технологічних, технічних, економічних, культурологічних та інших, які виникають при використанні кіберпросторі. 3) перетворення керованих комп'ютерною технікою автоматизованих кібернетичних систем на повноцінні суб'єкти інформаційної взаємодії (першочергово це сфера IoT). У наукових дискурсах все частіше побутує думка, що нинішній світоустрій утворено саме за допомогою розумних машин, штучного інтелекту. Відповідно, серйозну небезпеку може становити можливість шляхом віддаленого управління через вказаних суб'єктів делегувати певні повноваження, реалізовувати, чи навіть перекручувати їх та спотворювати. Сьогодні в умовах тотального поширення інформаційно-телекомунікаційних технологій, використання кіберпростору часом важко визначити справжнє джерело управління й контролю – людина це чи машина й виявити при цьому якісь відмінності.

5. Обгрунтовано, що на сьогодні є всі підстави стверджувати, що на сучасному етапі розвитку суспільство потребує (в межах прийнятої моделі кібернетичної безпеки) розроблення державної соціальної стратегії застосування інформаційних технологій та використання кіберпростору, котра би вказувала на головні пріоритети прогресивного розвитку суспільства і закладала базис для створення механізму координування соціальних норм.

6. Доведено, що для успішного розв'язання проблем забезпечення кібернетичної безпеки потрібне впровадження комплексу заходів, а саме:

– активний науковий пошук у межах розвитку інформаційної етики – нової галузі етичного знання, котра перебуває на етапі свого становлення;

– освітні та виховні заходи поведінки у кіберпросторі;

– всебічна популяризація в суспільній свідомості способів, моделей і

форм морально-етичної поведінки у глобальному та національному кіберсередовищі із застосуванням при цьому найсучасніших цифрових технологій, із залученням усіх можливих ЗМІ та активною участю державних структур.

Основні результати розділу висвітлено в публікація автора [344-351].

РОЗДІЛ 5
НАПРЯМИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

5.1 Концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів

У другому десятилітті XXI століття завдяки небувалому прогресу техніки й інформаційно-телекомунікаційних технологій наші традиційні уявлення про відстані та часовий простір зазнали докорінних змін, унаслідок яких сформувався новий тип цивілізації – інформаційний. Сутність інформаційної цивілізації полягає в розвитку інтернет-технологій і розширенні супутникового зв'язку, у практично необмежених в обсязі взаєминах і спілкуванні поза просторовими межами, розробленні та миттєвому поширенні інформації і новин, а також появі та розвитку цифрової дипломатії.

У зазначених умовах глобальний кіберпростір перетворюється на майданчик зіткнення економічних, політичних і культурних інтересів та центрів сили сучасного світу, дієвий інструмент формування громадської думки та її спрямування в інтересах певних гравців. Слід визнати, що поряд із позитивними і конструктивними тенденціями, які забезпечують поінформованість про новітні досягнення людства під час розвитку світового кіберпростору, можна помітити і негативні процеси, що містять ризики для кібербезпеки держав, зокрема України.

З огляду на це інформаційна дипломатія України вважає сприяння забезпеченню кібербезпеки країни своєю головною метою і в межах реалізації

та відстоювання цієї мети прикладає значні зусилля для виконання таких завдань:

– забезпечення належного і реального сприйняття широкою міжнародною громадськістю суті зовнішньої та внутрішньої політики України;

– сприяння створенню ефективних засобів інформаційного впливу на закордонну громадську думку з метою позитивного сприйняття України;

– здійснення активної міжнародної співпраці в інформаційній сфері;

– розширення можливостей засобів масової інформації країни в міжнародному кіберпросторі;

– своєчасної й ефективної протидії кіберзлочинам і кіберзагрозам державній незалежності та національним інтересам України, духовно-етичним цінностям українського народу та історичним святиням.

Україна є прихильницею розробки комплексу міжнародних правових та етичних норм, спрямованих на забезпечення кібербезпеки, та їхнього всебічного дотримання у світовому кіберпросторі. Зважаючи на це, реалізація інформаційної дипломатії України спиратиметься на широке використання можливостей сучасних інформаційно-комунікаційних технологій [352, с. 141].

Аналіз актуальних загроз конфіденційній інформації, на основі якого формується система кібербезпеки і будується організація захисту інформації, розпочинається з усвідомлення та класифікації цих загроз. У зв'язку із цим підкреслимо, що теорія кібербезпеки оперує кількома формами класифікації інформаційних ризиків і загроз захисту інформації. Вважаємо за доцільне акцентувати на поділі загроз кібербезпеці, що бувають зовнішніми і внутрішніми.

У разі зовнішніх атак супротивник відшукує слабкі місця в інформаційній структурі, що уможливлять доступ до ключових вузлів внутрішньої мережі, сховищ даних, локальних комп’ютерів співробітників. При цьому зловмисник використовує широкий набір інструментів і шкідливе програмне забезпечення для виведення з ладу систем захисту, шпигунства,

фальсифікації або знищення даних, копіювання, завдання шкоди об'єктам власності тощо. З огляду на це не дивно, що в доповіді Всесвітнього економічного форуму «Глобальні ризики 2012» («Global Risks 2012») [353] кібератаки визначені як одна з основних загроз світовій економіці. За ймовірністю настання кібератаки входять до п’ятірки найбільших потенційних глобальних загроз. Зазначений висновок Всесвітнього економічного форуму доводить значну актуальність і велику небезпеку електронної злочинності. Спектр загроз кібербезпеці, викликаних застосуванням шкідливого програмного забезпечення, дуже широкий. Нині, наприклад, фахівці виокремлюють такі види загроз захисту інформації [49, с. 354-355]:

– упровадження вірусів та застосування інших руйнівних програмних впливів;

– упровадження програм-шпигунів з метою аналізу мережевого трафіку й отримання даних про систему та стан мережевих з'єднань;

– аналіз і модифікація / знищення встановленого програмного забезпечення;

– розкриття, розкрадання та перехоплення секретних паролів і кодів;

– використання вразливостей програмного забезпечення для виведення з ладу програмного захисту з метою отримання несанкціонованих прав читання, копіювання, модифікації або знищення інформаційних ресурсів, а також порушення їхньої доступності;

– блокування роботи користувачів системи програмними засобами тощо.

Варто відмітити, що нами наведено базовий склад загроз кібербезпеці держави у зв’язку з тим, що вичерпний перелік таких загроз зробити не можливо. Адже вони значною мірою, залежать від динаміки розвитку суспільно-політичної та міжнародної обстановки. З огляду на це стали реальними загрози:

а) створенню і розвитку національної індустрії інформації, зокрема індустрії засобів інформатизації, зв’язку та телекомунікації, задоволенню

потреб внутрішнього ринку в її продукції, а також забезпеченню накопичення, ефективного використання та збереження вітчизняних і зарубіжних інформаційних ресурсів;

б) безпеці інформаційних і телекомунікаційних засобів та систем, як створюваних на території України, так і вже розгорнутих й упроваджуваних.

Згідно з теоретичними і практичними джерелами складовими кібербезпеки є:

– стан безпеки кіберпростору, за якого забезпечується його формування і розвиток в інтересах держави, організацій та громадян;

– стан безпеки інформаційної інфраструктури, за якого інформація використовується суворо за призначенням і при цьому не здійснює негативного впливу на об’єкт;

– стан безпеки власне інформації, за якого унеможливлюється або суттєво ускладнюється погіршення таких її характеристик, як конфіденційність, доступність, цілісність.

До найнебезпечніших загроз безпеці в сучасній Україні в зазначеній сфері також належать:

– наявність зовнішніх і внутрішніх центрів політичної, релігійної, міжнаціональної та іншої напруженості в прикордонних районах суміжних Україні країн;

– збільшення на державному кордоні та прикордонній території масштабів розвідувально-підривної діяльності іноземних спецслужб;

– здійснення бандформуваннями бойових дій і терористичних акцій у прикордонній смузі та прикордонних територіях, зокрема проти військ й органів Державної прикордонної служби України.

Завдяки застосуванню сучасних інформаційно-комунікаційних технологій уявлення суб’єктів у реальному часі інтернаціоналізуються рідше, а їхню оцінку й відповідь на різні міжнародні події можна почути одразу ж після події. Усе це сприяє веденню дискусій на міжнародному рівні, створенню асоціацій між новими учасниками політичної інтерактивності.

Щоб розв’язати проблему «цифрового розриву», міжнародне співтовариство здійснює важливі кроки. На саміті «Великої вісімки», що проходив у липні 2000 р. в Японії (Окінава), наприклад, було ухвалено «Хартію глобального інформаційного співтовариства» [356]. У документі вперше у світовий контекст було введено поняття «цифровий розрив» й одним з основоположних принципів визначено імператив доступності інформаційних технологій для громадян усіх держав світу. Відповідно до основних положень Хартії було засновано міжнародну експертну раду «Група з можливостей цифрових технологій» (Digital Opportunity Task Force, G8DOT Force), головним завданням якої є пошук шляхів подолання наявної нерівності між різними державами у доступі до новин та інформації. Рада також розробила програму дій і представила її очільникам держав «вісімки» на саміті, що проходив улітку 2001 р. в Генуї. Результати саміту уможливили вироблення плану конкретних рекомендацій (так звана «Генуезька ініціатива») стосовно зазначеного питання [357]. Слід додати, що нині ініціатива з координації дій програми перейшла до Міжнародної експертної ради з інформаційно-комунікаційних технологій ООН, яку згодом було перетворено в Робочу (цільову) групу ООН з інформаційно-комунікаційних технологій (ІКТ). Виконання завдання подолання інформаційної нерівності в загальному контексті боротьби з бідністю нині покладено на ООН. Крім того, ООН у межах надання допомоги у впровадженні інформаційних технологій країнам, що розвиваються, ухвалила рішення про створення спеціального фонду обсягом 500 млн дол. Звісно, цього поки що явно недостатньо для врегулювання проблеми. З огляду на це можна зробити висновок, що нині розвиток і поширення інформаційно-комунікативних технологій у державах світу проходить дуже незбалансовано, щоб стати переконливою передумовою для соціальної інтеграції та рівності в масштабі всієї планети. «Подолання цифрової нерівності сьогодні стало пріоритетом у багатьох міжнародних організаціях.

Проблема особливо посилилась з поширенням на планеті коронавірусної

інфекції COVID-19» [358]. У цій ситуації ми спостерігаємо й інший бік проблеми: протягом останнього року спостерігалося безпрецедентне впровадження цифрових технологій в усі сфери життя. Працівники почали виконувати свою роботу он-лайн, освітні заклади усіх рівнів перейшли на дистанційну форму навчання, що значно підвищило рівень обізнаності інформаційно-комунікаційних технологій як учителів, викладачів так і тих, хто отримує знання, лікарі та пацієнти звернулися до телемедицини, політичні лідери почали відвідували віртуальні саміти, та багато інших прикладів.

Весь цифровий світ акомулював свої можливості для пошуку дієвих засобів протидії подальшому поширенню хвороби. Цифрові інструменти, такі як програми та дані смартфонів, також використовуються для перевірки розповсюдження вірусу, тоді як технічні компанії, включаючи Alibaba та Tencent в Китаї та IBM, Google і Microsoft в США, почали застосовувати свої високопродуктивні комп'ютерні можливості, щоб допомогти дослідники у пошуку ліків від цієї хвороби.

Отже, процес глобальної інформатизації, поряд із розмиванням традиційних основ національно-державної ідентичності, може сприяти актуалізації інших форм об'єднання людей. Наслідком нерівномірної та експансіоністської інформатизації може бути посилення релігійної та етнічної ідентичності людей і їхнє об'єднання за ідеологічними принципами. Це, зі свого боку, може створити передумови для появи так званих конфліктів «нового покоління». З огляду на це вона здійснює політику «відкритих дверей» та активно співпрацює з міждержавними об'єднаннями, що не пред'являють попередніх вимог до рівня її військової могутності (ООН, НАТО, ОБСЄ та ін.) та соціально-економічного розвитку.

Проте визначальним у міжнародному співробітництві нашої держави з іноземними партнерами є російський чинник. Його досить вдало визначив голова Парламентської асамблеї НАТО Паоло Алліу своєму виступі на урочистому засіданні Верховної Ради, присвяченому 20-й річниці підписання Хартії про особливе партнерство між Україною та Організацією

Північноатлантичного договору: «*Агресія Росії проти України в 2014 році відкрила нову главу в міжнародних відносинах. Україна і Східна Європа на сьогоднішній день є лінією фронту із захисту європейської безпеки і захисту того світового порядку, який склався після Другої світової війни*» [359].

Сьогодні беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх здобутків нашої держави на цьому шляхи слід вважати надання у червні 2020 року Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти так званої секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв'язку, управління військами, конкретних родів військ тощо). Крім того, EOP дає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО [360]. До цього такий статус мали лише п'ять країн, зокрема Грузія, країни-члени ЄС Швеція та Фінляндія.

Варто зауважити, що на теперішньому етапі розвитку України стан її національної безпеки залежить насамперед від ефективності результатів процесу інформатизації та прогресу у впровадженні ІКТ у військовій сфері.

У сучасних умовах проникнення глобалізації в усі сторони суспільного життя забезпечення кібербезпеки вимагає від дослідників виконання завдання наукового осмислення та здійснення наукового аналізу проблем, що тісно пов'язані з гарантуванням кібербезпеки, як найважливішого компонента міжнародної та національної безпеки. Однак, на жаль, слід констатувати: нині майже всі підходи, що покликані забезпечити кібербезпеку України, орієнтовані на військово-політичні процеси. Безумовно, це пріоритетний напрям у забезпеченні національної безпеки. Та, попри це, вони мають також акцентувати увагу на таких проблемах, як регіональна політична нестабільність, незаконний обіг наркотиків, злочинність, захист інформаційних прав людини тощо. Водночас імідж держави залишається ще одним проблемним аспектом, що прямо залежить від її інформаційної

політики. Нерідко нас сприймають як зручний полігон кіберзлочинності. Отже, глобалізація кіберпростору породила таке явище, як всеосяжний взаємообмін інформацією на загальносвітовому рівні.

В експертному середовищі останнім часом дедалі голосніше лунає така думка: щоб успішно втілювати в життя державну інформаційно-іміджеву політику, Україні слід створити інформаційну систему, яка б формувала та затверджувала позитивний образ нашої країни в російсько- та англомовному медіапросторах [82; 361]. У контексті зазначеного вище усе ж варто додати, що нині проблемі забезпечення кібернетичної безпеки приділяється достатня увага як на державному, так і на приватному рівнях. У зв'язку з проникненням технічних засобів обробки і передачі даних практично в усі сфери людської діяльності особливої актуальності набуває протидія кіберзагрозам.

Очевидно, що інформаційна сфера є самостійною галуззю національної безпеки, де необхідно гарантувати охорону інформаційних ресурсів, механізми їхнього створення, застосування та поширення, комунікаційну інфраструктуру, реалізацію прав на інформацію держави, суспільства і громадян тощо.

На сучасному етапі перед Україною постало завдання здійснення переходу до якісно нового рівня управління шляхом забезпечення всіх учасників інформаційних правовідносин достовірною, своєчасною та повною інформацією. Це можливо виконати лише завдяки послідовному реформуванню інформаційного впровадження в системі органів державної влади й управління та правильній реалізації інформаційної політики. Інформаційна політика – це здатність і можливість суб'єктів політики впливати на свідомість та психіку людей, їхню діяльність і поведінку за допомогою інформації в інтересах держави та громадянського суспільства [362]. Нині вже ні в кого не викликає сумнівів той факт, що доступність і якість інформаційних ресурсів багато в чому визначають рівень розвитку країни, її статус у світовому співтоваристві і, безперечно, стануть базовим показником статусу в перші десятиліття XXI ст. Зважаючи на це, стратегічними напрямами

національної політики забезпечення кібербезпеки мають бути:

– захист національних інформаційних інтересів, забезпечення кібербезпеки, захист від інформаційних експансій, кіберзагроз та інших недружніх акцій, їхнє усунення;

– створення, розвиток і забезпечення безпеки національних інформаційних ресурсів;

– входження у світове інформаційне співтовариство.

Продовжуючи аналіз, варто додати, що стан формування інформаційних ресурсів в Україні нині перебуває на низькому рівні. Однією з найважливіших умов розвитку єдиного кіберпростору України є всеохопна (домашня) комп'ютеризація, що дозволила б розширити кіберпростір і відкрити широкий доступ до інформаційних ресурсів, готуючи ґрунт для діалогу влади із населенням. Заслуговує на увагу те, що в Україні поступово формується ринок інформаційно-комунікаційних технологій, продуктів і послуг, зростає мережа абонентів відкритих світових мереж, збільшується кількість персональних комп'ютерів. Прискореними темпами здійснюється забезпечення населення мобільними засобами зв'язку, розширюються національна мережа зв'язку та супутникова мережа. Триває інформатизація органів державної влади, галузей економіки, банківської сфери, зв'язку, транспорту, освіти та культури тощо.

Іншим важливим аспектом внутрішнього чиннику забезпечення кібербезпеки є теоретичне осмислення та практична реалізація на рівні законодавчого забезпечення національних інтересів України в кіберсфері. Попри те, що поняття національного інтересу різними дослідниками інтерпретується неоднозначно, усе ж проглядається розуміння загальної концепції щодо нього. Концепція національного інтересу це також і концепція ідеологічна, ціннісна та суб'єктно-абстрактна. Його визначення (національного інтересу) залежить не тільки від усвідомлення та сприйняття реальної дійсності суб'єктом, що формує національний інтерес, а й від світоглядних аспектів, ціннісних орієнтирів, особистісних характеристик суб'єкта і рівня амбіційності впливу на нього з боку груп інтересів.

Вивчення й аналіз забезпечення кібербезпеки охоплює різні вияви інформації та інформування, а також є необхідним для розвитку інформаційної сфери. Під джерелами загроз кібербезпеці розуміють, зокрема, загострення міжнародної конкуренції за володіння інформаційно-технічними ресурсами, прагнення потенційних супротивників до ущемлення інтересів України у світовому кіберпросторі, витіснення її із зовнішнього та внутрішнього ринків тощо. Цілком очевидно, що в кібернетичній сфері національні інтереси і національна безпека України будуються на основі стратегічних і поточних завдань зовнішньої та внутрішньої політики держави щодо забезпечення кібербезпеки. Їх слід узгодити із цілями забезпечення кібербезпеки України.

У кібернетичній сфері можна виокремити чотири основні складові національних інтересів України:

– *Перша* – забезпечує дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни;

– *Друга* – передбачає інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів;

– *Третя* – забезпечує застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв’язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів;

– *Четверта* – передбачає захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й

інформаційних систем, як створюваних, так і тих, що функціонують на території України, тобто зазначає, що в разі несанкціонованого доступу до інформаційних систем, що містять персональні дані громадян, можуть бути порушені їхні конституційні права.

Отже, досліджуючи національні інтереси України в кібернетичній сфері, необхідно наголосити, що особливість національних інтересів полягає в тому, щоб створити в українського народу захисні механізми, які б унеможливлювали будь-які спроби зсередини і ззовні використовувати національне різноманіття в недружніх цілях національного розколу з далекосяжними намірами. З огляду на це національна політика в галузі забезпечення кібербезпеки має будуватися з урахуванням необхідності захисту життєво важливих інтересів людини, суспільства та держави, дотримання їхнього балансу, поступового розширення можливостей та неухильного дотримання основоположних прав та свобод. Представники державної влади зобов'язані надавати всебічну допомогу в захисті національних й актуальних для держави життєво важливих інтересів в кібернетичній сфері. Зважаючи на це, доцільно створити спеціальний аналітичний Центр з кібернетичної політики при РНБО України чи Інституті стратегічних досліджень, основними завданнями діяльності якого мають бути:

– вироблення концептуальних підходів до забезпечення кібербезпеки;

– підготовка проєктів постанов і розпоряджень з питань кібербезпеки та захисту інформації;

– організація і проведення експертизи проектів галузевих нормативних документів з кібербезпеки;

– надання пропозицій щодо виконання вимог нормативних актів з кібербезпеки тощо.

5.2 Міжнародні аспекти кібербезпеки України

У сучасній ситуації у світі простежується висока динаміка міжнародних політичних процесів як на глобальному, так і на регіональному рівнях. Для сучасних глобальних процесів притаманні два основні тренди – упорядкування і хаотизація. Тренд упорядкування (структуризації, управління, регуляції) процесів світового політичного розвитку проявляється у створенні різних формальних і неформальних структур: міжнародних організацій; міждержавних коаліцій, союзів, форумів, до складу яких входять державні і недержавні структури (наприклад, Давоський форум); різних міждержавних «клубів» (приміром, Група семи, Група двадцяти) тощо. Хаотизація спостерігається в таких процесах, як розпад об'єднань і коаліцій, очевидне порушення міжнародних договорів, норм, виникнення нових явищ, сутність яких погано узгоджується з тим, що було раніше, тощо. Нині досить виразно проглядаються міжнародні політичні процеси, що відображають хаотизацію й ускладнюють бачення перспектив світового розвитку. Тренд хаотизації є індикатором деструктивних явищ, що негативно впливають на підвалини політичної організації міжнародного співтовариства. Саме в межах цього тренду і проявляються кіберзагрози, які порушують міжнародну стабільність.

За таких умов зростає рівень невизначеності напрямів світового політичного розвитку, створюються передумови для значної трансформації всієї світової соціально-політичної структури і, відповідно, засад забезпечення міжнародної безпеки. Зазначені політичні зміни глобального рівня поєднуються з кардинальними і не менш значущими зрушеннями в науці і техніці. Завдяки науково-технічному прогресу розширюються сфери діяльності для акторів світової політики. Він надає їм нові засоби впливу на членів світової спільноти, міжнародні політичні процеси й інститути.

Зростання політичної активності внаслідок упровадження в життя науково-технічних інновацій також зумовлює зниження політичної організації структуризації світової спільноти.

Таким чином, на основні тенденції еволюції сучасних міжнародних відносин, а також структуру й особливості діяльності акторів, що беруть участь у цих відносинах, прямо впливає новий етап науково-технічної революції, що безпосередньо пов'язаний із розвитком інформаційно-комунікаційних технологій. Науково-технічний прогрес посприяв становленню глобального інформаційного суспільства, що уособлює новий етап розвитку цивілізації. На зазначеному етапі ключовою сферою людської життєдіяльності стає кіберпростір, що розвивається до глобальних масштабів, а найважливішими продуктами виробництва й обміну – інформація та знання. Суб'єкти глобального інформаційного суспільства часто відіграють роль акторів міжнародних відносин і, навпаки, безпосередніми й активними учасниками глобального інформаційного суспільства стають актори міжнародних відносин.

Водночас слід звернути увагу, що проблема забезпечення глобальної кібербезпеки стала зворотною стороною глобальної інформатизації людської спільноти. В усіх основних групах учасників глобального інформаційного суспільства Україна представлена досить активно. Зважаючи на це, забезпечення національної безпеки нашої країни безпосередньо залежить від рівня підтримки глобальної кібербезпеки. Дослідники проблем забезпечення кібербезпеки в сучасному світі підкреслюють, що нині інформаційно-комунікаційні технології мають реальні можливості для створення загроз і завдання шкоди безпеці світової спільноти й окремих його членів, про дані тенденції наголошується в багатьох дослідженнях [363-365].

У сучасних умовах дедалі більшого значення набуває проблема створення позитивного образу нашої країни в міжнародного співтовариства. Значний вплив на вирішення цього питання здійснюють процеси, що відбуваються у глобальному кіберпросторі.

Нині при дослідженні питань забезпечення кібербезпеки України особлива увага приділяється вивченню місця і ролі геополітичних чинників світового розвитку. Зазначені фактори істотно впливають на захист національних інтересів нашої країни в умовах формування нової геополітичної моделі світу.

Водночас варто зауважити, що інформаційний фактор як важливий інструмент впливу на міжнародну політику поєднується із традиційними геополітичними чинниками, такими як військова міць держави, її демографічний потенціал, екологічний вимір тощо. Інформаційний фактор, при з'ясуванні зовнішньополітичного потенціалу держави в сучасних умовах, слід розглядати поряд не тільки з геополітичними, а й із науково-технічними, економічними та правовими характеристиками тієї чи іншої країни. Під час розроблення та реалізації політики забезпечення національної безпеки нашої держави зазначений підхід дає змогу повніше враховувати просторові характеристики України, провідних світових держав та сусідніх країн. Слід також узяти до уваги, що нині роль кіберпростору у процесі забезпечення безпеки країни, збереження та зміцнення її суверенітету і територіальної цілісності, авторитетних та міцних позицій у світовому співтоваристві постійно зростає.

Ситуація, що склалася, потребує детального вивчення фахівцями, оскільки це істотно впливає на зміну геополітичної картини світу при забезпеченні національної безпеки нашої країни. Дослідження особливостей забезпечення національної безпеки в кіберпросторі у площині геополітики зумовлене такими обставинами:

– по-перше, подібний аналіз робить значний внесок у формування наукового забезпечення комплексного підходу до розроблення і втілення в життя концепції національної безпеки України і її важливої складової – системи заходів із забезпечення кібербезпеки;

– по-друге, дослідження геополітичних факторів у тісному взаємозв'язку з інформаційним фактором світового розвитку сприяє розгляду

міжнародних процесів з урахуванням їхнього стрімкого прискорення в наш час і зміцнення нових тенденцій у трансформації глобального співтовариства. Такий підхід може бути корисним для розроблення' політики кібербезпеки, адекватної політичним реаліям сучасного світу. Зазначена політика має стати ключовим компонентом системи заходів із забезпечення національної безпеки України, передбачаючи заходи із протидії викликам у кіберпросторі;

по-третє, геополітичний підхід має визначальне значення для осмислення участі України у глобалізаційних процесах, що безпосередньо пов'язані з інформаційними процесами як на регіональному, так і на міжнародному рівнях. Значний вплив глобалізація здійснює і на стан кібербезпеки на всесвітньому рівні. Новітні досягнення науково-технічного прогресу уможливили створення глобальних інформаційних структур, зокрема глобальної мережі Інтернет, глобальних медійних телекомпаній і мереж тощо. Як важливий інструмент інформаційного супроводу зовнішньополітичної діяльності найбільш розвинених держав, подібні системи здатні істотно впливати на міжнародно-політичну ситуацію у світі;

по-четверте, у міжнародних відносинах нові інформаційні технології створюють сприятливі умови для демократизації і розширення сфери дипломатичної діяльності. Вони відіграють активну роль у розвитку публічної (або народної) дипломатії.

Володіння (або використання) зазначеним потенціалом допомагає сучасним державам захищати національні інтереси і досягати зовнішньополітичних цілей на світовій арені. Географічне середовище й інші природні характеристики держав при цьому розглядаються в тісному взаємозв'язку з найважливішими зовнішньополітичними і міжнародними процесами як у регіональному, так й у глобальному кіберпросторах. Згадані обставини визначають статус держав у міжнародному співтоваристві та світовому кіберпросторі, а також їхні зовнішньополітичні можливості, серед яких і зовнішньополітичний інформаційний потенціал. До зазначених процесів, насамперед, належать такі:

– ведення інформаційної політики в контексті геополітичних процесів;

– досягнення інформаційної переваги в геополітичній конкуренції в кіберпросторі;

– забезпечення кібербезпеки в межах геополітичних процесів.

Беручи до уваги реалії сучасного глобального світу, розглянемо виокремлені процеси докладніше. Деякі дослідники справедливо вважають інформаційну перевагу формою реалізації геополітичної конкуренції в кіберпросторі [366].

Геополітична конкуренція – це така форма політичної взаємодії, що відображає суперництво, претензії або боротьбу двох (чи більше) держав за контроль над певним геополітичним простором (або лінією). «Геостратегічними регіонами називають найбільші за своїми розмірами і найзначніші за своєю роллю в міжнародних процесах простори. Їх також поділяють на геополітичні регіони і субрегіони, які зазвичай стають об’єктами геополітичної конкуренції. Ці процеси мають безпосередній вплив на економічний чинник» [367, с. 31]. У геополітичній конкуренції важливе значення має суперництво за контроль над геостратегічними лініями. Вони відіграють визначальну роль у формуванні геополітичного простору. Під геостратегічними лініями розуміють осі, навколо яких відбувається процес геополітичного структурування й організації простору в певному регіоні. Роль таких ліній зазвичай відіграють: морські і сухопутні комунікації (морські та океанські шляхи руху суден, залізні і шосейні дороги тощо); напрями поширення релігій, культур, ідеологій, лінії суперництва або співпраці між державами та ін. У сучасних умовах конкуренція між державами перемістилася в кіберпростір і ведеться також за інформаційно-комунікаційні канали, що формують каркас цього простору, деякі з яких є трансконтинентальними. Отже, нині в геополітичній конкуренції інформаційний фактор починає відігравати дедалі помітнішу роль. Держава, що володіє значним інформаційним потенціалом і для досягнення зовнішньополітичних цілей та захисту національних інтересів у глобальному

або регіональному масштабах здатна ефективно його застосовувати, істотно підсилює свою міць, тобто здатність впливати на міжнародні процеси у вигідному для себе ключі. Загальновідомо, що сила (або міць) держави є важливим елементом геополітичного аналізу. Категорія «сила» позначає надзвичайно складне і багатофакторне геополітичне явище. З одного боку, сила держави – це здатність однієї держави досягати в зовнішній політиці своїх цілей шляхом здійснення істотного (визначального) впливу на політику інших країн. З іншого боку, сила відображає можливості держави відстоювати свої інтереси, самостійно вирішувати життєво важливі завдання свого економічного та політичного життя. На підставі поданого можна зробити висновок: актуальним дослідницьким завданням для політичної науки, що має як теоретичне, так і практичне значення, є геополітичний аналіз кіберпростору сучасних міжнародних відносин і впливу нових інформаційних технологій на трансформацію геополітичних характеристик міжнародних процесів нашого часу. Водночас слід додати, що на формування геополітичного підходу до вивчення кіберпростору в контексті глобальних і регіональних міжнародних процесів певний вплив мали і результати геополітичного аналізу повітряно-космічного простору, накопичені в політологічних дослідженнях.

Результати геополітичного аналізу кіберпростору доводять, що інформаційні ресурси при розгортанні конкуренції в ньому відіграють особливу роль. Їхня наявність змінює характер геополітичної конкуренції у кіберпросторі, складовій частині певного геополітичного регіону. Зазначена конкуренція, як принципово важливий напрям, передбачає боротьбу за панування в кіберпросторі. Досягнення такої переваги можливе завдяки володінню інформаційними ресурсами, що за своїми якісними та кількісними показниками істотно перевершують подібні ресурси конкуруючої сторони.

У контексті геополітичних процесів цілі та завдання інформаційної політики визначаються насамперед державним устроєм і політичною системою суспільства, від яких прямо залежить організаційна структура й ефективність управління країною. Ефективність управління в сучасній

демократичній державі забезпечує і наявність таких факторів, як розвинене громадянське суспільство, функціонування засобів масової інформації та свобода громадської діяльності. Важливе значення також мають якість і традиції національної дипломатії, що забезпечує ефективну взаємодію з іншими державами і міжнародними об'єднаннями. Разом із громадськими організаціями та засобами масової інформації дипломатія формує у міжнародного співтовариства імідж країни, що істотно впливає на можливості зовнішньої політики держави, зокрема на сферу національної та міжнародної безпеки.

Отже, інформаційна політика є сферою життєдіяльності людей в умовах сучасного інформаційного суспільства, в основі якої лежать процеси збирання, оброблення та поширення інформації в інтересах органів державного управління і структур громадянського суспільства. За певних умов поширювана у процесі здійснення такої політики інформація може виходити за межі державної території та національного кіберпростору. Унаслідок виходу в міжнародний кіберпростір інформація перетворюється на важливий фактор, що впливає на геополітичні процеси, а сама інформаційна політика стає одним із ключових інструментів ведення зовнішньої політики сучасної держави.

Важливе значення для дослідження кібербезпеки має аналіз її геополітичних аспектів. Зазначений підхід зумовлений низкою причин. Насамперед геополітичний аналіз спрямований на визначення силового потенціалу держави та рівня її захищеності від зовнішніх загроз й, у підсумку, – на оцінку рівня безпеки країни. Такий аналіз ґрунтується на просторових характеристиках держави. Нині, як важливий геополітичний показник забезпечення безпеки держави, слід розглядати і конфігурацію, позиціонування та рівень її захищеності у глобальному кіберпросторі.

Збереження силової політики у світі зумовлює й актуальність у наші дні принципу балансу сил. Дії держав, інтереси яких на світовій арені то перетинаються, то зіштовхуються як у глобальному, так і регіональних

вимірах, можуть призводити до порушення балансу сил. Водночас у світовій геополітиці реалізується й інша тенденція – підтримання рівноваги балансу сил. Якщо така рівновага не суперечить інтересам більшості учасників світових і регіональних політичних процесів, то її встановлюють і підтримують, а суб'єкти, які прагнуть її порушити, опиняються або на периферії міжнародних відносин, або в ізоляції. З огляду на це слід наголосити, що баланс сил – це динамічно рівноважний процес. А політика підтримання балансу сил є ключовим напрямом зовнішньої політики України й інших провідних держав сучасного світу. Зазначена політика ведеться в таких основних вимірах:

– забезпечення національної безпеки держави, насамперед її військово-політичної складової;

– збереження військово-політичного статус-кво в усьому світі або в конкретному геополітичному регіоні;

– досягнення зовнішньополітичних цілей держави, визначених відповідно до головних пріоритетів її національної безпеки;

– забезпечення умов для стабільного та стійкого внутрішнього розвитку держави.

Виникнення глобального кіберпростору сприяє активнішому поширенню в сучасних міжнародних відносинах принципу балансу інтересів. З огляду на це концепція балансу сил – вагомий фактор у взаємовідносинах держав на міжнародній арені, які задовольняють власні інтереси, що часто суперечать інтересами інших держав. Конфлікт інтересів держав може призвести до війни. У такій ситуації сила стає неодмінною умовою для самоствердження держави у світі. Переважаюча сила примушує інших робити те, що вони ніколи б не зробили за інших обставин. Сила є сукупністю всіх можливостей (ідеологічної, військової, культурної тощо), які політичний суб'єкт має для втілення своїх інтересів. Сенс балансу сил зводиться до рівноваги силових характеристик кількох держав. Фахівці наголошують, що баланс інтересів і баланс сил різняться за низкою параметрів і характеристик.

Розглянемо ці відмінності під кутом забезпечення кібербезпеки у площині геополітичних процесів. По-перше, у процесі знаходження балансу інтересів урівноважуються національні інтереси держав та інтереси міжнародного співтовариства, а не силові потенціали. Зазначений підхід стимулює конструктивну діяльність і під час його здійснення великого значення набуває інформаційне забезпечення.

По-друге, у процесі досягнення балансу інтересів здійснюється взаємне з'ясування та врахування сторонами інтересів одна одної. Це підвищує рівень довіри у дво- і багатосторонніх відносинах, що вимагає збільшення інформаційної прозорості та дозволяє уникати великих витрат. Натомість збереження силової рівноваги характеризується неминучим для цього процесу вдосконаленням та нарощуванням озброєнь.

По-третє, принцип балансу інтересів ближчий до інформаційної сфери міжнародних відносин, ніж принцип балансу сил. Це випливає із сутності інформаційних процесів. З їхньою допомогою держави в міжнародному співтоваристві презентують свої інтереси, формують імідж своїх країн. Узгодження інтересів допомагає пошуку взаємовигідних компромісів, сприяє розвитку діалогу з найскладніших проблем світової політики. Зважаючи на це, слід підкреслити, що у сфері міжнародних відносин принцип балансу інтересів у багатьох випадках є ефективнішим, ніж принцип балансу сил. Водночас між державами, союзами держав, геополітичними регіонами і міжнародними організаціями, поряд із пошуком балансу інтересів або сил, на світовій арені часто спостерігається і конкуренція. Зміни в геополітичній структурі світу зумовлюють зміни в конфігурації геостратегічних осей і геополітичних регіонів, зміщення центрів сили. Держави, що претендують на створення полюсів світового розвитку, намагаються домінувати і в інформаційній сфері. Такі геополітичні трансформації зумовлюють зміни шляхів інформаційних потоків і розміщення інформаційних вузлів та магістралей у глобальному кіберпросторі. Зазначені зміни здійснюють вплив на стан кібербезпеки всіх основних суб'єктів міжнародних відносин, зокрема і на масову суспільну

свідомість як окремих держав, так і світової спільноти загалом. Зрушення геополітичних позицій головних учасників суперництва та конкуренції на світовій арені викликають трансформації й у сфері глобальної кібербезпеки. Згодом подібні процеси ведуть і до зміни геополітичної картини в регіональному та глобальному масштабах. З огляду на це слід наголосити, що при формуванні та веденні національної зовнішньої політики слід ураховувати окреслені проблеми забезпечення кібербезпеки в контексті геополітичних процесів.

Нині протистояння в інформаційній сфері є важливим напрямом глобальної конкуренції. Зазначені зміни у світовому розвитку експерти пояснюють низкою причин [368]. По-перше, становлення глобального інформаційного суспільства – одна з найважливіших сутнісних характеристик сучасного етапу світового розвитку. Саме інформаційно-комунікаційні технології стали основою для створення такого суспільства. Інформаційно-комунікаційні технології кардинально вплинули на спосіб життя людей, сферу державного управління, громадянське суспільство, освіту, працю та міжнародні відносини. Держави лідирують у сучасному світопорядку, якщо вони займають провідні позиції в такому важливому для XXI століття напрямі світового розвитку, як становлення глобального інформаційного суспільства. По-друге, держава, що володіє потужнішим інформаційним потенціалом, ніж її конкуренти, може ефективно просувати і відстоювати свої національні інтереси, відігравати провідну роль у регіональних і світових політичних процесах. Останнім часом для врегулювання багатьох принципових проблем зовнішньої політики ефективнішими виявляються інформаційно-пропагандистські й інформаційно-психологічні методи, замість військово-силових засобів, що широко використовувалися раніше.

По-третє, на ієрархію держав у світовому співтоваристві дедалі більше починає впливати «цифрова нерівність». Країни конкурують за доступ до інформаційних магістралей і ресурсів, до високих інформаційно-комунікаційних технологій тощо. Для сучасних країн наявність такого

доступу створює значні можливості для просування своїх національних інтересів у різних частинах світу та здійснення реального впливу в потрібному для себе напрямі на економічні та політичні процеси як глобального, так і регіонального масштабів. І навпаки, обмеження на шляху входження у глобальне інформаційне суспільство дуже негативно позначаються на можливості участі країни в сучасних міжнародних відносинах або взагалі відтісняють її на периферію світового розвитку.

Отже, слід визнати, що доступ до інформаційно-комунікативної інфраструктури є одним із важливих виявів конкуренції у глобальній інформаційній сфері. Однак велике значення для суперництва в зазначеній галузі має також здатність держави не тільки застосовувати інформаційно-комунікаційні технології, але й відтворювати їх. Країни, де телекомунікаційна галузь економіки існує як матеріальна основа національної інформаційно-комунікаційної сфери, у глобальному інформаційному протистоянні мають очевидні переваги. У сучасній телекомунікаційній сфері науково-технічний розвиток нині обумовлюється технологічними досягненнями, що пов’язані із широкомасштабним упровадженням мікропроцесорної техніки та цифрових методів передачі і комутації.

Кожне інформаційне протистояння на світовій арені має цілком визначену мету. Водночас їхній аналіз дозволяє виявити цілі загальнішого характеру, що властиві глобальному інформаційному суперництву в нинішніх умовах. До них належить:

– забезпечення національної безпеки держави у глобальному кіберпросторі;

– просування і захист національних інтересів в інформаційній сфері;

– забезпечення кібербезпеки як важливої складової системи національної безпеки;

– посилення міжнародної кібербезпеки шляхом зменшення у глобальному кібернетичному просторі можливостей для ворожого використання інформаційно-комунікаційних технологій.

Для досягнення зазначених цілей у процесі глобального інформаційного протистояння використовують відповідні методи і способи боротьби, серед яких:

– інформаційне домінування або досягнення переваги в кіберпросторі;

– інформаційна асиметрія як базовий принцип інформаційного впливу, що використовується як відповідь на зовнішній вплив, так і при здійсненні впливу на іншу сторону інформаційного суперництва;

– зовнішній контроль кіберпростору держави та управління інформаційними процесами, що здійснюється з іноземних центрів;

– інформаційне стримування як спосіб управління кризовими ситуаціями в зонах конфліктів;

– кіберагресія, в основі якої лежить незаконне здійснення однією державою інформаційного впливу на кіберпростір іншої держави, що завдає шкоди її суверенітету, життєдіяльності в різних сферах та політичній незалежності;

– кібервійна, що є найбільш гострою формою інформаційного протистояння між державами, здійснюваного насильницькими засобами і способами впливу на інформаційну сферу супротивника з метою досягнення стратегічних завдань. Нині сутність кібервійни полягає у прихованому управлінні економічними, політичними, військовими й іншими процесами держави-супротивника.

Розглянемо докладніше зазначені способи і методи, що застосовуються в умовах глобального кіберпротистояння з урахуванням потреб забезпечення національної безпеки України в інформаційному вимірі:

1. *Інформаційне домінування* (або досягнення переваги в кіберпросторі) допомагає провідним державам досягати на світовій арені політичних цілей, що відповідають захисту і просуванню їхніх національних інтересів, без застосування збройної сили. Військові дії зазвичай пов’язані із чималими матеріальними та політичними втратами. Вони завдають шкоди іміджу держави, що вдається до застосування сили, особливо коли це суперечить

нормам міжнародного права і викликає неоднозначні оцінки у світовому співтоваристві. Однак інформаційне домінування в глобальному кіберпросторі здійснює різноспрямований і неоднозначний вплив на світові політичні процеси та зовнішню політику великих держав. У багатьох випадках таке домінування створює умови для застосування військової сили, а не замінює використання збройних сил.

Інформаційне домінування є складним, багатоаспектним процесом, що зачіпає основні сфери життєдіяльності суспільства. Із проблемами забезпечення національної безпеки цей процес прямо пов’язує його вплив на життєво важливі сторони розвитку держави і суспільства.

Сутність процесу інформаційного домінування (або переваги) – збирання та поширення інформації, що безпосередньо пов'язує його з розвідувальною та військовою діяльністю. У потужному впливі на суспільну свідомість проявляється інформаційна перевага, а через нього, як і для інших цілей, здійснюється вплив на економічні та політичні процеси, поведінку політичних і бізнес-еліт, діяльність засобів масової інформації у державах, на які направлено інформаційний тиск домінуючої держави.

Інформаційна перевага, як комплексний і багатоаспектний процес, пов'язана з іншими важливими процесами і діями в регіональному та глобальному кіберпросторах. Розглянемо їх також детальніше.

2. Одним із фундаментальних принципів інформаційного впливу є *інформаційна асиметрія*. Він може бути використаний як стороною, що має інформаційну перевагу і прагне до інформаційного домінування, так і стороною, що в інформаційному протистоянні захищається від зовнішнього впливу. Застосування інформаційної асиметрії помітно впливає на побудову конфігурації кіберпростору сучасної держави. Асиметрія (від грец. *asymmetria*) означає нерівномірність, невідповідність. Стосовно питання інформаційної асиметрії зазначене поняття в сучасних дослідженнях застосовують у кількох значеннях. По-перше, асиметрію розглядають як ситуацію, у якій для порівняння не існує спільної основи. У галузі

кібербезпеки асиметрія може проявлятися як використання асиметричних інформаційних стратегій і поява асиметричних загроз. Інформаційний вплив може поєднуватися із діями з інших сфер, наприклад, у поєднанні з військовими і політичними кампаніями. У такому випадку кіберпростір сполучається з просторами інших видів діяльності: економічним, політичним, військовим тощо. По-друге, асиметрію застосовують для характеристики діяльності, що ведеться приховано. На такі впливи або відсутня будь-яка реакція, або робляться захисні дії загального порядку в межах усього інформаційного поля держави, оскільки вони не помічаються і не фіксуються протилежною стороною. Держави не можуть забезпечити належний захист (або такий захист відсутній взагалі), тому що такі дії не фокусуються на асиметричній загрозі та не мають цілеспрямованого характеру. По-третє, асиметрію розуміють як вибіркову, обмежену відповідь на недружні інформаційні впливи супротивника.

Нині очевидно, що для стримування немає необхідності в підтриманні паритету з можливим агресором ні в завданих збитках, ні в кількості озброєнь. Достатньо зберігати можливість завдати йому неприйнятного збитку як ударними силами – у відповідних діях, так й оборонними: у процесі відбиття збройного нападу. Вибіркове стримування виправдано ще й в умовах, коли противники незіставні ні за економічною, ні за військовою міццю. Для тотального стримування стороні, що має слабший військовий потенціал, доведеться мобілізувати максимально великі ресурси, руйнуючи тим самим інші складові національної безпеки. Саме тому менш потужні в економічному і військовому сенсах країни змушені уникати спроб досягнення і підтримання паритету із сильнішими потенційними супротивниками. Зазначену стратегію застосовують для забезпечення національної безпеки. У нинішніх умовах подібний підхід актуальний і для забезпечення кібербезпеки України.

3. Як спосіб управління кризовими ситуаціями в зонах конфліктів, а також інших сферах глобального інформаційного протистояння, застосовують *інформаційне стримування*. У нинішніх умовах глобального інформаційного

суспільства структура військового стримування сучасної держави має, поряд із системою озброєння для виконання завдання стримування армії ймовірного противника, передбачати систему сил і засобів для інформаційного протистояння експансії можливого агресора в інформаційній сфері. Основними напрямами дій інформаційної системи, що є структурним елементом військового стримування, є виконання таких завдань:

– по-перше, активна протидія зовнішньому інформаційному тиску та спробам з боку супротивника послабити оборонний потенціал і завдати шкоди національній безпеці держави;

– по-друге, інформаційна компонента структури військового стримування має бути спрямована на: а) надання міжнародній спільноті інформації про наявність у нашої країни військового потенціалу для стримування будь-якого агресора; б) інформаційний вплив, спрямований на створення у військово-політичного керівництва та широких прошарків суспільства держав – потенційних супротивників переконливого уявлення про невідворотність завдання по них удару з неприйнятним для них збитком.

Вплив на масову суспільну свідомість зовнішнього контролю й управління інформаційними потоками має надзвичайно критичний характер. Думка громадян в умовах демократичних суспільств безпосередньо враховується при ухваленні владою відповідальних зовнішньо- і внутрішньополітичних рішень; підтримка суспільством конкретних політичних дій уряду сприяє їхній успішній реалізації; негативне ставлення громадськості до таких дій може призвести до їхнього провалу і погіршення ситуації в країні. Отже, з огляду на це, громадську думку слід вважати головним об’єктом інформаційно-психологічного впливу, що дійсно може містити певні загрози національній безпеці держави.

Інформаційна агресія – одна із форм активного інформаційного протистояння, для заподіяння конкретного відчутного збитку іншій державі у важливих для неї сферах життєдіяльності. Зазвичай інформаційна агресія локалізована в геополітичному просторі й обмежена за масштабами

застосування інформаційного впливу. Зазначений вид інформаційного протиборства спрямований на реалізацію конкретних цілей і зазвичай завершується після їхнього досягнення. Інформаційна агресія може бути як самостійним видом глобального інформаційного протистояння, так і доповнювати ворожі дії, що здійснюються за допомогою звичайних збройних сил.

Отже, інформаційна війна має на меті набуття військово-стратегічної переваги над ворогом завдяки потужнішому інформаційному потенціалу. На практиці здійснення інформаційної війни реалізується за допомогою виконання інформаційних операцій. Вони спрямовані на маніпулювання інформацією для досягнення і підтримання інформаційної переваги над супротивником унаслідок вирішального впливу на його інформаційну інфраструктуру за одночасного захисту власної. Інформаційні операції здійснюють комплексно. Вони бувають двох видів: наступальними та оборонними. Проведення інформаційних операцій в межах інформаційної війни призводить до загострення на світовій арені глобального інформаційного протистояння.

Таким чином, по-перше, нині у світовому розвитку досить виразно проявляється тренд хаотизації міжнародних політичних процесів, що зумовлює формування передумов для значної трансформації всієї світової соціально-політичної структури і, відповідно, принципів забезпечення міжнародної кібербезпеки. Політичні зміни у світовому співтоваристві поєднуються з кардинальними і не менш значущими зрушеннями в науці і техніці, які пов’язані із фантастичним стрибком в удосконаленні інформаційно-комунікаційних технологій. Найважливіший результат таких змін – становлення глобального інформаційного суспільства, що уособлює новий етап розвитку цивілізації. Виник тісний взаємозв’язок між акторами міжнародних відносин та суб’єктами глобального інформаційного суспільства, яків доповнюють один одного, хоча часто їхню роль виконують одні й ті ж учасники міжнародних процесів. До них належать держави,

транснаціональні медіакорпорації, великий бізнес, транснаціональні соціальні мережі, некомерційні та неурядові організації, громадянські інститути, індивідууми. З огляду на те, що Україна безпосередньо і широко представлена в усіх основних групах учасників глобального інформаційного суспільства, забезпечення національної безпеки нашої країни пов’язане насамперед із феноменом глобальної інформаційної безпеки. Водночас від дій України як загальновизнаної світової держави певною мірою залежить підтримання глобальної кібербезпеки. Зазначений взаємозв'язок конкретизує і підвищує роль міжнародного чинника в забезпеченні національної безпеки нашої країни в сучасних умовах.

Міжнародний фактор відіграє вагому роль у створенні загроз національній безпеці нашої країни, що виходять із глобального кіберпростору. Вони пов’язані із: діяльністю регіональних і глобальних ЗМІ; виникненням й активізацією приватних PR-агентств, що в кіберпросторі виконують завдання з ведення підривних операцій проти інших країн; з мережевими комунікаціями, що утворюють нову додаткову структуру нинішнього суспільства. Загрози інформаційного забезпечення державної політики України безпосередньо пов’язані з міжнародними та зовнішньополітичними аспектами діяльності нашої держави. Міжнародний фактор відіграє вагому роль у створенні загрози розвитку національної індустрії інформації, зокрема телекомунікаціям і зв’язку, індустрії засобів інформатизації.

Питання забезпечення кібербезпеки в сучасному глобальному світі перебуває у фокусі уваги національної зовнішньої політики. При цьому Україна пропонує важливі ініціативи стосовно міжнародно-правового забезпечення глобальної кібербезпеки.

В умовах сучасного глобального світу традиційні геополітичні чинники, серед яких військова міць держави, її демографічний потенціал, екологічний вимір тощо, доповнюються інформаційним фактором як важливим інструментом здійснення впливу на національну безпеку і міжнародну політику. Унаслідок упровадження у міжнародні процеси інформаційних

технологій, наприклад, з’явилися нові загрози геополітичного характеру національній безпеці України. Для їхнього вивчення й осмислення необхідне виконання відповідного аналізу з позицій сучасної геополітичної теорії. Географічне середовище й інші просторові характеристики держав розглядаються при цьому в тісному взаємозв'язку зі станом регіонального, національного та глобального кіберпросторів.

Статус держави в міжнародному співтоваристві дедалі більше починає залежати від її зовнішньополітичного інформаційного потенціалу та від її місця і ролі у світовому кіберпросторі. У глобальному кіберпросторі, що перебуває в тісному зв’язку зі світовим геополітичним простором, розгортаються такі міжнародні процеси: суперництво між провідними державами за досягнення інформаційної переваги у процесі геополітичної конкуренції; забезпечення кібербезпеки в межах геополітичних процесів; реалізація інформаційної політики із захисту геополітичних інтересів конкретних держав тощо.

Інформатизація сучасного міжнародного співтовариства нині відбувається в тісному взаємозв’язку з ускладненням та зміною геополітичної структури світу. Зазначений процес, зокрема за рахунок формування та розвитку глобального, регіонального та національних кіберпросторів, сприяє подальшій диференціації всередині цієї структури. Зростання ролі інформаційних ресурсів у сучасних геополітичних процесах зумовлює геополітична конкуренція між різними державами й іншими суб’єктами міжнародних відносин у цих просторах. Інформаційна міць провідних держав сучасного світу дозволяє їм у деяких випадках втілювати в життя свої ключові геополітичні цілі без допомоги силових інструментів. Водночас розвиток глобального кіберпростору сприяє активнішому поширенню принципу балансу інтересів у забезпеченні кібербезпеки в межах геополітичних процесів.

Протистояння в інформаційній сфері є одним з основних напрямів глобальної конкуренції в сучасному світі, важливими сторонами якого слід

розглядати доступ до інформаційно-комунікаційної інфраструктури, а також здатність держави відтворювати інформаційно-комунікаційні технології, а не тільки бути в змозі використовувати їх. Для глобального інформаційного суперництва характерні такі цілі:

– забезпечення національної безпеки держави в глобальному кіберпросторі;

– просування і захист національних інтересів в інформаційній сфері;

– зміцнення міжнародної кібербезпеки шляхом зменшення можливостей для агресивного використання інформаційно-комунікаційних технологій у глобальному кіберпросторі;

– забезпечення кібербезпеки як значущого елемента в системі національної безпеки.

5.3. Пріоритети розвитку правових основ державної політики України у сфері кібербезпеки

З огляду на те, що необхідною складовою забезпечення кібербезпеки є захист інформації, державних інформаційних ресурсів, інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, то і діяльність щодо розв’язання цих питань, насамперед шляхом формування державної політики, слід розглядати як основу для забезпечення захищеності життєво важливих інтересів держави, суспільства і людини, за якої запобігається завдання шкоди внаслідок негативних наслідків застосування інформаційних технологій, а також порушення конфіденційності, цілісності та доступності інформації, що шириться в інформаційних та технологічних системах. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв’язку) відповідно до чинного законодавства в межах

забезпечення інформаційної безпеки здійснює формування та реалізацію державної політики у сферах технічного та криптографічного захисту інформації, інформаційно-телекомунікаційних систем, захисту державних інформаційних ресурсів у кіберпросторі. До актуальних проблем кібербезпеки, від урегулювання яких безпосередньо залежить ефективність діяльності українських державних інформаційних ресурсів в умовах сучасних викликів і загроз у кіберпросторі у сфері захисту інформації та кіберзахисту, належить проблема підготовки і перепідготовки кадрів, насамперед у сфері інформаційної безпеки та кібербезпеки.

У контексті розв'язання поставлених завдань у 2016 р. було затверджено Стратегію кібербезпеки України. У травні 2018 р. набув чинності Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Кіберзакон), де на законодавчому рівні закріплено основні цілі, напрями та принципи державної політики в галузі кібербезпеки, а також обов'язки і повноваження державних органів, установ, організацій, підприємств, осіб і громадян у цій сфері, що дало можливість розвивати в нашій країні сучасну цілісну національну систему кібербезпеки. Ухвалення Кіберзакону стало могутнім поштовхом до втілення в життя таких актуальних європейських практик, як управління інформаційною безпекою та її аудит, застосування галузевих стандартизованих вимог до кіберзахисту об'єктів критичної інфраструктури тощо. Отже, уперше у правове поле України було введено базовий понятійно-термінологічний апарат сфери кібербезпеки, зокрема визначення понять критичної інфраструктури і її технологічних/комунікаційних систем; визначення понять кіберзахист, кіберзагрози, кібертероризм, кібератаки, кібероборона та ін. Упродовж останніх двох років було реалізовано низку практичних рішень організаційно-технічної моделі кібербезпеки, зокрема:

– відкрито Центр реагування на кіберзагрози (Cyber Threat Response Centre, CRC);

– створено державний контур кіберзахисту;

– активно розвивається Національна телекомунікаційна мережа;

– здійснено докорінну модернізацію Системи захищеного доступу до Інтернету тощо.

Зазначені рішення, упроваджені Держспецзв'язком, відповідають найпотужнішим і найсучаснішим аналогам у світі, їхнє розроблення і реалізація стали можливими завдяки наявному національному науково-технічному потенціалу. У наш час активно здійснюється масштабування системи кіберзахисту на всі регіони України із приєднанням до неї ІТ-систем критичної інфраструктури, насамперед галузей енергетики, фінансового і транспортного секторів, охорони здоров'я, а також заснування галузевих центрів кібербезпеки і розбудова мережі команд реагування на комп'ютерні надзвичайні події, зокрема і спираючись на механізми державно-приватної взаємодії та партнерства. Держспецзв'язком завдяки втіленим унікальним технологічним рішенням здатна з високою точністю фіксувати в режимі 24/7 раннє виявлення аномальної активності і потенційно небезпечних подій у кіберпросторі, спрямованих на мережі і системи, підключення до Інтернету, зокрема на об'єктах критичної інфраструктури. Це значно підвищило оперативність й ефективність діяльності основних суб'єктів забезпечення кібербезпеки із протидії кіберзагрозам, боротьби з кібертероризмом та розслідування кіберзлочинів. Нині в галузі кібербезпеки також відбувається формування нормативно-правової бази діяльності. Проєкти нормативно-правових актів, підготовлені на виконання Кіберзакону, закладуть основи для:

– формування переліку об'єктів критичної інформаційної інфраструктури, ведення їхніх реєстрів;

– проведення незалежного аудиту стану кіберзахисту об'єктів критичної інфраструктури;

– ужиття заходів із захисту від кіберзагроз об'єктів критичної інфраструктури;

– організації заходів щодо взаємодії основних суб′єктів діяльності у сфері кібербезпеки при запобіганні, виявленні, припиненні кібератак, усуненні їхніх наслідків;

– упровадження альтернативного способу підтвердження відповідності інформаційної системи вимогам щодо захисту інформації через упровадження вимог стандартів Системи управління інформаційною безпекою (СУІБ);

– уведення процедури оцінювання відповідності та процедури оцінки відповідності і забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, які застосовують у процесі взаємодії між суб'єктами різних держав при наданні юридично значимих електронних послуг та ін.

Крім того, передбачені заходи із визнання іноземних й українських сертифікатів відкритих ключів та електронних підписів. Слід підкреслити, що в підготовлених проєктах нормативно-правових актів ураховані вимоги директив ЄС 2016/1148 та 2008/114, стандартів з управління інформаційною безпекою ISO/IEC серії 27000 і стандартів, відповідно до яких забезпечується інформаційна безпека в НАТО. Україна для процвітання своєї економіки і держави поступово досягає цілей програми МСЕ «Connect 2020» і разом із міжнародними партнерами консолідує зусилля для досягнення максимального прогресу в розвитку інформаційного суспільства та використанні переваг інноваційних ІКТ.

Слід зауважити, що нині Україна має у своєму арсеналі сучасні засоби кіберзахисту і постійно рухається в напрямку їхнього вдосконалення, як у технічній так і нормативно-правовій площині. Проте варто визнати, що спостерігається нагальна потреба залучення фахівців із кібербезпеки інших країн з метою обміну досвідом у сферах розслідування кіберінцидентів, експертизи програмного коду, здійснення аудиту інформаційної безпеки на об'єктах критичної інфраструктури, проведення тестів на проникнення, виявлення мережевих вразливостей, реагування на кіберінциденти й усунення їхніх наслідків. Також гостро стоїть питання участі фахівців Держспецзв'язку

в міжнародних заходах із кіберзахисту об’єктів критичної інфраструктури (семінари, конференції, тренінги тощо), оскільки такі заходи постійно відбуваються у провідних країнах-партнерах. Крім того, з метою підвищення рівня кібербезпеки пропонуємо на міжнародному рівні порушити питання створення єдиної міжнародної інтерактивної бази кіберінцидентів. Серед конкретних заходів, що могли б бути реалізовані міжнародним співтовариством на глобальному рівні для посилення кібербезпеки, можна назвати такі:

– розроблення і впровадження правових повноважень, юрисдикційних правил та інших процедурних положень для забезпечення ефективного розслідування злочинів, скоєних за допомогою ІКТ, зокрема:

- коригування норм збирання, зберігання, засвідчення і використання у кримінальному розслідуванні електронних доказів;
- ухвалення положень, що регулюють проведення внутрішніх і міжнародних обшуків;
- розроблення положень, що стосуються міжнародних та національних відстежень повідомлень;
- ухвалення положень, що стосуються перехоплення повідомлень, переданих через комп′ютерні мережі й аналогічні засоби масової інформації тощо;

– для подолання розриву між швидкістю, з якою працюють кіберзлочинці, і темпами реагування правоохоронних органів, здійснити розширення міжнародної співпраці між правоохоронними органами, прокуратурою та судовими органами, а також інтернет-провайдерами;

– реалізація за умови наявності ресурсів міжнародних проектів технічної взаємодії та допомоги. Зазначені проєкти могли б об'єднати експертів у галузі законодавства, запобігання злочинності, судового переслідування, комп′ютерної безпеки, методів розслідування і суміжних питань з державами, що потребують інформації або допомоги в цих сферах;

– розроблення освітньої програми, що сприятиме підвищенню рівня знань та поінформованості про протидію кіберзлочинності.

Виокремлена проблема обґрунтовується великою кількістю випадків промислового кібершпигунства, що залишаються неврахованими. Це можна пояснити, зокрема:

– складністю виявлення факту витоку конфіденційної інформації (відомостей, що становлять комерційну або банківську таємницю, персональних даних);

– небажанням приватних осіб або компаній визнавати себе жертвами зловмисників через стурбованість можливістю правоохоронних органів отримати доступ до інформації, яку від них приховували постраждалі, та небажання зашкодити іміджу фірми;

– тим, що зазвичай окремій компанії хакери завдають несуттєвих збитків, унаслідок чого менеджментом ухвалюється рішення про недоцільність розслідування їхніх дій, що не виправдає витрачених на нього ресурсів (коштів, робочого часу тощо).

Для України характерний досить високий ступінь розвиненості інформаційно-телекомунікаційної інфраструктури. Сфера ІКТ – одна з небагатьох, що невпинно розвивається протягом усього періоду розвитку нашої держави. Унаслідок цього у критичну залежність від необхідності стабільного та безпечного функціонування комп’ютерних систем, зокрема й приєднаних до мережі Інтернет, уже потрапила значна кількість українських підприємств, організацій та установ усіх форм власності. Водночас національне законодавство України у царині захисту важливих для держави і суспільства підприємств, організацій та установ недержавної форми власності перебуває на початковій стадії формування. Наприклад, досі не ухвалений Закон «Про критичну інфраструктуру і її захист», не розроблені норми кіберзахисту, рекомендації щодо їхньої реалізації, методики контролю за їхнім дотриманням для недержавного сектору, хоча варто визнати, що уповноваженими державними органами України заходи в цьому напрямі

вживаються.

Зважаючи на глобальний характер мережі Інтернет, кіберзлочинність набула транскордонного характеру. Це означає, що злочинець й об'єкт злочину можуть проживати в різних державах, навіть на протилежних кінцях земної кулі. Цілком імовірна також ситуація, коли зловмисник і потерпілий перебувають в одній країні, а провайдер інтернет-послуг, допомогу якого зловмисник використав для скоєння злочину, – за кордоном. Отже, у питаннях розслідування кіберзлочинів назріла гостра необхідність ефективного міжнародного співробітництва. Однак національний суверенітет без дозволу місцевої влади не допускає збирання слідів злочину на території країни. Міжнародна співпраця вимагає дотримання багатьох формальностей і значного часу. При цьому іноземні правоохоронні органи надають допомогу на принципі добровільності, тобто не завжди. Її надання ускладнюється, а іноді взагалі стає неможливим у разі, якщо в країні, до якої звертаються за допомогою, діяння, що розслідується, не визнано злочином, або воно має інший рівень суспільної небезпеки. Зазначений фактор зловмисники можуть свідомо використовувати для здійснення кіберзлочинів через територію третіх країн з метою ускладнення їхнього розслідування.

Кримінальна відповідальність є персональною. Це означає, що до відповідальності за вчинення злочину притягується конкретна особа. Інакше кажучи, за результатами розслідування кіберзлочинів слід встановити персоналії зловмисника. Однак Інтернет надає значні можливості анонімного доступу до інформаційних ресурсів, що активно використовується з протиправною метою. Таким чином, для приховування злочину зловмисник може вийти в Інтернет через безпровідну точку доступу загального користування, що часто розміщуються в супермаркетах, аеропортах та інших громадських закладах; через обладнання трансляції мережевих адрес (NAT) і віртуальні приватні мережі (VPN); скористатися послугами передплаченого мобільного зв'язку, анонімними поштовими скриньками або анонімними серверами зв'язку тощо.

Розслідування кіберзлочинів значно ускладнюється вільним доступом в Інтернеті до засобів шифрування повідомлень. Остання версія операційної системи Microsoft, наприклад, дає можливість шифрування всього жорсткого диска. Доступні також засоби шифрування інтернет-телефонії та електронної пошти. В Україні злочинці можуть безперешкодно користуватися програмами криптографічного захисту, що розміщені на багатьох ресурсах. А вітчизняні правоохоронні органи, навпаки, набагато відстають від них у можливості отримати доступ до зашифрованих повідомлень. Для подолання шифрування методом перебору ключів при використанні 128-бітного ключа, наприклад, потрібні мільярди років. Зате для шифрування PGP в одній із нових версій загальнодоступного продукту застосовують 1024-бітний ключ [369-370].

Для нормалізації правового статусу цифрових доказів Україна вживає певних заходів. Національною поліцією і СБУ, наприклад, спільно розроблений законопроєкт про внесення змін і доповнень до Кримінального процесуального кодексу України в частині, що стосується цифрових доказів [371]. Водночас занадто повільний процес ухвалення необхідних державі законів ускладнює розв’язання досліджуваної проблеми.

У деяких випадках розбіжність інтересів українських бізнес-структур сфери ІКТ і держави іноді стає причиною конфліктних ситуацій, що гальмують проведення своєчасних, ефективних і повних розслідувань комп’ютерних злочинів. Такі конфліктні ситуації в Україні неодноразово проявлялися у:

– спробах зашкодити вилученню телекомунікаційного обладнання, що містило фактичні дані про злочин;

– намаганнях законодавчо заборонити вилучення телекомунікаційного обладнання в інтересах кримінальних розслідувань;

– рішеннях інформаційних кампаній, що дискредитують слідчі дії правоохоронних органів щодо бізнес-суб′єктів сфери ІКТ.

Вимагає також урегулювання питання про збереження в автентичному вигляді комп’ютерних даних з моменту встановлення факту їхньої наявності в

комп’ютерному обладнанні до моменту вилучення (копіювання) правоохоронним органом.

Обіг й емісія криптовалюти характеризуються децентралізацією й анонімністю. Фахівці прогнозують зростання ризиків, пов’язаних із легалізацією (відмиванням) коштів за допомогою криптовалюти, оскільки зазначений інструмент фінансових розрахунків стає дедалі більш популярним та життєздатним методом оплати товарів і послуг [372]. Зокрема, зростання кількості підприємств, що приймають платежі у криптовалюті, збільшить ризик використання останніх злочинцями без виведення їх у фіатні гроші (насамперед через «DarkNet», з використанням засобів посилення анонімізації угод на кшталт мережі «Tor») [373]. За оцінкою фахівців, фінансування тероризму при цьому залишається одним із найбільш затребуваних напрямів використання криптовалюти з протиправною метою, оскільки криптовалюта дозволяє здійснювати швидкі анонімні транскордонні грошові перекази. До того ж криптовалюта зазвичай функціонує в межах складної інфраструктури, до якої входить низка осіб, які часто перебувають у різних країнах і забезпечують здійснення платежів та перекази грошових коштів. Зазначена сегментація послуг зумовлює плутанину, внаслідок чого не завжди зрозуміло, хто конкретно відповідає за реалізацію правозастосовних заходів та забезпечення дотримання вимог здійснення нагляду. Окреслена проблема дуже актуальна для Служби безпеки України через нестачу практичного досвіду протидії фінансуванню тероризму із застосуванням криптовалютних угод, та брак сил і засобів, залучених до зазначеного напряму роботи.

У цьому контексті існує й інший погляд. Так, аналітики ForkLog взяли за основу дослідження дані Chainalysis, Управління ООН з наркотиків та злочинності і дійшли висновку, що на кожен долар, витрачений у так званому даркнеті за допомогою біткоїну, припадає $ 800, що відмиваються через фіатні гроші [374].

Відомо, що переважну більшість справ ведуть неспеціалізовані судді і прокурори, оскільки рівень спеціалізації фахівців у боротьбі з

кіберзлочинністю не завжди відповідає сучасним викликам і загрозам. Це негативно позначається на процесі проведення розслідування.

Проблема ускладнюється функціонуванням розвиненого комерційного сектора ІКТ, розмір заробітної плати в якому значно перевищує рівень грошового утримання правоохоронців, наслідком чого є масові звільнення останніх. При аналізі стану інформаційної безпеки на рівні держави саме у царині протидії кіберзлочинності слід ураховувати те, що зазначений пріоритетний напрям діяльності перебуває на стадії формування, створення ефективних інструментів і методики та напрацювання необхідного досвіду і практики. Упродовж останніх років і натепер у сфері кіберзлочинності прослідковується значний рівень латентності і неочевидності кримінальних правопорушень. За винятком окремих масштабних кібератак, про більшість кіберзлочинів жертви не повідомляють у правоохоронні органи і вони залишаються невиявленими або непоміченими. Водночас у загальній картині яскраво виділяються саме злочини, які виявляють підрозділи Національної поліції України, що пов’язані з:

– протиправним заволодінням грошовими коштами внаслідок несанкціонованого втручання шкідливого програмного забезпечення в роботу засобів дистанційного банківського обслуговування – так званих банківських троянів (англ. – banking trojans), або шляхом компрометації електронних поштових бізнес-скриньок (англ. – business email compromise);

– протиправним заволодінням і поширенням конфіденційної службової або приватної інформації шляхом несанкціонованого використання вразливостей систем управління базами даних і веб-серверів (англ. – Sqlinjections);

– протиправним заволодінням і поширенням конфіденційної приватної, або службової інформації шляхом несанкціонованого доступу до облікових записів корпоративних або публічних електронних поштових сервісів, соціальних мереж, зокрема і шляхом вивчення баз даних, викрадених раніше (англ. – leaked database parsing);

– блокуванням інформації, що обробляється в електронно-обчислювальних машинах під впливом шкідливого програмного забезпечення – так званих шифрувальників-вимагачів (англ. – ransomware), поширених, зокрема, через отриманий допуск шляхом атаки грубого перебору паролів та логінів (brute force attack).

Протягом останніх років в експертному середовищі активно вживають термін «інформаційна війна» як відображення крайнього прояву інформаційного конфлікту. З огляду на це постає закономірне запитання про правове розуміння суті й ознак зазначених категорій, чи можна здійснювати вплив на конфліктні інформаційні відносини, що сформувалися в середовищі інформаційних технологій, чи є досліджувані категорії правовими поняттями.

Річ у тім, що в національному законодавстві не зустрічаються терміни «інформаційна зброя» й «інформаційна війна», хоча в доктрині та офіційних публічних виступах і заявах такі категорії досить поширені.

У широкому розумінні, з погляду інформаційного права, під інформаційною зброєю розуміють інформаційні технології, засоби і методи, призначені для ведення інформаційної війни. На нашу думку, таке визначення має входити до основних термінів, що містяться в Законі України «Про основні засади забезпечення кібербезпеки України».

До того ж вважаємо за доцільне доповнити Кіберзакон таким змістом: «*основною загрозою в галузі міжнародної інформаційної безпеки є використання інформаційно-комунікаційних технологій для вчинення різних протиправних дій, зокрема як інформаційну зброю у військово-політичних цілях. Умови, що створюють можливості протидії загрозам використання ІКТ, належать до основних напрямів державної політики*».

Використання ІКТ можливе з метою втручання у внутрішні справи суверенних держав, зокрема шляхом ведення екстремістської діяльності. Задля захисту від таких агресивних дій передбачається розроблення міждержавної системи заходів із протидії екстремістській діяльності. Серед першочергових заходів має бути створення міжнародного механізму із

запобігання протиправним діям та забезпечення постійного моніторингу за використанням ІКТ з метою недопущення шкідливого інформаційного впливу на інформаційну інфраструктуру, для боротьби з екстремізмом тощо. Інформаційний вплив, відповідно до звіту, опублікованого Корпорацією РЕНД (Research and Development) – це принципово новий самостійний вид стратегічного протистояння, використовуючи яке можна створювати конфлікти і без застосування збройної сили [375].

Держави пов’язують зазначені протиправні дії з інформаційними загрозами. Це доводить те, що останнім часом як стратегічну мету держави визначили боротьбу з можливим використанням ІКТ у галузі ведення інформаційних війн і з метою руйнування держави.

Сферу, масштаб і глибину можливого інформаційного впливу можна визначити, оцінивши кількісні та якісні параметри поширюваної інформації. Кількість інформації визначає сферу і масштаб охопленого впливу і може служити мірилом інформаційної агресії. Якість інформації виражається структурою сукупної інформації і визначає можливі сторони впливу.

У зв’язку з поширенням і використанням інформації виникає закономірне запитання: чи можна технологічно регламентувати, зафіксувати та визначити її поширення і чи можливо здійснити нормативне регулювання її кількості та якості.

Інформаційною зброєю можна вважати інформацію, техніко-технологічні й апаратно-програмні засоби, за допомогою яких можливо поширювати інформацію. Прикладами інформаційної зброї можуть служити апаратно-програмні засоби (комп’ютерні програми), будь-які канали зв’язку, техніко-технологічні системи, матеріальні носії інформації тощо.

Донедавна поняття «конфлікт» і «війна» розглядали як частину і ціле. Активне застосування інформації та інформаційних технологій як інструменту інформаційного впливу на державу, людину та суспільство вимагало розмежувати поняття інформаційного конфлікту й інформаційної війни. Цей факт формально був закріплений Законом «Про основні засади забезпечення

кібербезпеки України», яким у п. 3 ст. 1 визначено інцидент кібербезпеки (далі – кіберінцидент) як «подію або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у т. ч. зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів тощо».

При цьому подано класифікацію воєн (великомасштабна війна, регіональна війна, локальна війна) і конфлікту (військовий конфлікт, збройний конфлікт, військова загроза). У Воєнній доктрині України згадано «інформаційну війну Російської Федерації проти України» [376].

Міжнародною групою експертів НАТО у 2013 р. підготовлено Талліннське керівництво із застосування міжнародного законодавства до кіберсфери [377]. У ньому, серед іншого, зазначено, що у 2011 р. Департамент США з безпеки ухвалив Стратегію «Операції в кіберпросторі», де кіберпростір визначено як експлуатаційну зону. США створили державну структуру «кіберкомандування», мета якої – проведення кібероперацій [378]. Подібні документи прийняли Канада і Велика Британія: Канада – «Стратегію кібербезпеки в Канаді», Велика Британія – «Стратегію кібербезпеки у Великій Британії: захист та представництво Великої Британії в цифровому світі». З огляду на те, що законодавство в галузі міжнародної кібербезпеки досі не розроблено, у Талліннському керівництві передбачені правила та дії, яких держави мають дотримуватися і виконувати у процесі ведення кібератак на їхній території або території інших держав. Оновлену версію Талліннського керівництва розроблено у 2017 р. У ньому набули закріплення 154 правила проведення кібероперацій, зокрема тих, що дозволяють державам вести самооборону, а також подано правовий аналіз найпоширеніших випадків

кіберінцидентів, з якими зіштовхуються держави. Документ також містить усі напрацювання міжнародного права стосовно кібероперацій, починаючи від правових режимів мирного часу і до збройних конфліктів. Крім цього, у ньому зібрано широкий спектр принципів міжнародного права і режимів, за допомогою яких урегульовуються інциденти в кіберпросторі, інформаційно розвинені держави розробляють й ухвалюють стратегічні документи, спрямовані на забезпечення кібербезпеки, визначення підстав і правил реагування на кіберінциденти та проведень кібероперацій.

Іноді (особливо в РФ) [379] право на застосування фізичної сили у відповідь на кібернапади розцінюється як сукупність рекомендацій щодо ведення кібервійни. Це не відповідає дійсності.

По-перше, Талліннське керівництво не є офіційним документом ні центру CCD COE, ні НАТО, ні країн, що є членами НАТО. Це лише приватна думка учасників робочої групи, яка і підготувала Талліннське керівництво. Та й із самим керівництвом пов’язано чимало міфів. Часто можна почути, наприклад, що Талліннське керівництво дозволяє фізичне усунення хакерів, які ведуть військові дії в кіберпросторі. Це не зовсім так. Група експертів взагалі чітко не визначилася, чи вважати тих чи інших осіб учасниками кіберконфліктів. Наприклад, якщо хтось напише шкідливу програму, яку згодом використають у кібервійні, то чи буде автор такої програми учасником кібервійни. При цьому автори чітко зафіксували у ст. 33 правило, відоме багатьом російським правознавцям: «*будь-які сумніви у винуватості особи мають трактуватися на користь підозрюваного*". У Талліннському керівництві йдеться, що "*в разі виникнення сумнівів щодо того, чи є особа цивільною, ця особа вважається цивільною*».

Автори документа зробили такі ключові висновки:

– Держави відповідальні за кібероперації проти інших держав, що ведуться з їхньої території, навіть якщо такі операції ведуть не спецслужби, але при цьому держава дає «хліб і дах» тим, хто атакує інші країни. Якщо який-небудь державний чиновник, наприклад, звертається до хакерів із закликом

про допомогу у проведенні кібероперацій проти інших держав, то держава, що закликає, буде нести весь тягар відповідальності за наслідки, як ніби сама вона здійснювала такі дії. До речі, зазначений висновок одразу спростовує всі доводи експертів, які вважають, що Талліннське керівництво написано НАТО (читай США) для виправдання своїх дій у кіберпросторі. Адже саме керівництво Агентства національної безпеки (АНБ) закликало американських хакерів допомогти Батьківщині;

– проти незаконних кібероперацій держави мають право застосовувати різні контрзаходи. При цьому зазначені контрзаходи можуть бути визнані незаконними, але тільки не у випадку дій у відповідь (тут їхнє застосування вважають виправданим);

– заборона на застосування сили, зокрема і сили в кіберпросторі. Експерти все ж не дають чіткої відповіді, що є застосуванням кіберсил, але сходяться в тому, що це, як мінімум, має супроводжуватися завданням шкоди окремим особам або навіть пошкодженням тих чи інших об'єктів. При цьому застосуванням сили не вважають дії, що викликають роздратування або незручність у певній іншій країні;

– держава – жертва «збройного нападу» в кіберпросторі, що спричинив людські втрати або іншу серйозну шкоду, вправі відповісти за допомогою сили в кіберпросторі або фізичному світі;

– застосування контрзаходів допустиме щодо кібертерористів, зокрема на території іноземних держав;

– збройні конфлікти, що перейшли у воєнні злочини, зумовлюють кримінальну відповідальність для тих осіб, які керують кіберопераціями, що є частиною збройного конфлікту;

– цілком прийнятно відносити збройні конфлікти, що повністю ведуться в кіберпросторі, до міжнародного поняття «збройний конфлікт» зі свого боку, застосовувати норми міжнародного гуманітарного права;

– кібероперації, спрямовані проти цивільних об’єктів та осіб, що не призводять до завдання шкоди життю та здоров’ю, не заборонені міжнародним

гуманітарним правом. При цьому заборонено використовувати кібероперації для того, щоб сіяти паніку серед населення (прикладом цьому є, на нашу думку, недавній злом Twitter'a Associated Press);

– кібератаки мають спрямовуватися лише проти конкретних цілей та об’єктів. «Віялові» атаки, які можуть зачепити цивільних, повинні бути забороненими;

– керівництво кібероперацій, що призвели до жертв серед цивільного населення (або можуть спричинити таку шкоду), класифікують як воєнні злочини;

– об’єкти, необхідні для виживання цивільного населення (лікувальні установи, об'єкти ЖКГ, продовольчі магазини), а також служителі церкви і медичний персонал підпадають під міжнародне гуманітарне право і проти них не мають бути спрямовані кібероперації (навіть випадково).

В Україні з метою запобігання кібернападам в Інтернеті на базі СБУ створено структуру, цілями якої є запобігання, виявлення та ліквідація комп’ютерних атак і наслідків шкідливого інформаційного впливу на інформаційні ресурси, розміщені на території нашої країни.

Отже, викладене вказує на те, що і в Україні, і за кордоном уживаються заходи із забезпечення кібербезпеки, але багато що ще слід зробити. В Україні вимагають негайного вирішення питання, що стосуються:

– взаємодії органів державної влади, що забезпечують урегулювання інформаційних конфліктів;

– організації та побудови системної інформаційної діяльності на міжнародному, регіональному та внутрішньодержавному рівнях.

Насамперед це має забезпечити можливість висвітлення державної позиції щодо подій, які відбуваються, у світовому інформаційному просторі в режимі реального часу. Крім того, необхідно розробити стратегічний документ, у якому також мають бути передбачені підстави і вимоги здійснення кібероперацій і визначені державні органи, відповідальні за такі операції.

5.4. Нормативно-правове забезпечення окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки

Виконання основних завдань національної інформаційної політики відбувається шляхом здійснення різних керуючих впливів на головні об’єкти інформаційного середовища, об'єкти інформаційної політики тощо. Інформаційні ресурси й інформаційно-телекомунікаційна інфраструктура, інформаційні та телекомунікаційні технології, системи і засоби їхньої реалізації, споживання та виробництво засобів інформатизації, інформаційних продуктів і послуг є об’єктами інформаційної політики.

Прогресуючі нині кібертероризм та кіберзлочинність становлять особливу національну, суспільну та міжнародну небезпеку. З огляду на це особливої актуальності набуває проблема співвідношення політичних і силових засобів протидії цим загрозам. Запобігання несанкціонованому доступу до інформації обмеженого поширення, що має значення для забезпечення цілей колективної безпеки, також тісно пов’язане із зазначеним напрямом роботи. У сфері військово-технічної співпраці надзвичайно актуальними є питання захисту державних таємниць організації.

В Україні ефективність організаційних і правових заходів кіберзахисту критичної інфраструктури значно ускладнює відсутність ухвалення Закону «Про критичну інфраструктуру та її захист» [380]. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» критично важливі об’єкти інфраструктури (далі – об’єкти критичної інфраструктури) – «це підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості,

функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки й оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей».

У проєкті Закону «Про критичну інфраструктуру та її захист» критична інфраструктура – це сукупність об'єктів, що є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам.

З огляду на предмет нашого дослідження особливий науковий інтерес становлять питання захисту об'єктів критичної інформаційної інфраструктури, якими є технологічні або комунікаційні системи об'єкта критичної інфраструктури, кібератака на які безпосередньо вплине на його стійке та безпечне функціонування. У цьому контексті логічним було б надати визначення поняття «інформаційна інфраструктура України», однак такого поняття в чинному законодавстві немає.

На нашу думку, інформаційна інфраструктура України – це сукупність об'єктів інформатизації, інформаційних систем, мереж зв'язку і сайтів у мережі Інтернет, розміщених на території України, а також на територіях, що перебувають під юрисдикцією України або використовуваних на підставі міжнародних договорів України.

Дефініції зазначених вище понять дещо схожі між собою. Однак, з огляду на аналіз їхніх формулювань, можна зробити висновок, що критична інформаційна інфраструктура відрізняється від інформаційної інфраструктури наявністю автоматизованої системи управління суб'єктів критичної інформаційної інфраструктури і систем електронного зв'язку в ролі об'єктів критичної інформаційної інфраструктури.

Що стосується аналізу проекту закону України «Про критичну інфраструктуру та її захист», то натепер законопроект не містить переліку підстав віднесення організацій до суб'єктів критичної інформаційної

інфраструктури і як наслідок – інформаційно-телекомунікаційних мереж, інформаційних систем, та автоматизованих систем управління, що належать цим організаціям, до об'єктів критичної інформаційної інфраструктури. Така невизначеність гальмує ідентифікацію критичних інформаційних систем й ефективність забезпечення її безпеки.

У межах реформування СБ України з метою підвищення ефективності організаційного забезпечення кіберзахисту об’єктів критичної інфраструктури та критичної інформаційної інфраструктури пропонуємо серед її функціональних завдань передбачити такі заходи:

– здійснювати правове забезпечення діяльності національного координаційного центру кібербезпеки;

– вносити пропозиції про вдосконалення нормативно-правового забезпечення;

– оцінювати безпеку критичної інформаційної інфраструктури;

– координувати дії суб′єктів критичної інформаційної інфраструктури в напрямі обміну і надання інформації про комп′ютерні інциденти, щодо використання коштів, призначених для запобігання, виявлення і ліквідації наслідків комп'ютерних атак та реагування на комп′ютерні інциденти.

Усе ж нині слід визнати, що в Україні відбувається здійснення певних заходів із забезпечення кібербезпеки й активного формування системи правового забезпечення використання критичної інформаційної інфраструктури. Хоча, як видно з результатів аналізу нормативно-правового забезпечення необхідно насамперед, ухвалити базовий закон і доопрацювати положення кримінального законодавства щодо визначення відповідальності за завдання шкоди критичній інформаційній інфраструктурі.

Однією з найважливіших правових проблем, що також безпосередньо впливає на стан кібербезпеки і потребує свого вирішення на рівні держави, є правовий вимір відносин в Інтернеті. На цій практичній проблемі наголошує багато фахівців [381-384]. Інтернет, як людино-машинна взаємодія, демонструє появу об’єктів і суб’єктів, нових видів відносин, сприяє розвитку

суспільства і виявляє проблемні ділянки правового забезпечення. У цій галузі існує низка питань, що потребують відповіді та врегулювання, серед яких, наприклад, такі:

– які технологічні особливості впливають на регулювання відносин, що виникають у глобальному середовищі;

– у чому саме полягають особливості інтернет-відносин і чи є відмінності між відносинами, що виникають у віртуальному і реальному середовищах;

– чи можна стверджувати, що технології визначають вибір можливих методів правового забезпечення;

– чи можна обмежитися для забезпечення інтернет-відносин тільки правовими нормами, або необхідно застосовувати комплексний підхід, що передбачає облік й орієнтацію на технологічні норми та принципи.

Світова спільнота упродовж тривалого часу обговорює проблеми регулювання зазначених відносин і не може виробити єдиної позиції. Незважаючи на уявну віртуальність Інтернету, відносини в інтернет-середовищі є абсолютно реальними, оскільки в мережі обертається інформація реального світу. З технологічного погляду Інтернет – система величезної кількості мережевих протоколів у безлічі локальних мереж, а із соціального – Інтернет є засобом комунікації користувачів, що перебувають під дією різних державних юрисдикцій. Взаємодією величезної кількості централізованих окремих мереж, що створюють децентралізоване середовище зв’язку і комунікації, забезпечується функціонування мережі. Отже, головна особливість Інтернету – це функціонування не на географічному (територіальному), а на логічному рівні.

Можна окреслити перелік проблем, пов’язаних із регулюванням інтернет-відносин: визначення національної юрисдикції, території, об’єктного і суб’єктного складу суспільних відносин, технологічної сумісності, анонімності тощо. Вивчення особливостей технологічного функціонування Інтернету дозволяє дати відповідь на запитання про територіальність й

ефективність поширення державних законів на відносини, що формуються в окремій державній локальній мережі.

Пропонуємо розглянути особливості, що накладають технології на формування і регулювання інтернет-відносин. Необхідно насамперед узяти до уваги, що ознаки фізичної та юридичної особи, яка веде діяльність в Інтернет, відрізняються від ознак, зафіксованих у цивільному кодексі. У реальному середовищі, наприклад, фізичну особу ідентифікують за іменем, прізвищем та по батькові, у мережі – за логіном і паролем, IP-адресою того вузла мережі або технологічного обладнання, з яких фізична особа здійснює доступ в Інтернет.

IP є частиною протоколу TCP/IP, на якому працює Інтернет і IP-адреси пристрою або вузла мережі. IP-адреса – це унікальний ідентифікаційний номер, який розробник присвоює будь-якому пристрою. Якщо за допомогою пристрою відбувається вихід в Інтернет, то IP-адреси вузла мережі і пристрою взаємодіють і з'являється адреса того пристрою, з якого людина вийшла в мережу Інтернет. За допомогою IP-адреси відбувається взаємодія вузлів мережі в Інтернеті. Структура IP-адреси містить, серед іншого, й інформацію про параметри регіональної зони. Зазначені зони можуть належати будь-яким регіонах або державам, яким присвоєно код зони відповідно до міжнародної класифікації. Для систематизації і структуризації IP-адрес ведуть їхній реєстр. Кожен провайдер має свій діапазон IP-адрес. Для забезпечення взаємодії осіб, отримання IP-адреси та організації інтернет-відносин необхідна взаємодія провайдерів різних послуг, для чого слід дотриматися такого порядку дій. Internet Assigned Numbers Authority (IANA), що перебуває під контролем корпорації Internet Corporation for Assigned Names and Numbers (ICANN), має наділити повноваженнями щодо реєстрації провайдерів хостингу регіонального інтернет-реєстратора (Regional Internet Registry – RIR), що займається питаннями адресації та маршрутизації в Інтернеті. Провайдери хостингу мають зареєструватися в нього й отримати свій діапазон IP-адрес. Дрібніші провайдери доступу через послуги провайдерів хостингу надають вихід в Інтернет своїм користувачам (клієнтам) – юридичним і фізичним

особам. Провайдери хостингу передають їм для цього певний діапазон IP-адрес. З IP-адресою пов'язано доменне ім’я, що містить частину IP-адреси, пов'язаної із зоною хостингу, що дозволяє отримати детальнішу інформацію про місце виходу в мережу в будь-якому регіоні. Відповідно до встановленого порядку доменне ім’я реєструють на конкретну особу, завдяки чому можна визначити адміністратора доменного імені. Отже, належність до певного регіону в мережі визначається за зоною, що належить IP-адресі. З огляду на те, що мережа є транскордонною, має розмиті або неіснуючі межі, розуміння регіональної зони IP-адреси дозволяє визначити регіон учинення правопорушення з високою часткою вірогідності. Усе ж слід визнати, що питання визначення території в мережі і вибору права досі залишається дискусійним. Це обумовлено технологічними особливостями, внаслідок яких є можливість існування динамічних IP-адрес й анонімних доменних імен. Доменне ім’я – невід’ємна частина технології Інтернету і значна частина інтернет-адреси, використання якого також регламентовано протоколами, що визначають шлях пакетів в Інтернеті. Для з’ясування пристрою, наприклад, з якого відбувся вихід людини в мережу або місця вчинення юридично значущої дії, часто використовують доменне ім’я.

Проте для визначення місцезнаходження пристрою, з якого відбувся вихід у мережу, такий метод не ефективний, оскільки, по-перше, існують різні технології, що змінюють справжнє доменне ім’я і його зв’язок із територією певної держави. Ефективна система доменних імен успішно буде функціонувати тільки з погляду технології й управління. Однак з точки зору нормативного правового забезпечення такий метод не завжди спрацьовуватиме. По-друге, якщо пов’язувати доменне ім’я з територією і, відповідно, із законом держави, то для таких доменних розширень як .org, .com, .net й інші неможливо визначити право, що можна застосувати до відносин, які виникають у зазначених доменних зонах.

До того ж існують держави, які з метою подолання невизначеності у правовому забезпеченні інтернет-відносин прямо вимагають від усіх суб’єктів,

що ведуть діяльність в Інтернеті, перевести в національну інтернет-зону всі свої технології. Наприклад, в Указі Президента Республіки Білорусь від 4 лютого 2010 року № 60 «Про переведення всіх учасників інтернет-відносин в білоруську зону» [385] передбачено, що з 1 липня 2010 рок діяльність із реалізації товарів, виконання робіт, надання послуг на території Білорусі з використанням інформаційних систем, мереж і ресурсів, що мають підключення до Інтернету, здійснюється юридичними особами, їхніми представництвами та філіями, створеними відповідно до законодавства республіки, з місцезнаходженням у республіці, а також індивідуальними підприємцями, зареєстрованими в Білорусі, з використанням інформаційних систем, мереж і ресурсів національного сегменту мережі «Інтернет», розміщених на території республіки і зареєстрованих у встановленому порядку.

Комп'ютерні технології поширюють цифровий контент і така реплікація визначена протоколами Інтернет для функціонування та взаємодії всіх її технологічних складових, копії інформації при виконанні стандартних операцій створюються комп'ютерними технологіями автоматично. Звісно, у зв'язку із цим з'являються проблеми забезпечення довіри до інтернет-середовища, пов'язані з недостатньою інформацією, одержуваною користувачами Інтернету стосовно запобігання несанкціонованому доступу, щодо принципів регулювання тощо. Дедалі активніше висловлюється позиція, що в інтернет-середовищі найефективнішим регулятором буде саморегулювання – це одна з наявних у правових межах можливість, що дозволяє забезпечити кібербезпеку, спрямовану на розробку і реалізацію захисних політик і технологій. Наприклад, часто лунає думка про те, що відкриті мережі зможуть забезпечити надання на створення інфраструктури більш інформаційно безпечних послуг і за нижчими витратами, ніж закриті мережі.

Однак слід наголосити, що необхідно розробляти механізми правоохоронної діяльності для забезпечення реакції держави на

правопорушення, що здійснюються, оскільки орієнтація на саморегулювання не вирішить усі правові проблеми.

Проте визначення застосовного права в Інтернеті пов'язане з розробленими нормами правового забезпечення, орієнтованими на технології, за допомогою яких можна втілити в життя вимогу закону. Отже, інтернет-простір вимагає враховувати специфіку технологій, на базі яких формуються інтернет-відносини, а не тільки змінює фізичні аспекти традиційних методів комунікації. Оцінка правопорушень здійснюється відповідно до закону країни, на території якої сталося порушення. У зв'язку з цим необхідно підкреслити, що, крім поданих прикладів визначення території за доменним іменем, використовують також прив'язку за громадянством особи, яка вчинила правопорушення. Крім того, учені висловлюють думку про можливу персональну юрисдикцію, засновану тільки на прив'язці до «національності» інтернет-сайту [386]. Забезпечення захисту інтернет-користувачів від довільних дій третіх осіб і покладання обов'язків із забезпечення технологічного обмеження виникнення можливих правопорушень провайдерами хостингу, а також організація їхньої взаємодії з органами, що забезпечують контроль і нагляд у цій сфері, – мета інтернет-регулювання. Для досягнення зазначеної мети інтернет-спільнота розробляє відкриті стандарти, які дозволяють забезпечити відкриту функціональну сумісність технологій, що використовують в Інтернеті. Відкриті стандарти можуть бути реалізовані як апаратні і програмні продукти, що визначають технологічну політику, управління технічною передачею інформації, протоколи сумісності. Якщо розглядати структуру Інтернету як складну багаторівневу, багатофункціональну транскордонну структуру, що охоплює різні національні сегменти, комутація та передача інформації за якими можлива різними способами, то можна помітити, що роль національних інтернет-сегментів у функціонуванні мережі є другорядною. Її загальне технологічне функціонування не залежить від функціонування будь-якого національного інтернет-сегмента. У випадку відключення національного інтернет-сегмента

постраждає тільки ця національна мережа, оскільки вона не зможе взаємодіяти з іншими національними мережами. Населення цієї держави опиниться в ізоляції від глобальних мережевих відносин і різних послуг, що здійснюються за допомогою глобальної мережі. Однак за таким принципом побудовані не всі національні інтернет-мережі. Китайський Інтернет, наприклад, спочатку створювався таким чином, що відключення від глобальної мережі не повинно було вплинути на його функціонування. Зазвичай національні інтернет-мережі пов’язані між собою і розміщення інформації в одній національній мережі дозволяє отримати до неї доступ з іншої. З огляду на це дії суб'єкта в одному національному сегменті мережі пов’язані з інтересами інших держав. Тобто дозволені дії відповідно до законодавства однієї держави (наприклад, розміщення формули слабких наркотичних речовин) на території іншої держави можуть спричинити юридичні наслідки.

Визначення території, на якій скоєно юридичну дію, є однією з важливих проблем у сфері інтернет-відносин. Від її розв’язання залежить, право якої держави може бути застосовано для регулювання відносин, що виникли. Незважаючи на транскордонність Інтернету, юридичні дії вчиняються на певній національній території мережі, і визначення інтернет-зони має важливе значення для правового забезпечення, вона утворює простір, у межах якого держава реалізовує свою владу.

Однак, слід наголосити, що розвиток технологій і їхнє застосування щодо вирішення питань правового забезпечення в зазначеній сфері тривають. Держави почали активно впроваджувати технології оброблення інформації різного роду (наприклад, технології хмарних обчислень, Інтернет речей, великих даних), що складаються з апаратно-програмного комплексу. Світовою практикою визнано регламентування державами інформаційних відносин у суспільстві, використання ними інформаційних технологій і засобів для досягнення різних цілей. Простежується тенденція, що держава в особі уповноважених органів визначає напрями діяльності державних інформаційних структур, цілі та завдання інформаційного обміну. Водночас

вважається, що лише міркування національної безпеки є єдиним розумним обмежувачем доступу до інформації. Інформаційне суспільство не може бути побудоване без вирішення проблеми безпеки і довіри у використанні ІКТ. У своїй Резолюції № A/64/211 [387] 2010 року Генеральна Асамблея ООН зазначає про необхідність формувати, розвивати, заохочувати культуру кібербезпеки та посилювати державну співпрацю, визначаючи її основні напрями. Щоб уряди на рівних засадах могли відігравати свою роль і виконувати свої зобов'язання – у розв'язанні питань міжнародної державної політики, які стосуються Інтернету, а не у площині повсякденної діяльності технічного й експлуатаційного характеру, що не впливає на питання міжнародної державної політики. Для таких цілей національні зусилля мають підкріплюватися взаємодією на міжнародному рівні й обміном інформацією, з тим, щоб можна було ефективно протистояти зазначеним загрозам, що дедалі більше набувають транснаціонального характеру.

Відповідаючи на запитання про можливості правового забезпечення відносин, що виникають у сфері ІКТ, слід ураховувати технологічну специфіку, що дозволить розробити відповідні правила і норми, які мають потенційну вагу і реально відображають можливість і порядок регулювання відносин, що виникають в ІКТ.

Прикладом технологій, застосовуваних для ухиляння від дотримання вимог щодо ідентифікації, можуть бути анонімні протоколи, що називаються «tor» (the Onion Router), або анонімні мережі [388]. У 1995 році Міністерством військово-морських досліджень США було розроблено Концепцію цибулевої маршрутизації, у 1997 році до проєкту приєдналося Управління перспективних дослідницьких проектів Міністерства оборони США (Defense Advanced Research Projects Agency). До анонімних мереж належать комп'ютерні мережі, що створені для обходу вимоги ідентифікації користувача в Інтернеті і працюють у глобальній мережі як надбудова. Першою такою мережею була Freedom, що функціонувала з 1998 р. по 2001 р. У ній використовували криптографічний протокол, завдяки чому треті особи

не могли ідентифікувати повідомлення, що приходили для користувачів зазначеної мережі. Одночасно почали активно впроваджувати інші проекти, що отримали назву «цибульні». За такими технологічними моделями було розроблено протокол «tor», на базі якого функціонує «tor-мережа». Нині для забезпечення анонімності учасників мережі активно використовують tor-мережі [389-390].

За даними японського поліцейського агентства, безпосередньо пов'язаними з анонімністю є функціонування фальшивих онлайн-торгів та інші кіберзлочини [391]. Китай, наприклад, відкрито пригнічує «tor-мережі», у цій країні заборонено використання протоколу tor, у зв’язку з чим доступ до вхідних вузлів tor блокується. Так само діють Об'єднані Арабські Емірати, Саудівська Аравія й Ірак. Агентство національної безпеки США повідомило, що регулярно застосовує атаки проти осіб, які використовують протокол tor [392], і збирає трафік від деяких вузлів tor-мережі. Як засвідчує низка джерел, це агентство також відстежує користувачів, які шукають або завантажують програму tor, чи подають запит на інформацію про мости tor по електронній пошті [393]. У США розроблено систему аналізу статистичної інформації щодо кількості та частоти використання «tor-мереж» й обсягу запитів до неї, а також керівництво для практиків стосовно спрощення процедури створення універсальної системи відстеження та підвищення прозорості Інтернету. Конвенцію про злочинність у сфері комп’ютерної інформації застосовують у Великій Британії. У ст. 32, що регламентує транскордонний доступ до даних, які зберігаються на комп’ютері, зазначено, що: «Сторона може без згоди іншої Сторони:

a) отримувати доступ до загальнодоступних (відкритого джерела) комп'ютерних даних незалежно від їхнього географічного розташування;

b) отримувати через комп'ютерну систему на своїй території доступ до комп’ютерних даних, що зберігаються на території іншої Договірної Сторони, або отримувати їх, якщо ця Сторона має законну і добровільну згоду особи, яка має законні повноваження розкривати ці дані такій Стороні через таку

комп’ютерну систему».

Англійські дослідники дотримуються такої думки: якщо tor – це послуга, що вільно доступна для громадськості і програмне забезпечення розроблене на основі відкритого коду, то положення ст. 32 Конвенції має поширюватися і на цю технологію для збирання доказів. Однак при цьому висловлюється й інша позиція, прибічники якої стверджують: те, що певна інформація публічно доступна, зовсім не передбачає відсутність обмежень на її оброблення [394].

У контексті зазначеного слід додати, що відповідно до ст. 177 Цивільного кодексу України об’єктом цивільних прав є інформація, тому її можна розглядати як докази. Проте з огляду на цю ситуацію доцільно розробити вимоги до:

– проведення оперативно-розшукової діяльності з використанням потокових даних і забезпечення їхнього збереження;

– збирання в режимі реального часу даних про потоки інформації в комп'ютерних системах;

– порядку проведення обшуку і вилучення комп’ютерних даних, що зберігаються;

– визначення змісту інформації.

Водночас необхідно переглянути повноваження органів державної виконавчої влади зі збирання доказів в Інтернеті.

Прикладом такого підходу є КПК Естонії [395], де зазначено: якщо для збору доказів використовують інформаційну технологію з відкритим вихідним кодом, тоді до відома сторін, що застосовують такий пристрій, заздалегідь доводять інформацію про можливе збирання органами правопорядку інформації в цій технології і заздалегідь роз’яснюються мету використання таких технологій. Такі пропозиції можуть викликати питання, що стосуються дотримання принципів збирання цифрових доказів, особливо коли це роблять з використанням Інтернету, tor- і торрент-мереж або інших технологій, що ускладнюють ідентифікацію інформації й осіб. Збирання інформації в Інтернеті пов’язане з іще однією дуже важливою проблемою щодо місця

інформації як доказу.

Федеральна асоціація інформаційних технологій, телекомунікацій і нових засобів інформації ФРН (BITKOM) рекомендує з великою обережністю користуватися будь-якими безкоштовними додатками, що дозволяють застосовувати аудіо- і відеоматеріали [396]. У ФРН боротьба з порушеннями прав правовласників розпочалася з посилення Закону про авторське право [397] у 2008 році. Тепер вважають злочином не тільки відтворення фільмів і музики з мережі, копіювання дисків в обхід захисту, але і несумлінне розміщення посилань на інтернет-ресурси. Крім того, заборонені запис і зберігання записів передач загальнодоступних і платних телеканалів. Уряд ФРН радить обережно розміщувати музику на персональних веб-сторінках й у блогах, для цих дій користувач має придбати права на її використання в Gema [398].

Отже, складності правового забезпечення в інтернет-середовищі, проаналізовані вище, обумовлені технологічними особливостями мережі. Відповідно, будь-яке правове регламентування відносин у зазначеній сфері має здійснюватися з описом технологічних методів, використання яких уможливить досягнення необхідного правового результату.

Державний суверенітет визначається сукупністю зовнішнього і внутрішнього суверенітетів. Стратегічними завданнями реалізації національних інтересів і пріоритетів України в зовнішньополітичній діяльності є забезпечення безпеки суверенітету і територіальної цілісності держави. Інформаційно-комунікаційні технології випробовують державний суверенітет на міцність, розхитуючи межі інформаційного простору держави. Транскордонний характер Інтернету призвів до проблеми визначення юрисдикції держави в мережі. На порядку денному постала проблема забезпечення державного суверенітету в кіберпросторі. Річ у тім, що міжнародно-правові механізми, які дозволяли б відстоювати суверенне право держав на регулювання інформаційного простору, зокрема в національному сегменті мережі «Інтернет», не визначені. Більшість держав змушена поспіхом

адаптувати державне забезпечення галузі інформації та інформаційних технологій до нових обставин уже в процесі виконання завдань із захисту інформаційного простору від недружніх дій.

У зв'язку із цим закономірно постає запитання про те, наскільки територіальна концепція суверенітету реалізується в галузі цифрового державного управління. При дослідженні зазначеного питання доходимо висновку про можливе розширення та переосмислення змісту поняття «територія держави» поняттям «кіберпростір», оскільки кіберпростір також є сферою здійснення економічних, політичних і соціальних відносин.

Отже, цифровий суверенітет має спиратися на цифрову територію, що, як вважається у галузі кіберпростору, реалізувати неможливо. З огляду на це слід виокремити інші нетериторіальні ознаки визначення юрисдикції держави в кіберпросторі.

Зважаючи на транстериторіальність Інтернету і його правовий режим, необхідно виділити інші, цифрові, ознаки цифрового суверенітету держави. У такому контексті проявляється підхід, прийнятий у міжнародному праві, коли під територією розуміють весь простір планети Землі і щодо кожної конкретної території встановлено свій міжнародний режим. Наприклад, до «територій з міжнародним режимом належить відкрите море, простір над ним і морське дно за межами континентального шельфу держав. Крім того, міжнародний режим може встановлюватися щодо окремих територій або їх частин відповідно до міжнародних договорів» [399].

Регламентуванню інтернет-відносин сприятиме розроблення спеціального правового режиму [400], за прикладом регулювання космосу, Антарктики або інших територій, підпорядкованих міжнародному праву. Однак на Інтернет поширити міжнародний режим неможливо, оскільки дві третини кореневих серверів Інтернету розміщені на території США й управління Інтернетом, фактично, здійснюється однією державою. Нині середовище ІКТ є юридичною фікцією, яка полягає в тому, що відповідну сукупність технічних й організаційних засобів розглядають як складову

території держави. Об’єднавши суб'єктів різних держав, інтернет-відносини вже не обмежуються територією однієї держави і мають глобальний характер. Глобального характеру набули і негативні впливи – ризики та небезпеки від технічних і технологічних помилок, закладених у комп’ютерних системах, що збільшують кримінальні можливості інформаційного впливу на свідомість людини шляхом маніпулювання нею. Торкнулися зміни і станів держав. Тепер держави можуть існувати лише в активній взаємодії з міжнародною системою, їм доводиться спільно вирішувати і міжнародні проблеми, і виконувати завдання, які держави ще вчора розглядали як суто внутрішні. Дедалі більша кількість громадських відносин виходить за межі державних кордонів. У посланні Генерального секретаря ООН з нагоди всесвітнього дня телекомунікації та інформаційного суспільства від 17 травня 2010 року наголошується, що нині телекомунікація є чимось більшим, ніж просто базовою послугою: вона є засобом, що сприяє розвитку, порятунку життя людей і поліпшенню суспільства. Її роль ще більше посилиться в майбутньому [401].

Усі країни світу постали перед необхідністю розв’язання проблеми забезпечення цифрового суверенітету і «цифрової незалежності». Ефективне виконання державою своїх функцій, таких як регулювання надання послуг в електронному вигляді, забезпечення захищеності громадян від шкідливого інформаційного впливу залежить від використання інформаційних технологій. Деякі вчені дотримуються думки, що держави вже позбулися своїх суверенних повноважень у законодавчій, судовій та правовій системах з огляду на інформаційну глобалізацію. Держави до виникнення та розвитку глобальної мережі передавали наднаціональним органам частину свого суверенітету, а з появою глобального віртуального світу у держав забирають частину їхніх функцій організації, що діють у мережі. Це надає підстави для припущення про втрату державами суверенної ідентичності. Втрата ідентичності виражається в тому, що держави розпадаються на окремі інститути й соціально-політичні групи, а вертикальні і горизонтальні мережі втягують їх у

себе, «освоюють» по частинах, руйнуючи звичні перегородки між внутрішньою та зовнішньою політикою. На думку деяких дослідників, такі зміни призводять до відмирання державних інститутів та зміни природи держави. Створення міжнародних судів, що привнесли у світову політику ідеї міжнародної спільноти і міжнародної відповідальності, стало першим кроком до обмеження суверенітету держав. Взаємодія держав має форму взаємопроникнення, що виражається у створенні «наддержавних мережевих інститутів». Унаслідок цього державні інститути «розчиняються» в різних інтернаціональних мережах і ведуть свою діяльність автономно від «власної» держави. Завдяки розвитку перспектив, що надаються мережевим середовищем, зберігається можливість втілення політичної стратегії та застосування контрольних дій з боку міжнародних і національних органів щодо ринкових господарств з тим, щоб реалізувати соціальні цілі.

Отже, можна зробити висновок, що ІКТ-середовище впливає на:

– сукупність застосовуваних правових і технічних норм для врегулювання спорів, встановлення юрисдикції в Інтернеті, зокрема зв’язку юрисдикції і географічного положення розшукуваного суб'єкта;

– з’ясування фізичного місця розташування користувачів Інтернету, процедури встановлення контролю над діями суб'єктів у мережі і за її межами, зокрема над владою держави зі встановлення контролю над онлайн-поведінкою;

– визначення законності регулювання інтернет-відносин.

ІКТ і їхній розвиток надають нові значні можливості для забезпечення суспільних відносин, впливають на процес регулювання цих відносин і на роль у світовій взаємодії кожної держави. Інформація стає механізмом, що впливає на суспільство і стає керуючою системою, оскільки саме вона формує відносини всередині суспільства. У здійсненні правового забезпечення відносин в інформаційному просторі територіальна ознака стає все менш значущою, а технологічна ознака, навпаки, набуває дедалі більшої ваги.

Висновки до розділу 5

Серед пріоритетних напрямів наукового пошуку цього розділу передбачалося визначити концептуальні засади правового забезпечення кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, дослідити міжнародні аспекти кібербезпеки України, розробити пріоритети розвитку правових основ державної політики України у сфері кібербезпеки, обґрунтувати шляхи вдосконалення правового забезпечення окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки. За результатами реалізації означених завдань отримано такі основні висновки:

1. Підтверджено, що беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх здобутків нашої держави на цьому шляхи слід вважати надання у червні 2020 року Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти так званих секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв'язку, управління військами, конкретних родів військ тощо). Крім того, EOP дає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО.

2. Констатовано, що нині майже всі підходи, що покликані забезпечити кібербезпеку України, орієнтовані на військово-політичні процеси. Безумовно, це пріоритетний напрям у забезпеченні національної безпеки України, поряд із врахуванням проблем регіональної політичної нестабільність, незаконного обігу наркотиків, злочинності, захисту інформаційних прав людини тощо. Та й імідж держави залишається ще одним проблемним аспектом, що прямо залежить від її інформаційної політики. Нерідко нас сприймають як зручний полігон кіберзлочинності. Отже, глобалізація кіберпростору породила таке

явище, як всеосяжний взаємообмін інформацією на загальносвітовому рівні.

3. Розроблено чотири основні складові національних інтересів України у кібернетичній сфері: *перша* – забезпечення дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереженню та зміцненню моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни. *Друга* – передбачає інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів. *Третя* забезпечує застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів. *Четвертий компонент* національних інтересів України в кібернетичній сфері передбачає захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України.

4. Констатовано, що кожне інформаційне протистояння на світовій арені має цілком визначену мету. Водночас результати їх аналізу дали змогу виявити цілі загальнішого характеру, що властиві глобальному інформаційному суперництву в нинішніх умовах. До них належить: забезпечення національної безпеки держави у глобальному кіберпросторі; просування і захист національних інтересів в інформаційній сфері; забезпечення кібербезпеки як важливої складової системи національної безпеки; посилення міжнародної кібербезпеки шляхом зменшення у глобальному кібернетичному просторі можливостей для ворожого

використання інформаційно-комунікаційних технологій.

Для досягнення зазначених цілей у процесі глобального інформаційного протистояння використовують відповідні методи і способи боротьби, серед яких: інформаційне домінування або досягнення переваги в кіберпросторі; інформаційна асиметрія як базовий принцип інформаційного впливу, що використовується як відповідь на зовнішній вплив, так і при здійсненні впливу на іншу сторону інформаційного суперництва; зовнішній контроль кіберпростору держави та управління інформаційними процесами, що здійснюється з іноземних центрів; інформаційне стримування як спосіб управління кризовими ситуаціями в зонах конфліктів; кіберагресія, в основі якої лежить незаконне здійснення однією державою інформаційного впливу на кіберпростір іншої держави, що завдає шкоди її суверенітету, життєдіяльності в різних сферах та політичній незалежності; кібервійна, що є найбільш гострою формою інформаційного протистояння між державами, здійснюваного насильницькими засобами і способами впливу на інформаційну сферу супротивника з метою досягнення стратегічних завдань. Нині сутність кібервійни полягає у прихованому управлінні економічними, політичними, військовими й іншими процесами держави-супротивника.

5. Встановлено, що увага міжнародного співтовариства має бути зосереджена на забезпеченні кібербезпеки у сфері інформаційних технологій, оскільки більшість відносин базується на цифрових транскордонних технологіях. Урегулювання зазначених проблем у галузі права дозволяє сформувати правову систему кібербезпеки суб’єктів, зокрема захистити від деструктивної інформації, що впливає на них. Запропоновано комплексну нормативно-організаційну модель, що передбачає: створення системи сертифікації інформаційних технологій, що використовуються на території України, і посилення сертифікаційних випробувань; визначення нових вимог до забезпечення довіри до розроблюваних апаратно-програмних комплексів; підтримку стійкості системи протягом усього життєвого циклу інформаційної інфраструктури й усунення вразливостей, що дозволить реалізувати напрями

стратегічного цифрового розвитку України.

6. Розроблено конкретні заходи, які доцільно реалізувати міжнародним співтовариством на глобальному рівні для посилення кібербезпеки:

1) розроблення і впровадження правових повноважень, юрисдикційних правил та інших процедурних положень для забезпечення ефективного розслідування злочинів, скоєних за допомогою ІКТ, зокрема: коригування норм збирання, зберігання, засвідчення і використання у кримінальному розслідуванні електронних доказів; ухвалення положень, що регулюють проведення внутрішніх і міжнародних обшуків; розроблення положень, що стосуються міжнародних та національних відстежень повідомлень; ухвалення положень, що стосуються перехоплення повідомлень, переданих через комп'ютерні мережі й аналогічні засоби масової інформації тощо;

2) для подолання розриву між швидкістю, з якою працюють кіберзлочинці, і темпами реагування правоохоронних органів, розширити міжнародну співпрацю між правоохоронними органами, прокуратурою та судовими органами, а також інтернет-провайдерами;

3) реалізація за умови наявності ресурсів міжнародних проектів технічної взаємодії та допомоги, які могли б об'єднати експертів у галузі законодавства, запобігання злочинності, судового переслідування, комп'ютерної безпеки, методів розслідування і суміжних питань з державами, що потребують інформації або допомоги в цих сферах;

4) розроблення освітньої програми, що сприятиме підвищенню рівня знань та поінформованості про протидію кіберзлочинності.

7. Встановлено, що в широкому розумінні, з погляду інформаційного права, під інформаційною зброєю розуміють інформаційні технології, засоби і методи, призначені для ведення інформаційної війни. Запропоновано визначення включити до основних термінів, що містяться в законі України «Про основні засади забезпечення кібербезпеки України» і доповнити ст. 14 згаданого закону таким змістом: «*основною загрозою в галузі міжнародної інформаційної безпеки є використання інформаційно-комунікаційних*

технологій для вчинення різних протиправних дій, зокрема і як інформаційну зброю у військово-політичних цілях. Умови, що створюють можливості протидії загрозам використання ІКТ, належать до основних напрямів державної політики».

8. Визначено інформаційну інфраструктуру України як сукупність об’єктів інформатизації, інформаційних систем, мереж зв’язку і сайтів у мережі Інтернет, розміщених на території України, а також на територіях, що перебувають під юрисдикцією України або використовуваних на підставі міжнародних договорів України. Обґрунтовано доцільність законодавчого закріплення терміна «критична інформаційна інфраструктура», яка відрізняється від інформаційної інфраструктури наявністю автоматизованої системи управління суб’єктів критичної інформаційної інфраструктури і систем електронного зв'язку в ролі об’єктів критичної інформаційної інфраструктури.

9. Констатовано, що забезпечення кібербезпеки критичної інформаційної інфраструктури можливе, насамперед, шляхом визначення її об’єктів, розв’язання проблеми кібербезпеки об'єктів із значним життєвим циклом, розробки методики модернізації критичної інформаційної інфраструктури для кожної організації, інформаційні структури та технології якої є об'єктами критичної інформаційної інфраструктури. Крім того, необхідно систематизувати акти Уряду України й органів виконавчої влади, виявивши положення, які не відповідають забезпеченню кібербезпеки інформаційних технологій у міжвідомчій взаємодії, а також уточнити визначення понять «інформаційна система» й «інформаційно-телекомунікаційна мережа». Для забезпечення кібербезпеки використовуваних і створюваних інформаційних інфраструктур доцільно впровадити в українське законодавство термін «кібербезпека», оскільки з його допомогою можна точніше охарактеризувати відносини в галузі забезпечення безпеки ІКТ. Інформаційна безпека охоплює ширше коло відносин, зокрема безпеку комп’ютерних технологій, інформації та інформаційних відносин зі

створення, поводження, прийому, передачі, поширення інформації. З метою забезпечення кібербезпеки необхідно надати правову оцінку діяльності віртуальних й анонімних спільнот. Їхнє функціонування має схожі риси із функціонуванням адміністративно-територіальних утворень, але здійснюється в Інтернеті. Адміністрування діяльності зазначених спільнот можливе в межах інформаційної технології, на базі якої вони об’єднані. Крім того, з огляду на те, що термін «територія» не може бути застосований для характеристики інтернет-відносин, назріло визначення правового терміна «транскордонний простір». А віртуальні спільноти вважаємо за можливе визнати «адміністративно транснаціональними утвореннями».

Основні результати розділу відображено в наукових працях автора [402-407].

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та вирішено актуальну наукову проблему формування теоретичної моделі стратегії забезпечення кібернетичної безпеки України та розробки теоретико-правових засад механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Положення дисертації можуть стати теоретичними орієнтирами для удосконалення нормотворчої та правозастосовної практики забезпечення кібербезпеки України, розвитку інформаційного права та юридичної науки. Отримані в ході дослідження результати дають підстави стверджувати про досягнення поставленої мети і реалізацію визначених завдань та сформулювати такі основні висновки:

1. Спираючись на отримані результати дослідження генезису правового регулювання кібербезпеки людини, суспільства й держави у роботі запропоновано авторське трактування терміна «*культура кібербезпеки*». Під цим терміном ми розуміємо систему переконань, уявлень та етичних норм щодо ведення інформаційної діяльності у кіберпросторі, знань, умінь і навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності в кіберпросторі.

«Глобальну культуру кібербезпеки», зі свого боку, у роботі розглянуто як наднаціональну масову культуру кібербезпеки людини, суспільства, держави.

Водночас доведено, що основною *метою формування глобальної культури кібербезпеки* є досягнення такого стану соціальної взаємодії між суб'єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів

кіберпростору.

2. На основі понятійно-категоріального аналізу правового регулювання кібербезпеки України з'ясовано, що термін «кібербезпека» – похідний від родового терміна «безпека», відтак «кібербезпека» є частиною загальнішого поняття «безпека», що вирізняється специфічними особливостями, й одночасно має бути результатом синтезу поняття «безпека» та прикметника «кібернетична» (скороч. – «кібер»).

Базовою категорією у дослідженні кібербезпеки є категорія «безпека». В основу авторського підходу до сутності категорії «кібербезпека» покладено наукові уявлення видатних учених сучасності, зокрема О. Довганя, В. Пилипчука, О. Баранова, І. Коржа, які поняття «кібербезпека» розглядають у соціальному розумінні «безпеки», що означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних і потенційних загроз або уникнути їх, що, з іншого боку, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їхній розвиток. Зазначений підхід у дисертації взятий як базовий у дослідженні змісту кібербезпеки.

На цій теоретичній основі удосконалено такі категорії:

– «*кібербезпеку»* визначено як безпечність об'єктів кіберпростору й захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, у процесі чого забезпечено розвиток інформаційного суспільства, розвиток кіберкультури людини, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз безпеці України у кіберпросторі, а також постійний процес попередження й протидії відповідним загрозам;

– *«забезпечення кібербезпеки»* – це діяльність відповідних суб'єктів із досягнення такого стану захищеності життєво важливих інтересів людини і

громадянина, суспільства та держави під час використання кіберпростору, що унеможливлює його порушення;

– *кіберзагрози* – це такі явища, дії, чинники й умови, що становлять небезпеку для життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, яка полягає в можливості порушення властивостей одного чи декількох із зазначених складників;

– *кібератака* – це дії з метою порушення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Обґрунтовано гіпотезу, що сучасний рівень розвитку інформаційної сфери зумовлює потребу у перспективі виокремлення кібернетичної безпеки в самостійного виду безпеки, що дасть змогу, ураховуючи особливості відповідних систем і процесів управління, реалізувати правові, організаційні й технічні можливості захисних заходів. Це також передбачає підвищення вимог до захисту згаданих систем і процесів залежно від їхнього призначення, рівня, складу тощо.

3. Доведено, що кібернетична безпека – це також сукупність умов, які у фізичному, емоційно-психічному, духовно-освітньому, професійному, фінансовому, політичному й інших аспектах гарантовано забезпечують захищеність усіх компонентів інформаційних систем від якомога більшої кількості загроз і негативних впливів у кіберпросторі або ж від руйнівних наслідків у разі похибок, нещасних випадків, псування, аварій та іншої шкоди в цій сфері.

Аргументовано, що до предмета вивчення безпекової науки стосовно кіберсередовища належать: природні, соціально-економічні, соціально-політичні та техногенні процеси в контексті їхнього розвитку, взаємодії й утворення нових об’єктів і явищ, та їхніх елементів з навколишнім середовищем задля виявлення існуючих і потенційних небезпек, оцінювання відповідних ризиків та розробки адекватних методів і способів протидії, а також розробки належної нормативної бази для належної правової

регламентації вимог, методик, механізмів, алгоритмів, застосування яких гарантує досягнення мети захищеності інтересів людини, суспільства й держави від наявних і можливих загроз.

4. На основі теоретичного аналізу співвідношення кібербезпеки й інформаційної безпеки розроблено логічну схему підпорядкованості різного роду безпек, зокрема кібербезпеку визначено нами як складову частину інформаційної безпеки. Кібербезпека формується в реляційних відносинах із безпекою мереж, безпекою інтернету і безпекою додатків, а також здійснює підтримку безпеки критичної інформаційної інфраструктури у частині, що її стосується; кіберзлочинність і безпечну діяльність у кіберпросторі (насамперед дітей і молоді в інтернеті). Кіберзлочинність має вплив на інформаційну безпеку та, відповідно, кібернетичну безпеку. Безпечну діяльність у кіберпросторі визначається певним орієнтиром ідеальної поведінки.

У поняття «кібербезпека» входить широкий спектр практичних прийомів, інструментів і концепцій, тісно пов’язаних із технологіями інформаційної та операційної безпеки. Відмітна риса кібербезпеки полягає в тому, що вона передбачає використання інформаційних технологій в наступальних цілях для атак противника. Запропоновано, що кібербезпека повинна охоплювати не тільки заходи оборони та контрзахисту, а й наступу. Що стосується сучасного стану кібербезпеки України – її пріоритетним напрямом мають стати заходи активної оборони. Термін кібербезпека слід використовувати тільки для позначення практичних методів забезпечення безпеки, що поєднують у собі заходи наступального й оборонного характеру, які є сукупністю або системою інформаційних технологій, або ґрунтуються на них.

5. На основі аналізу базових категорій, що наведені в Законі України «Про основні засади забезпечення кібербезпеки України», виявлено низку невідповідностей, а також протиріч базисних категорій кібербезпеки. На цій основі обґрунтовано пропозиції визначити на законодавчому рівні такі

поняття:

– «*стан захищеності*», яке є системоутворюючим до категорії «безпека» та її еквівалентом. Запропоновано під цим терміном розуміти наявність параметрів, відповідно до яких об'єкти кібербезпеки перебувають під захистом. Основними параметрами визначено дотримання прав особи в кіберпросторі, реалізація національних інтересів в інформаційній сфері, здатність суб'єктів забезпечення кібербезпеки діяти і застосовувати засоби для усунення або зниження рівня небезпеки для об'єктів кібербезпеки та кіберзахисту;

– запропоновано у визначенні терміна «*кіберзлочин*» словосполучення «міжнародними договорами» замінити словосполученням «міжнародним правом». Зазначений підхід забезпечить єдність термінологічного тлумачення на рівні національного законодавства та міжнародного права;

– обґрунтовано, що законодавче визначення терміна «кіберзагроза» не співвідноситься за обсягом інформації, наведеної в терміні «кібербезпека», та не відповідає визначенню цього терміна. Адже кіберзагроза – це також злочинний акт, метою якого є пошкодження, викрадення цінних даних, доступ до несанкціонованих файлів або порушення цифрового життя загалом. Під кіберзагрозою слід також розуміти тактику, техніку та процедуру, що використовується під час кібератаки.

6. Досліджуючи систему суб'єктів забезпечення кібербезпеки України, запропоновано розглядати таку систему як органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб'єктів, що беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки. У цьому контексті важливе значення має розвиток державно-приватного партнерства, яке може мати різні форми: обмін інформацією, консультації, експертизи, сприяння в захисті інформації з обмеженим доступом тощо. Першочерговим завданням сьогодення є розробка оптимальних механізмів співпраці між приватним сектором і державними

органами у сфері забезпечення кібербезпеки України.

7. На основі системного підходу удосконалено критерії класифікації кіберзагроз в Україні, зокрема виокремлено нові критерії класифікації: загрози існуванню нації, за деструктивним впливом на основні сегменти національного кіберпростору, за посяганням на національні цінності кібербезпеки (життєво важливі інтереси людини і громадянина, суспільства та держави).

8. З огляду на аналіз правового регулювання кібербезпеки у зарубіжних країнах, запропоновано доповнити Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 р. № 242/2016 у частині вдосконалення основних завдань органу. У цьому контексті пропонуємо розширити п. 3 зазначеного положення, додавши до основних завдань центру такі: упровадження в Україні стандартів безпеки мережевих й інформаційних систем; визначення критеріїв, за якими буде складатися перелік операторів базових послуг і провайдерів цифрових послуг; контроль за дотриманням мережевої нейтральності та міжнародних і європейських стандартів і заборон уведення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами; аудит системи мережевої й інформаційної безпеки; організація та підтримка системи сповіщення про кіберінциденти, системи аудиту й упровадження заходів мережевої та інформаційної безпеки; забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема щодо персональних даних і захисту комерційних інтересів операторів та провайдерів.

9. У межах дослідження правових засад кібербезпеки людини *інформаційну дієздатність,* як складову інформаційної правосуб’єктності, визначено як спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав, брати на себе певні правові обов’язки, а також нести юридичну відповідальність у разі неправомірної поведінки.

10. На основі теоретичного аналізу правової природи відносин у процесі забезпечення кібернетичної безпеки людини комплексно досліджено усі її складові – суб'єкт (людина у глобальному інформаційному просторі, яка потребує належного правового регулювання своєї безпеки при користуванні кібернетичним простором), об'єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов'язків усіх учасників зазначених суспільних відносин).

Удосконалено зміст поняття «кібернетична безпека людини», яке запропоновано розуміти як стан її захищеності, що визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.

Наголошено, що найбільш уразливим суб'єктом інформаційних правовідносин є людина. Зумовлено це постійним виникненням нових викликів і загроз інформаційній безпеці особи, пов'язаних із недосконалістю інформаційно-телекомунікаційних технологій, інформаційно-психологічними впливами, використанням інформації для досягнення геополітичних, терористичних та інших протиправних, руйнівних цілей. Отже, в умовах глобального інформаційного суспільства особистість у процесі задоволення своїх потреб найбільш яскраво виявляє свою соціальну складову, і, з огляду на нові безпекові виклики й загрози, змушена на основі культури інформаційної безпеки виробляти відповідні заходи протидії.

Визначено декілька основних критеріїв класифікації загроз кібербезпеці людини. Зокрема: за впливом на національну свідомість; за посяганням на національні цінності; за природою виникнення.

11. Усебічне дослідження новітніх викликів і загроз кібербезпеки в глобальному інформаційному суспільстві, а також небезпечних тенденцій у цій сфері дало змогу виокремити критерії їх можливої класифікації: джерело загрози (виклику), залежність від джерела загрози, розташування джерела загрози стосовно об'єкта, характер впливу. На цій основі, з метою

вдосконалення вітчизняної системи правового забезпечення кібернетичної безпеки людини, запропоновано авторську класифікацію видів відповідних викликів і загроз. Зокрема, з огляду на значущість соціальних мереж, визначено джерела загроз в інтернеті, а саме: сайти, що становлять небезпеку для особистості (мають на меті вплив на свідомість індивіда, рекламовані задля отримання зиску та ін.); спам, тотальне розсилання реклами й іншої інформації без бажання користувача тощо.

Крім того, вивчення сучасних інформаційно-телекомунікаційних технологій дало змогу виявити специфічну групу загроз, пов'язаних із цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin та ін.), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie тощо).

12. Запропоновано теоретичну модель Концепції кібернетичної безпеки людини, а також потребу долучення до її складу документів стратегічного планування України. Подано пропозиції зі структурно-змістовного наповнення зазначеної концепції, зокрема її головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення інформаційної безпеки особи. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави в цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість концепції.

Визначено, що доцільність розробки Концепції кібернетичної безпеки людини зумовлена необхідністю вдосконалення національного законодавства про кібернетичну безпеку в сенсі закріплення поняття «кібернетична безпека людини», правового регулювання кібернетичної безпеки людини, формування системи забезпечення безпеки особи в інформаційній сфері як сукупності відповідних сил і засобів.

13. Зазначено, що недосконалість вітчизняного інформаційного законодавства, неузгодженість системи міжнародної кібербезпеки, брак

дійового інструментарію протидії викликам і загрозам в інформаційному (кібернетичному) просторі залишаються основними чинниками, які, з огляду на динаміку відповідних правопорушень, а також викликів і загроз, що негативно впливають на головного суб'єкта інформаційних відносин – людину, здійснюють значний вплив на характер цих відносин у суспільстві.

14. Теоретичний аналіз основних концепцій інформаційного суспільства дозволив з'ясувати, що реальні загрози глобальному інформаційному суспільству на сучасному етапі сконцентровані в таких сферах: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо. На цій основі обґрунтовується висновок, що успішне розв'язання зазначених глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об'єднаних зусиль усього світового співтовариства.

15. Досліджуючи роль правового чинника в запобіганні кіберзагрозам сучасному українському суспільству, доведено необхідність створення оптимального співвідношення між правом особи на захист від зловживань її персональними даними й іншою конфіденційною інформацією і небезпекою несанкціонованого доступу до неї. Такий підхід визначається важливим аспектом інформаційної політики всіх держав у сучасних умовах.

На сучасному етапі розвитку суспільство потребує (у межах прийнятої моделі кібернетичної безпеки) розроблення державної соціальної стратегії застосування інформаційних технологій і використання кіберпростору, що вказувала б на головні пріоритети прогресивного розвитку суспільства і закладала базис для створення механізму координування соціальних норм. На цій основі правове забезпечення кібернетичного середовища розглянуто і як об'єкт морально-правового регулювання. Сутність останнього полягає в налагодженні суспільних відносин, урегулювання яких базується на нормах права та моралі.

16. Доведено та науково обґрунтовано, що важливим елементом забезпечення кібернетичної безпеки України на сучасному етапі державотворення має стати освітня і просвітницька діяльність за активного й дієвого державного сприяння. Для продуктивної інформаційної взаємодії конче потрібна належна освіченість користувачів та їхня поінформованість щодо відповідних прав й обов'язків. Провідною ідеєю сучасної інформаційно-технологічної освіти є гуманізм, усвідомлення того, що головна мета розвитку суспільства – людина, її фізичне, інтелектуальне, духовне і психологічне зростання, яке визначає її потреби, пріоритети, інтереси й, урешті-решт, сенс життя.

17. Концептуальними засадами правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів визначено: розвиток державно-приватного партнерства у сфері взаємодії державних органів із громадськими організаціями та громадянами з метою забезпечення кібербезпеки України; інформаційно-просвітницьку, ідеологічну й освітню роботу із протидії радикальній ідеології та екстремізму; удосконалення нормативно-правового забезпечення протидії використанню інтернету в терористичних й екстремістських цілях, а також забезпечення національних інтересів суверенної України в інформаційній сфері; розвиток міжнародного чинника з метою утвердження України як повноправного учасника глобальних інформаційних процесів заради подальшої інтеграції в НАТО та поліпшення іміджу нашої держави серед міжнародних партнерів; створення, розвиток і забезпечення безпеки національних інформаційних ресурсів; практичну реалізацію на рівні законодавчого забезпечення національних інтересів України в кіберсфері.

18. З урахуванням міжнародного досвіду та на основі аналізу національної практики запропоновано основні складові національних інтересів України в кіберсфері: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних

цінностей суспільства, традицій гуманізму та патріотизму, наукового і культурного потенціалу країни; 2) інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України.

19. Щодо пріоритетів розвитку правових основ державної політики України у сфері кібербезпеки та правового регулювання окремих елементів інформаційної інфраструктури акцентовано увагу, що в Україні досі не ухвалений Закон «Про критичну інфраструктуру і її захист», не розроблені норми кіберзахисту, рекомендації щодо їхньої реалізації, методики контролю за їхнім дотриманням для недержавного сектора, хоча варто визнати, що уповноваженими державними органами України робота в цьому напрямі ведеться.

Обґрунтовано доцільність прискорення процесу прийняття ініційованого Національною поліцією України і СБ України спільно розробленого законопроекту про внесення змін і доповнень до Кримінального процесуального кодексу України в частині, що стосується цифрових доказів.

Доведено позицію стосовно необхідності додати до основних термінів, що містяться в законі України «Про основні засади забезпечення кібербезпеки України», поняття «інформаційної зброї». У широкому розумінні, з погляду інформаційного права, під інформаційною зброєю пропонуємо розуміти

інформаційні технології, засоби і методи, призначені для ведення інформаційної війни. Також обґрунтовано необхідність доповнити згаданий закон текстом такого змісту: «*основною загрозою в галузі міжнародної інформаційної безпеки є використання інформаційно-комунікаційних технологій для вчинення різних протиправних дій, зокрема і як інформаційну зброю у військово-політичних цілях. Умови, що створюють можливості протидії загрозам використання ІКТ, належать до основних напрямів державної політики*».

На основі аналізу основних підходів державної політики з реформування СБ України, доведено, що з метою підвищення ефективності організаційного забезпечення кіберзахисту об’єктів критичної інфраструктури та критичної інформаційної інфраструктури серед функціональних завдань СБ України необхідно передбачити такі заходи: здійснювати правове регулювання діяльності національного координаційного центру кібербезпеки; вносити пропозиції про вдосконалення нормативно-правового забезпечення; оцінювати безпеку критичної інформаційної інфраструктури; координувати дії суб’єктів критичної інформаційної інфраструктури в напрямі обміну і надання інформації про комп’ютерні інциденти, щодо використання коштів, призначених для запобігання, виявлення і ліквідації наслідків комп’ютерних атак та реагування на комп’ютерні інциденти.

20. Запропоновано такі перспективні напрями подальших наукових пошуків: дослідження у сфері оцінювання загроз кібернетичній безпеці України; визначення місця кібернетичної безпеки України в системі чинників національної безпеки; дослідження основних завдань кібернетичної безпеки України і напрямів її функціонування; розробки критеріїв оцінки негативного впливу на кібернетичну безпеку України; дослідження складових ІТ-права та його місця в національній і міжнародній системі права; обґрунтування правових основ функціонування штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. 10 років потому: що потрібно знати про п’ятиденну війну Росії та Грузії. Новини та аналітика про Німеччину, Україну та Європу. DW. URL: https://www.dw.com/uk/10 (дата звернення 10.02.2021).

2. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : Монографія. К. : ТОВ «*Видавничий дім «АртЕк*», 2018. 422 с.

3. Що таке RFID-технології, особливості і переваги їх застосування. *Вікна*. 04.02.2020р. URL: http://vikna.if.ua/cikavo/102674/view (дата звернення 04.02.2021).

4. Абетка медіа / За загал. ред. В. Ф. Іванов; Переклад з нім. В. Климченка. Київ: *Академія української преси*, Центр вільної преси, 2015. 177 с.

5. Бєляков К. І., Онопрієнко С. Г., Шоміна І. М. Інформаційна культура в Україні: правовий вимір : монографія: за заг. ред. К. І. Бєлякова. К. : КВІЦ, 2018. 169 с.

6. Новицька Н. Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності : дис. … канд. юрид. наук : 12.00.07.. Ірпінь, 2007. 210 с.

7. Довгань О. Д. Щодо деяких правових аспектів культури кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. IX Всеукр. наук.-практ. конф. К., 2018. С. 60-62.

8. Мельник С. В. Формування культури кібербезпеки : особистісний, корпоративний, державний та глобальний вимір. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. IX Всеукр. наук.-практ. конф. К., 2018. С. 115-118

9. Report The European Union Agency for Network and Information Security (ENISA) Cyber Security Culture in organisations. URL:

https://www.enisa.europa.eu/publications/cybersecurity-culture-in-organisations (дата звернення 04.01.2021).

10. Попович М. В. Культура в розмаїтості понять, явищ і схем поступу. *Енциклопедія історії України* : у 10 т. / редкол.: В. А. Смолій (голова) та ін.; Інститут історії України. НАН України. К. : Наук. думка, 2009. Т. 5 : Кон - Кю. 560 с.

11. Довгань О. Д. Литвинова Л. А. Щодо деяких змін до дослідницької культури і практики: перспективи відкритого доступу до знань. *Актуальні проблеми управління інформаційною безпекою держави* : Матеріали наук.-практ. конф. К., 2019. С. 175-179

12. Cybersecurity Research Directions for the EU's Digital Strategic Autonomy. EU Agency for Cybersecurity (ENISA) URL: https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy (дата звернення 04.02.2021).

13. Creation of a global culture of cybersecurity : resolution / adopted by the General Assembly. URL: https://digitallibrary.un.org/record/482184 (дата звернення 04.02.2021).

14. Дюльгер М. І. Інформаційна безпека на морі в контексті загальної безпеки мореплавства. *Інтернет речей: проблеми правового регулювання та впровадження* : Матеріали другої наук.-практ. конф., 29 лист. 2018 р., м. Київ / Упоряд. : В. М. Фурашев, С. О. Дорогих. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. 168 с.

15. Советский энциклопедический словарь / гл. ред. А.М. Прохоров. 3-е изд. М.: Сов. энцикл., 1985. 1632 с.

16. Капто А.С. Кибервойна: генезис и доктринальне очертания. URL: https://elibrary.ru/item.asp?id=19124172 (дата звернення 04.02.2021).

17. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2. С. 54-62

18. Логінова Н. І. Правові основи кібербезпеки в Україні. Правові та інституційні механізми забезпечення розвитку держави та прав в умовах

євроінтеграції: матеріали міжнар. наук.-практ. конференції. Одеса: 2016. Т. 1. С. 575-577

19. Ліпкан В., Діордіца І. Національна система кібербезпека як складові частина системи забезпечення національної. *Підприємництво, господарство і право.* 2017. № 5. С. 174-180

20. Тонконогов А. В. Кибернетическая безопасность: понятие и сущность феномена. *Право и кибербезопасность*. 2013. №2. С.36-43

21. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162-169

22. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 1. С. 312-320 с.

23. Діордіца І. В. Поняття та зміст національної системи кібербезпеки. URL: http://goal-int.org/ponyattya-ta-zmist-nacionalnoi-sistemi-kiberbezpeki/ (дата звернення 03.12.2020).

24. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К. : ДУТ, 2015. 288 с.

25. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. *Аспекти публічного правління*. Том 6 № 8 2018. С.49-55

26. P. W. Singer, Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Published in the United States of America by Oxford University Press 198 Madison Avenue, New York, NY 10016. 2014. 321 p.

27. Лук'янчук Р. В. Державне управління у сфері забезпечення кібербезпеки України: дис. … к.ю.н, 25.00.01. К. 2017. URL: http://instzak.rada.gov.ua/ uploads/documents/31444.pdf (дата звернення 04.02.2021).

28. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України": Указ Президента України від 26 травня 2015 р. № 287. URL: https://www.president.gov.ua/documents/2872015-19070 (дата звернення 03.12.2020).

29. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України": Указ Президента України від 24 вересня 2015 р. URL: https://zakon.rada.gov.ua/laws/show/555/2015 (дата звернення 03.12.2020).

30. Корж І.Ф. Безпека: методологічні підходи до поняття. JURNALUL JURIDIC NAȚIONAL: TEORIE ȘI PRACTICĂ. Серпень 2019 С. 68-72

31. ISACA, Глосарій з кібербезпеки, 2014 р.: URL: http://www.isaca.org/KnowledgeCenter/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf (дата звернення 03.12.2020).

32. ISACA Трансформація кібербезпеки. США. 2013 р., с. 11: www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx (дата звернення 03.12.2020).

33. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 04.02.2021).

34. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д.ю.н.: 12.00.07. Ужгород, 2019. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/19617 (дата звернення 03.12.2020).

35. Безкоровайный М. М. Татузов А. Л. Кибербезопасность - подходы к определению понятия. *Вопросы кибербезопасности.* 2014. №1(2). С. 22-27

36. Большая Советская Энциклопедия. Изд. 3-е. М.: «Советская Энциклопедия», 1973. Т.12, 624 с.

37. Klimburg A. et al. National cyber security framework manual //NATO CCD COE Publications (December 2012). URL: http://belfercenter.hks.harvard.edu/fi les/hathaway-klimburg-nato-manualch-1.pdf (дата звернення 03.12.2020).

38. Безкоровайный М. М., Татузов А. Л. Подходы к математическому моделированию в области кибербезопасности. *Информатизация и связь.* 2012. №. 8. С. 21-27

39. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року: URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення 03.12.2020).

40. National Cyber Security Strategy URL: https://www.enisa.europa.eu/topics/nationalcybersecuritystrategies/ncssmap/NCSS2Engelseversie.pdf (дата звернення 03.12.2020).

41. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (дата звернення 03.12.2020).

42. Присяжнюк М. М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 42-46

43. Конституція України: Основний Закон України від 28.06.1996 № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення 03.12.2020).

44. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. *Науково-технічний збірник*. К., 2004. С. 30-33

45. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263 (дата звернення 03.12.2020).

46. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. URL: http://zakon4.rada.gov.ua/laws/show/998_163 (дата звернення 03.12.2020).

47. National Cyber Security Action Plan (2019-2024). Public Safety Canada 2019. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx (дата звернення 03.12.2020).

48. The Department Of Defense Cyber Strategy URL: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата звернення 02.02.2021).

49. Ткачук Т. Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України «Київський політехнічний інститут». Політологія. Соціологія. Право*. 2017. № 1–2. С. 242–246

50. Ткачук Т. Ю. Кібербезпека: підходи до визначення в окремих країнах. Актуальні проблеми управління інформ. безпекою держави : мат. наук.-практ. конф. (Київ, НА СБ України. 24.05.17). 2017. С. 142–144

51. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» від 25.02.2017 № 47/2017: URL: www.president.gov.ua/documents/472017-21374 (дата звернення 03.12.2020).

52. Довгань О. Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: філософсько-правові та прикладні аспекти: матеріали круглого столу, 12 травня 2017 р., м. Вінниця / упоряд.: О. Д. Довгань, М. В. Беланюк, С. А. Лапшин, О. Г. Радзієвська, О. І. Яременко; Вінницький державний педагогічний університет ім. М. Коцюбинського. Київ : Видавничий дім «АртЕк», 2017. С. 31-39

53. Довгань О. Д. Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. №1. С. 86-100

54. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія; НАПрН України, НДІІП. К.: Видавничий дім «АртЕк». 2017. 107с.

55. Брижко В. М. Філософія права: герменевтика в сфері інформаційного права. *Правова інформатика*. 2014. № 1(41). С. 18-22

56. Ланде Д. В., Фурашев В. М. Основи інформаційного і соціально-правового моделювання: Монографія. Київ : ТОВ "ПанТот", 2012. 144 с.

57. Hacktivist («хакер» +«активіст») – активний член хакерської групи: Звіт про тенденції та ризики інформаційної безпеки за підсумками першого півріччя 2011 року IBMX-Force URL: http://www.ibm.com/news/ru/ru/2011/09/29/q138278b96341x82.html (дата звернення 03.12.2020).

58. Хатамле Омар Що відбувається у світі? Електронний ресурс «На часі» URL: https://nachasi.com/2017/09/08/omar-hatamle/ (дата звернення 03.12.2020).

59. Кириченко М.О. The impact of digital technologies on the development of human and social capital in the conditions of the digitalized society. *Humanities Studies*. 2019. Випуск 1 (78). С. 108-129

60. Систематизація і розвиток теоретичних основ трансформації інформаційних відносин на шляху до кіберцивілізації : наук. доп. Фурашев В. М., Петряєв С. Ю., Поперечнюк В. М. К.: ФСП НТУУ «КПІ», 2016. 55 с.

61. Hartley R.V.L. Transmission of Information. *Bell System Technical Journa*l. 1928. № 7. P. 335–363

62. Shannon C. E. A Mathematical Theory of Communication. *Bell System Technical Journal*. 1948. Vol. 27. P. 379-423

63. Stonier T. Towards a new theory of information. *First Published.* October 1, 1991. URL: https://journals.sagepub.com/doi/10.1177/016555159101700501 (дата звернення 03.12.2020).

64. Information Technology Laboratory /Applied Cybersecurity Division. An official website of the United States government. URL: https://www.nist.gov/itl/applied-cybersecurity (дата звернення 03.12.2020).

65. Довгань О. Д., Тарасюк А. В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

66. Довгань О. Д., Тарасюк А. В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності *Інформація і право*. 2018. № 2 (25). С. 51–61.

67. Тарасюк А. В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. 4(31)/2019. С. 73–82.

68. Тарасюк А. В. Досвід забезпечення кібербезпеки у зарубіжних країнах. *Науковий вісник публічного та приватного права* : зб. наук. праць. 2019. № 4. С. 204–209

69. Тарасюк А. В. Актуальні питання протидії кіберзлочинності в сучасних умовах. Досудове розслідування: актуальні проблеми та шляхи їх вирішення : мат. постійно діючого наук.-практ. Семінару. м. Харків, 26 жовт. 2018 р. 2018. С. 251-254.

70. Тарасюк А. В. Кібербезпека – один із важливих напрямків захисту держави. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.-практ. семінару, м. Харків, 23 трав. 2019 р. / редкол.: С. О. Гриненко (голов. ред.) та ін. Х. : Право, 2019. Вип. 10. С. 44-47.

71. Тарасюк А. В. Законодавчі підходи до кібернетичної безпеки України. Актуальні проблеми правових наук в євроінтеграційному вимірі зб. мат. Міжнародної наук.-практ. конф. м. Харків, 20-21 груд. 2019 р. 2020 р. С. 87-91

72. Єсімов С., Скриньковський Р., Ковалів М., Крет І. Правові аспекти формування системи безпеки об'єктів критично важливої інформаційної інфраструктури в Україні. *Traektoriâ Nauki = Path of Science. Section "Law"*. 2018. Vol. 4, No 7. С. 2001-2008

73. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. Київ : Едельвейс, 2014. 433 с.

74. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html (дата звернення 03.12.2020).

75. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 03.12.2020).

76. NIS Directive. URL: h https://digital-strategy.ec.europa.eu/en/policies/nis-directive (дата звернення 03.12.2020).

77. Трофіменко О. Г. Кібербезпека України: аналіз сучасного стану / О. Г. Трофіменко, Ю. В. Прокоп, Н. І. Логінова, О. В. Задерейко // Захист інформації. Том 21. 2019. № 3. С. 150-157

78. Стратегія кібербезпеки України: Указ Президента України № 96/ 2016 від 15.03.2016. URL: http://zakon4.rada.gov.ua/laws/show/96/2016 (дата звернення 03.12.2020).

79. Яцишин М.Ю. Проблеми та перспективи розвитку міжнародно-правового співробітництва у боротьбі з кіберзлочинністю. *Порівняльно-аналітичне право*. №5. 2018 URL: https://journals.indexcopernicus.com/api/file/viewByFileId/766964.pdf (дата звернення 03.12.2020).

80. Стратегія національної безпеки України: Указ Президента України № 287 від 26.05.2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#n14 (дата звернення 03.12.2020).

81. Ткачук Н.А. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право.* № 1(28)/2019. С.129-134

82. Ткачук Т. Ю., Довгань О. Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. № 2 (25). С. 73–85

83. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право*. № 1(20)/2017. С. 104-111

84. Бакалінська О. Правове забезпечення кібербезпеки в Україні. *Під приємництво, господарство і право*. 2019. № 9. С. 100-108

85. Безпека в мережі: як Україна регулюватиме кіберпростір. URL: https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir (дата звернення 03.12.2020).

86. Кримінальний кодекс України від 5.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення 03.12.2020).

87. Про Службу безпеки України: Закон України від 25.03.1992. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення 03.12.2020).

88. Про оперативно-розшукову діяльність: Закон України від 18.02.1992. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення 03.12.2020).

89. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30.06.1993. URL: https://zakon.rada.gov.ua/laws/show/3341-12 (дата звернення 03.12.2020).

90. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006. URL: https://zakon.rada.gov.ua/laws/ show/3475-15 (дата звернення 03.12.2020).

91. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5.07.1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення 03.12.2020).

92. Про інформацію: Закон України від 2.10.1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення 03.12.2020).

93. Про телекомунікації: Закон України від 18.11.2003. URL: http://zakon4.rada.gov.ua/laws/show/1280-15 (дата звернення 03.12.2020).

94. Про державну таємницю: Закон України від 21.01.1994. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення 03.12.2020).

95. Про захист персональних даних: Закон України від 1.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення 03.12.2020).

96. Про електронні документи та електронний документообіг: Закон України від 22.05.2003. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення 03.12.2020).

97. Про затвердження Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України № 505/98 від 22.05.1998. URL: https://zakon.rada.gov.ua/laws/show/505/98 (дата звернення 03.12.2020).

98. Положення про технічний захист інформації в Україні: Указ Президента України № 1229/99 від 27.09.1999. URL: https://zakon.rada.gov.ua/laws/show/1229/99 (дата звернення 03.12.2020).

99. Положення про Національний координаційний центр кібербезпеки: Указ Президента України № 242/2016 від 7.06.2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016 (дата звернення 03.12.2020).

100. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури: Указ Президента України № 8/2017 від 16.01.2017. URL: https://zakon.rada.gov.ua/laws/show/8/2017 (дата звернення 03.12.2020).

101. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»: Указ Президента України № 32/2017 від 13.02.2017 року. URL: https://zakon.rada.gov.ua/laws/show/32/2017 (дата звернення 03.12.2020).

102. Про затвердження Стратегічного плану розвитку державного підприємства «Галузевий центр цифровізації та кібербезпеки» на 2020-2024 роки: наказ Міністерства інфраструктури України № 558 від 11.09.2020. URL: https://icdc.gov.ua/storage/app/sites/8/Docs/plany/plan-rozvitku-dp-gtstsk-11-09-2020.pdf (дата звернення 03.12.2020).

103. Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям: Постанова КМУ № 1519 від 11.10.2002. URL: https://zakon.rada.gov.ua/laws/show/1519-2002-%D0%BF (дата звернення 03.12.2020).

104. Деякі питання організації міжвідомчого обміну інформацією в Національній системі конфіденційного зв'язку: Постанова КМУ № 303 від 14.05.2015. URL: https://zakon.rada.gov.ua/laws/show/303-2015-%D0%BF (дата звернення 03.12.2020).

105. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова КМУ № 563 від 23.08.2016. URL: https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF (дата звернення 03.12.2020).

106. Концепція створення державної системи захисту критичної інфраструктури: Розпорядження КМУ № 1009 від 06.12.2017. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80 (дата звернення 03.12.2020).

107. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: Постанова КМУ № 518 від 19.06.2019. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%B (дата звернення 03.12.2020).

108. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні. 2019. 35 с.

109. Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: проект Закону України, реєстр. № 2043. URL: https://zakon.rada.gov.ua/laws/show/379-20 (дата звернення 03.12.2020).

110. Бойко В. О. Європейський досвід державно-приватного партнерства: підходи до формування та нормативно-правові засади. STRATEGIC PRIORITIES № 1. 49, 2019. С. 28-36

111. Савчук М. М. Захист інформаційних технологій та кібербезпека. Стенограма наукової доповіді на засіданні Президії НАН України 25 вересня 2019 року. Вісн. НАН України, 2019, № 11. С. 23-28

112. Office for the Deputy Director, Acquisition Career Management, 1996.ArmyRD&A., Томи 996 – 998

113. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. Женева: МСЕ, 2010. С. 55. URL: www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru; (дата звернення 07.12.2020).

114. ITU Global Cybersecurity Agenda. Framework for International Cooperationin Cybersecurity. URL: https://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf (дата звернення 03.12.2020).

115. International Strategy For Cyberspace: Prosperity, Security and Opennessin a Networked World. Washington DC:, May 2011. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf. (дата звернення 08.12.2020).

116. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: https://www.jcs.mil/Portals/36/Documents/ Doctrine/pubs/dictionary.pd (дата звернення 03.12.2020).

117. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова КМУ від 29 березня 2006 р. № 373 URL: https://www.kmu.gov.ua/npas/32791826 (дата звернення 03.12.2020).

118. Мельничук О. Управління критичною інфраструктурою держави: базові методи та критерії ідентифікації об'єктів. *Public Administration and Local Government, 2019, 3.* URL: http://www.dridu.dp.ua/zbirnik_dums2019_03(42)/4.pdf (дата звернення 03.12.2020).

119. Лісовська Ю. П. Концепція превентивних заходів у системі інформаційної безпеки України: адміністративно-правовий аспект. *Наукові праці МАУП*. Серія: Юридичні науки. 20171, 103–109

120. Директива 2002/21/ЄС Європейського Парламенту та Ради від 7 березня 2002 року про спільні правові рамки для електронних комунікаційних мереж та послуг (Рамкова директоива) URL: https://zakon.rada.gov.ua/laws/show/984_003-02 (дата звернення 03.12.2020).

121. Сучасна політична лексика : енц. словник-довідник. І. Я. Вдовичин та ін.; за наук. ред. Хоми Н. М. Львів : «Новий Світ-2000», 2015. 396 с.

122. Офіційний сайт Міністерства оборони України. URL:http://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html

123. Iran says Israel, exiled group killed scientist in complex operation. Fars. URL: https://news.yahoo.com/iran-lays-rest-nuclear-scientist-101617948.html? (дата звернення 03.12.2020).

124. ENISA – Європейське агентство з питань мережевої та інформаційної безпеки URL: http://www.enisa.europeu (дата звернення 03.12.2020).

125. Cybersecurity Strategy of the European Union: An Open, Safe and URL: http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf (дата звернення 03.12.2020).

126. Interview on the recently launched ENISA “Country Reports”. ENISA. URL: https://www.enisa.europa.eu/media/news-items/country-reports-interview (дата звернення 03.12.2020).

127. Strengthening trust and security. European Commission URL: https://ec.europa.eu/digital-single-market/en/policies/strengthening-trust-and-security (дата звернення 03.12.2020).

128. Цифровий порядок денний для Європи. URL: http://ec.europa.eu/digital-agenda/en/ (дата звернення 03.12.2020).

129. Спільне звернення до Європейського парламенту. Стратегія ЄС із кібербезпеки: відкритий, надійний і безпечний кіберпростір, Брюссель, 2.06.2013 р., с. 3: http://ec.europa.eu/information. (дата звернення 03.12.2020).

130. Спеціальний звіт із кібербезпеки Євробарометр 390, липень 2012 р., URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (дата звернення 03.12.2020).

131. Спеціальний звіт з кібербезпеки Євробарометр 404, листопад 2013 р., URL: http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

132. Європейський центр боротьби з кіберзлочинністю при ЄВРОПОЛі. URL: https://www.europol.europa.eu/ec3 (дата звернення 03.12.2020).

133. Документ ООН Комплексне дослідження кіберзлочинності, лютий 2013 р., URL: www.unodc.org/documents/organized-crime/ / CYBERCRIME_STUDY_210213.pdf (дата звернення 03.12.2020).

134. Кіберзлочинність виникла в Європі: статистика та звіт про тенденції, 4 серпня 2013 р., URL: http://www.pymnts.com/uncategorized/2013/cyber-crimeoriginates-in-europe-statistics-andtrends- report/ (дата звернення 03.12.2020).

135. Оцінка вартості витоку інформації: глобальний аналіз 2013, травень 2013 р., ТОВ «Інститут Понемона». URL: www.symantec.com/mktginfo/whitepaper/053013_ GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf (дата звернення 03.12.2020).

136. Аналітична записка за результатами дослідження Порушення інформаційної безпеки 2013, Міністерство підприємництва, інновацій і ремесел. URL: www. pwc.co.uk/assets/pdf/cyber-security-2013-exec-summary.pd

137. Дослідження команди реагування (CERT) на комп'ютерні надзвичайні ситуації. URL: www.cert.org/cybersecurity-engineering/publications/index.cfm (дата звернення 03.12.2020).

138. Баранов О. А., Інтернет речей (IoT) і блокчейн. *Інформація і право*. № 1(24)/2018. С. 59-71

139. Баранов О. А. «Інтернет речей» як правовий термін. *Юридична Україна*. № 5-6. 2016. С. 96-103

140. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання : монографія. Харків : Право, 2018. Т. 1 : Сфери застосування, ризики і бар'єри, проблеми правового регулювання. 2-ге вид. 2018. 342 с.

141. В Украине впервые вживили чип в руку человека. Корреспондент.net, 10.09 2016. URL: https://korrespondent.net/ukraine/3743253-

v-ukrayne-vpervye-vzhyvyly-chyp-v-ruku-cheloveka (дата звернення 03.12.2020).

142. xNT NFC Chip. URL: https://dangerousthings.com/product/xnt/ (дата звернення 03.12.2020).

143. Тімкін І. Ф., Новікова Н. Є. Структурно-функціональна характеристика системи забезпечення національної безпеки України. URL: er.nau.edu.ua

144. Гетьманчук М., Грищук В., Турчин Я. Політологія: навчальний посібник. К.: Знання, 2010. 415 с.

145. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України: дис. ... канд. юрид. наук: 12.00.07. Суми, 2018. 221 с.

146. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави: функціональний аналіз. *Jurnalul juridic national: teorie şi practică*. 2017. № 6. С. 42-46

147. Указ Президента України від 27 січня 2016 року «Про Стратегію кібербезпеки України». URL: https://zakon5.rada.gov.ua/laws/show/96/2016 (дата звернення 03.12.2020).

148. Закон України «Про національну поліцію». URL: https://zakon.rada.gov.ua/ laws/show/580-19 (дата звернення 03.12.2020).

149. Бурячок В. Л., Гнатюк С. О., Корченко О. Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. *Інформаційна безпека: виклики і загрози сучасност*і: зб. мат. наук.-практ. конф., 5 квітня 2013 року, К. : Наук.-вид. центр НА СБ України, 2013. 416 с.

150. Ковалев А. А., Балашов А. И., Международно-правовые аспекты политики Кибербезопасности некоторых европейских стран бывшего советского блока. *Вестник Поволжского института управления*. 2018. Том 18. № 5. С.105-114

151. СБУ посилює захист інформаційної безпеки підприємств енергетичної галузі України. СБУ. URL:

https://ssu.gov.ua/ua/news/1/category/2/view/5213#.1YMttXpZ.dpbs (дата звернення 03.12.2020).

152. Ситуаційний центр забезпечення кібербезпеки СБУ. URL: https://ssu.gov.ua/ua/pages/330 (дата звернення 03.12.2020).

153. Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242. URL: https://www.president.gov.ua/documents/ 272020-32041 (дата звернення 03.12.2020).

154. Проект Закону про внесення змін до Закону України Про Службу безпеки України щодо удосконалення організаційно-правових засад діяльності СБУ (реєстр.№ 3196). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347 (дата звернення 03.12.2020).

155. Українські правоохоронні органи посилюють співпрацю з бізнесом для ефективної протидії кіберзагрозам. URL: https://ssu.gov.ua/ua/news/1/category/301/view.dpbs (дата звернення 03.12.2020).

156. Cybersecurity Framework. URL: https://www.nist.gov/industry-impacts/cybersecurity-framework (дата звернення 03.01.2021).

157. Hipaa for dummies. Why was HIPAA Created? URL: https://www.hipaaguide.net/hipaa-for-dummies/ (дата звернення 17.01.2021).

158. Cybercrime Infographics: Illustrations Of The Past, Present, And Future Threats We Face. Sausalito, Calif. Mar. 24, 2020. URL: https://cybersecurityventures.com/cybercrime-infogr (дата звернення 17.01.2021).

159. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page. (дата звернення 17.01.2021).

160. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. URL: http://pircenter.org/media/content/files/13/148.pdf (дата звернення 17.01.2021).

161. Кибербезопасность объектов критической ядерной инфраструкутры. URL: http://pircenter.org/projects/46-cybersecurity-of-critical-nuclear-infrastructure (дата звернення 17.01.2021).

162. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України (аналітична доповідь). URL: http://old2.niss.gov.ua/content/articles/files/AD_Dubov_206x301_pp1-84_press-b44d7.pdf (дата звернення 17.01.2021).

163. Історія інтернету від ARPANET до сьогодні. URL: https://ucloud.ua/istoriya-internetu-vid-arpanet-doc (дата звернення 17.01.2021).

164. Ревенков П. В. Финансовый мониторинг в условиях интернет-платежей. М. : КноРус, 2016. С. 64-67

165. Ревенков П.В., Бердюгин А.А. ДБО: Интернет создает новых клиентов и расширяет профили рисков. *Банковское дело*. 2013. № 12. С. 64-67

166. Лямин Л.В. Противодействие компьютерным мошенничествам. *Внутренний контроль в кредитной организации*. 2013. № 3. С. 21-27

167. CYBER; Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02). URL: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (дата звернення 17.01.2021).

168. Slippery Slope. PAX. URL: https://www.paxforpeace.nl/publications/all-publicat (дата звернення 17.01.2021).

169. Скиннер К. Цифровой банк: как создать цифровой банк или стать им. М.: Манн, Иванов и Фербер, 2015. 320 с.

170. Крупенникова Л. Ш., Курбатов В. И. Виртуальная личность: Net-мышление, сетевой психотип, и Интернет-фобии. URL: https://cyberleninka.ru/article/n/virtualnaya-lichnost-net-myshlenie-setevoy-psihotip-i-internet-fobii/viewer (дата звернення 17.01.2021).

171. Ситнова И. В., Поляков А. А. Информационно-психодогическое воздействие как практика ведения войн четвертого поколения. URL: https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe-vozdeystvie-kak-praktika-vedeniya-voyn-chetvertogo-pokoleniya (дата звернення 17.01.2021).

172. United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009).

173. William A. Wulf and Anita K. Jones, “Reflections on Cybersecurity,” Science 326 (13 November 2009): 943-4.

174. Martin Charles Golumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law (New York: Springer, 2007).

175. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. United States Government Accountability Office. September 10, 2007. P. 12.

176. Wilshusen, Gregory C. Information Security: Cyber Threats and URL: http://www.gao.gov/assets/270/268137.pdf.

177. Vulnerabilities Place Federal Systems at Risk. Testimony Before the Subcommittee on Government Management.

178. Organization, and Procurement; House Committee on Oversight and Government Reform. United States Government Accountability. May 5, 2009. P. 3. URL: http://www.gao.gov/assets/130/122454.pdf (дата звернення 17.01.2021).

179. Terrorist use of the Internet: Information Operations in Cyberspace. March 8, 2011. P. 2

180. Хофман Л. Дж. Современные методы защиты информации: пер. с англ. Москва: Сов. Радио, 1980. 322 с.

181. Цензура (контроль) в интернете: опыт Китая. URL: http://www.tadviser.ru/index.php (дата звернення 17.01.2021).

182. Корсун К. Про «священну корову» української кібербезпеки: Наскільки дієва міжнародна кібер-допомога? URL: https://www.ukrinform.ua/rubric-technology/2567808-pro-svasennu-korovu-ukrainskoi-kiberbezpeki-naskilki-dieva-mizna.html (дата звернення 17.01.2021).

183. Kempf A. Considerations for NATO Strategy on Collective Cyber Defense. URL: http://csis.org/blog/considerations-nato-strategy-collective-cyberdefense (дата звернення 17.01.2021).

184. Резолюція 60/45, ухвалена Генеральною Асамблеєю Організації Об'єднаних Націй. Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки. URL: https://zakon.rada.gov.ua/laws/show/995_e45 (дата звернення 17.01.2021).

185. Господарик Ю.П., Пашковская М.В. Международная экономическая безопасность. М., 2016. 416 с.

186. Schreier F., Weekes B., Winkler T.H. Cybersecurity: The Road Ahead. Geneva Centre for the Democratic Control of Armed Forces (DCAF). DCAF Horizon 2015. Working Paper No. 4. URL: https://dcaf.ch/sites/default/files/publications/ documents/Cyber2.pdf (дата звернення 17.01.2021).

187. Камчатний М. В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій. URL: http://oaji.net/pdf.html?n=2016/3229-1477308.pdf (дата звернення 17.01.2021).

188. EU International Cyberspace Policy URL: http://www.eeas.europa.eu/policies/eu-cyberen.htm (дата звернення 17.01.2021).

189. Глобальный индекс кибербезопасности и профили по киберблагополучию: отчет. Женева, ABI Research, 2015. 516 с.

190. Software Management: Security Imperative, Business Opportunity. BSA URL: https://gss.bsa.org/ (дата звернення 17.01.2021).

191. InHope. URL: https://www.inhope.org (дата звернення 17.01.2021).

192. Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013). URL: https://www.cert.ro/vezi/document/strategia-de-secu (дата звернення 17.01.2021).

193. Ткачук Т. Ю., Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. № 4(23)/2017. С. 62-72

194. Countering cyberterrorism. URL: http://msz.gov.pl/en/foreign_policy/ security_policy/international_terrorism/countering (дата звернення 17.01.2021).

195. Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. 2017. № 4 (23). С. 62-72

196. Доктрина кибезбезопасности Польщи. URL: constitutions.ru/?p=11083 (дата звернення 17.01.2021).

197. Пантин В. И., Кардава Н. В. Кибербезопасность: проблемы формирования единой политики в Европейском Союзе. *Вестник Пермского университета. Политология.* 2018. №3. С.5-17

198. Елин В. М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: мон. М., 2016. 168 с

199. The National Cybersecurity Agency of France (ANSSI). URL: https://www.ssi.gouv.fr/en/ (дата звернення 17.01.2021).

200. Austrian Energy CERT (AEC) is the Computer Emergency Response Team (CERT). URL: https://cert.at/en/about-us/ (дата звернення 17.01.2021).

201. Austrian Security Strategy (2013). URL: https://www.bka.gv.at/DocView. axd?CobId=52251 (дата звернення 17.01.2021).

202. Austrian Cyber Security Strategy (2013). URL: https://www.bka.gv.at/ DocView.axd?CobId=50999 (дата звернення 17.01.2021).

203. A-SIT. URL: https://demo.a-sit.at/a-sit/ (дата звернення 17.01.2021).

204. Kuratorium Sicheres Österreich URL: https://kuratorium-sicheres-oesterreich.at/ (дата звернення 17.01.2021).

205. Austrian Trust Circle. URL: https://www.cybersecurityintelligence.com/austrian (дата звернення 17.01.2021).

206. Focus: Country Reports. URL: https://www.enisa.europa.eu/news/enisa-news (дата звернення 17.01.2021).

207. Finland's Cyber Security Strategy (2013). URL: http://www.yhteiskunnanturvallisuus.fi/ en/materials (дата звернення 17.01.2021).

208. Haeni R. 2016. Cybersecurity: New EU Directive. Published 20.07.2016. URL: https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published/ (дата звернення 17.01.2021).

209. Cyber rapid response teams and mutual assistance in cyber security. URL: https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/ (дата звернення 17.01.2021).

210. Six EU countries unite against cyber threats: the joint Cyber Rapid Response Teams are ready to counter cyber-attacks. Ministry of national defence republic of Lithuania 2020.03.04. URL: http://kam.lt/en/news_1098/current_issues/six_eu_countries_unite_against_cyber_threats_the_joint_cyber_rapid_response_teams_are (дата звернення 17.01.2021).

211. Šešios ES šalys susivienijo prieš kibernetines grėsmes: atakas atremti pasirengusios jungtinės Greitojo kibernetinio reagavimo komandos. Lietuvos respublikos krašto apsaugos ministerija. URL: http://kam.lt/lt/naujienos_874/aktualijos_875/sesios_es_salys_susivienijo_pries_kibernetines_gresmes_atakas_atremti_pasirengusios (дата звернення 17.01.2021).

212. Ответ официального представителя МИД России А. К. Лукашевича на вопрос СМИ в связи с обращением Центра государственного языка Латвии к жителям страны разговаривать на рабочих местах только на латышском языке. МИД России. URL: http://archive.mid.ru//brp_4.nsf/newsline/F1D4CD (дата звернення 17.01.2021).

213. Internet world stats, 2019. Top 20 countries with the highest number of internet users. URL: https://www.internetworldstats.com/top20.htm (дата звернення 17.01.2021).

214. CISCO, 2016. Цифровая революция в Индии. URL: https://www.cisco.com/c/ru_ua/about/press/2016 (дата звернення 17.01.2021).

215. Digital India, 2015. URL: https://www.digitalindia.gov.in (дата звернення 17.01.2021).

216. Ministry of Law, Justice and Company Affairs (Legislative Department), 2000. The Information Technology Act. URL: https://meity.gov.in/writereaddata/files/itbill.pdf (дата звернення 17.01.2021).

217. Moody, R., 2019. Which countries have the worst (and best) cybersecurity? URL: https://www.comparitech.com (дата звернення 17.01.2021).

218. Куприянов, А., 2019. Индия в эпоху кибервойн. URL: https://russiancouncil.ru/analytics-and-comments/analytics/indiya-vepokhu-kibervoyn/#detail (дата звернення 17.01.2021).

219. Ministry of Electronics & Information Technology, Government of India, 2013. National Cyber Security Policy-2013. URL: https://meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (дата звернення 17.01.2021).

220. Waghre, P. and Mehta Sh., 2019. 'India's National Cybersecurity Policy Must Acknowledge Modern Realities. India's National Cybersecurity Policy must bolster its global ambitions'. The Diplomat (December 20) URL: https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-mustacknowledge-modern-realities/ (дата звернення 17.01.2021).

221. Goel, V., Raj, S. and RavichandranJuly, P., 2018. How WhatsApp Leads Mobs to Murder in India. URL: https://www.nytimes.com/interactive/2018/07/18 (дата звернення 17.01.2021).

222. Government of Canada Announces New National Cyber Security Strategy and the Creation of the Canadian Centre for Cyber Security URL: https://cyber.gc.ca/en/guidance/government-canada-announces-new-national-cyber-security-strategy-and-creation-canadian (дата звернення 17.01.2021).

223. Maj Gen PK Mallick. U.S. National Cyber Strategy and Department of Defence (DoD) Cyber Strategy: An Analysis. 2018. URL: https://www.vifindia.org/sites/default/files/US-National-Cyber-Strategy-and-Department-of-Defence-Cyber-Strategy.pdf (дата звернення 17.01.2021).

224. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу сша, канади та інших Інформаційна довідка. *Європейське інформаційно-дослідницький центр*. 2018. URL: euinfocenter.rada.gov.ua

225. Israel National Cyber Directorate URL: https://www.gov.il/en/departments/israel_national_cyber_directorate (дата звернення 17.01.2021).

226. A Look at Israel's New Draft Cybersecurity. Blog Post *by* Guest Blogger for Net Politics. Law. *July 2, 2018* URL: https://www.cfr.org/blog/look-israels-new-draft-cybersecurity-law (дата звернення 17.01.2021).

227. Cyberwellness Profile Israel URL: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Israel.pdf (дата звернення 17.01.2021).

228. Гребенюк М.В., Леонов Б.Д. досвід Ізраїлю у сфері забезпечення кібербезпеки. *Інформація і право*. № 2(25)/2018. С. 45-50

229. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення 17.01.2021).

230. Власюк О. С. Російська інформаційна політика як виклик європейському політичному та безпековому простору. Блоги. URL: http://blogs.ukrinform.gov.ua/blog/oleksandr-vlasyuk/rosiyska-informaciyna-polityka-yak-vyklyk-yevropeyskomu-politychnomu (дата звернення 17.01.2021).

231. Меморандум про гарантії безпеки у зв'язку з приєднанням України до Договору про нерозповсюдження ядерної зброї від 05.12.1994 URL: http://zakon0.rada.gov.ua/laws/show/998_158 (дата звернення 17.01.2021).

232. Тристороння заява Президентів України, США та Росії від 14.01.1994 URL: http://zakon4.rada.gov.ua/laws/show/998_300 (дата звернення 17.01.2021).

233. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору від 09.07.1997 URL: http://zakon0.rada.gov.ua/laws/show/994_002 (дата звернення 17.01.2021).

234. Бєлоколос О. Деякі роздуми про Будапештський меморандум та міжнародні гарантії безпеки України. Дзеркало тижня. 28 листопада, 2014. URL: https://dt.ua/international/deyaki-rozdumi-pro-budapeshtskiy-memorandum-ta-mizhnarodni-garantiyi-bezpeki-ukrayini-_.html (дата звернення 17.01.2021).

235. Тарасюк А. В. Пріоритети національної політики України у сфері забезпечення міжнародної кібербезпеки. *Visegrad Journal on Human Rights*. 2021. № 1. С. 48-53.

236. Тарасюк А. В. Понятійно-категоріальний синтез правового забезпечення кібербезпеки України. *Порівняльно-аналітичне право*. С. 296-298. URL : http://www.pap.in.ua/5_2019/77.pdf. (дата звернення 17.01.2021).

237. Тарасюк А. В. Стан правового забезпечення кібербезпеки в Україні. *Наукові записки ЛУБП. Серія «Право»*. 2019. Вип. 23. С. 201–206.

238. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія «Юридичні науки»*. 2020. Т. 31 (70), № 2. – С. 119–124.

239. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. № 1. С. 133–136.

240. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи; Одеса : *Фенікс*, 2020. 404 с.

241. Тарасюк А. В. Пріоритетні питання забезпечення кібербезпеки України. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку* : зб. мат. III Міжнародної наук.-практ. конф., м. Острог, 14 черв. 2019 р. / упорядн.: С. О. Дорогих, І.М. Доронін та ін. ; НУОА, НДІІП НАПрН України. К. : ТОВ «Вид. дім «АртЕк», 2019. С. 181–185.

242. Тарасюк А. В. Новації у сфері кібербезпеки великої Британії. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. X Всеукр. наук.-практ. конф. м. К., 4 квіт. 2019 р. С. 217–218.

243. Яцишин М. Ю. Сучасні тенденції у сфері міжнародно-правового регулювання кіберпростору. *Проблеми ефективності міжнародного пр*ава : матеріали міжнар. наук.-практ. конф., м. К., 29 березня 2013 р. / за заг. ред. В.Н. Кубальського. Київ : Інститут держави і права ім. В.М. Корецького НАН України, 2013. С. 103–10

244. Булеца С. Б. Заборовський В. В., Стойка А. В. Деякі проблемні питання правового захисту прав людини четвертого покоління. *Науковий вісник Ужгородського національного університету*, 2019 Серія ПРАВО. Випуск 55. Том 1. С. 10-14

245. Ланде Д .В., Фурашев В. М., Юдкова К. В. Основи інформаційного та соціально-правового моделювання. К. : НТУУ "КПІ", 2014. 220 с.

246. Золотар О .О. Правові основи інформаційної безпеки людини. Автореф. дис. …. д.ю.н за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Харків. 2018. 39 с.

247. Пилипчук В. Г. Актуальні проблеми державної політики з питань захисту прав і безпеки людини в інформаційній сфері. Інформаційне право: сучасні виклики і напрями розвитку: Матеріали першої наук.-практ. конф. 18 жовтня 2018 р., м. Київ. / Упоряд.: В. М. Фурашев, С. Ю. Петряєв. К. : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2018. 196 с.

248. Philosophie des Rechts. Werke, т. VIII. 321 p.

249. Шершеневич Г. Ф. История философии права. СПб.: Издательство «Лань», 2001. 512 с.

250. Lane R. E. The Decline of Politics and Ideology in a Knowledgeable Society American Sociological Review Vol. 31, No. 5 (Oct., 1966), pp. 649-662

251. Pakulski J., Waters M. The Death of Class. First Published July 1, 1997 Volume: 21 issue: 2, page(s): 192-193

252. Белл Д. Грядущее постиндустриальное общество. М.: Academia, 2004 . 944 с.

253. Кастельс М. Информационная эпоха : экономика, общество и культура. Изд. дом ГУ-ВШЭ, 2000. 608 с.

254. Masuda, Yoneji. 1980. The Information Society and Post-Industrial Society. Washington: World Future Society. pp. vii–viii, 31–33 URL: https://newlearningonline.com/new-learning/chapter-3/yoneji-masuda-on-the-information-society (дата звернення 17.01.2021).

255. Martin W.J. The Information Society. 1995. London. 256 p.

256. Тапскотт Дон. Электронно-цифровое общество: Плюсы и минусы эпохи сетевого интеллекта : пер. с англ. / Дон Тапскотт ; Под общ.рук. Игорь М. Дубинский. Москва : Рефл-бук ; Київ : INT-пресс, 1999. 406 с.

257. Золотар О. О. Загрози інформаційній безпеці людини. *Правова інформатика*. № 2(42)/2014. С. 70-79

258. Гейтс Б. Бизнес со скоростью мысли. М. : Эксмо-Пресс, 2001. 445 с.

259. Hartley R. V. L. Information Theory of The Fourier Analysis and Wave Mechanics», August 10, 1955, publication information unknown

260. Шеннон К. Работы по теории информации и кибернетике. М. : ИЛ, 1963. 830 с.

261. Stonier T. Information as a basic property of the universe. Volume 38, Issues 2–3, 1996, Pages 135-140 URL: https://www.sciencedirect.com/science/article/abs/pii/0303264796883687 (дата звернення 17.01.2021).

262. Скулиш Є. Д. Інформаційна безпека: нові виклики українському суспільству. *Інформація і право*, 2012 - № 2/5, С.170-175

263. Резолюція Генеральної Асамблеї ООН від 14 грудня 1946 р. A/RES/59(I). URL: https://undocs.org/ru/A/RES/59(I) (дата звернення 17.01.2021).

264. Конвенція Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення 17.01.2021).

265. Резолюція Генеральної Асамблеї ООН від 9 грудня 1998 р. A /53/ 144. URL: http://www.un.org/ru/documents/decl_conv/declarations/defender.shtml (дата звернення 17.01.2021).

266. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *International relations, part "Political sciences"*. №18-19. 2018р. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468/3140 (дата звернення 17.01.2021).

267. Budapest Convention and related standards. Budapest, 23/11/2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення 17.01.2021).

268. Constitution of the international telecommunication union. Rev. Marrakesh, 2002). URL: https://www.itu.int/council/pd/constitution.html (дата звернення 17.01.2021).

269. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.EN (дата звернення 17.01.2021).

270. Войціховський А.В. Кібербезпека як напрям євроатлантичної інтеграції України. Право і безпека у контексті європейської та євроатлантичної інтеграції: Зб. сатей та тез наук. повідомл. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму, м. Харків, 28 верес. 2018 р. / редкол.: Ю.Г. Барабаш, Т.М. Анакіна. Харків: Право, 2018. 190 с.

271. Стратегічна концепція оборони та безпеки членів НАТО від 19.11.2010 р. URL: https://www.nato.int/cps/uk/natohq/official_texts_68580.htm (дата звернення 17.01.2021).

272. Декларації Чиказького саміту від 20.05.2012 р. НАТО. URL: https://www.nato.int/cps/uk/natohq/official_texts_87593.htm?selectedLocale=uk (дата звернення 17.01.2021).

273. Cyber defence / Офіційний сайт Організації Північноатлантичного договору. Організація Північноатлантичного договору. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm (дата звернення 17.01.2021).

274. Зміна підходів до кіберзахисту // Офіційний сайт Організації Північноатлантичного договору / НАТО РЕВЮ. 2016 р. URL: https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/UK/index.htm (дата звернення 29.01.2021).

275. Довгань О. Д., Тарасюк А. В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*. 2020. № 2. С. 85–98

276. 11. Тарасюк А. В. Системний підхід у дослідженні правових основ кібербезпеки. *Прикарпатський юридичний вісник*. 2020. № 2. С. 108–111

277. Тарасюк А. В. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254–258

278. Тарасюк А. В. Забезпечення кібернетичної безпеки людини: міжнародно-правовий аспект. *Юридичний вісник*. 2020. № 3. С. 254–261

279. Тарасюк А. В. Онтологічні засади поняття «кібербезпека». *Управління інформаційною безпекою*: зб. мат. наук.-практ. конф. НА СБУ. К., С.3 3-35

280. Тарасюк А. В. Окремі питання функціональних завдань суб'єктів забезпечення кібербезпеки. *Міжнародні та національні правові виміри забезпечення стабільності*: зб. мат. Міжн. наук.-практ. конф. м. Львів, 17–18 квіт. 2020 р. С. 72–76

281. Christopher Sabatini The Decline of Ideology and the Rise of "Quality of Politics" Parties in Latin America. World Affairs. Vol. 165, No. 2 (FALL 2002), pp. 106-110 URL: https://www.jstor.org/stable/20672655 (дата звернення 29.01.2021).

282. Pakulski J. The Visegrad Countries in Crisis. Warsaw, 2016. 128 p.

283. Daniel Bell The Coming of the Post-Industrial Society. A Venture in Social Forecasting (Heinemann, 1974), pp. 507

284. Bell D. The cultural contradictions of capitalism. N.Y.: Basic Books, 1976 p. 402 c.

285. McKinsey Global Institute. Applying artificial intelligence for social good. McKinsey Global Institute. 2018. URL: https://www.mckinsey.com/featuredinsights/artificial-intelligence/applying-artificial-intelligence-for-social-good (дата звернення 29.01.2021).

286. The Global Competitiveness Report 2018. World Economic Forum. Geneva. 2018. URL: www.weforum.org (дата звернення 29.01.2021).

287. Сучасне суспільство: філософсько-правове дослідження актуальних проблем: монографія / О. Г. Данильян, О. П. Дзьобань, С. Б. Жданенко та ін.; за ред. О. Г. Данильяна. Харків: Право, 2016. 488 с.

288. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: *колективна монографія* / за ред. д.ф.н., проф. В.Г. Воронкової. Запоріжжя: Вид-во ЗДІА, 2017. 292 с.;

289. Dzeban O., Aleksandrova O., Vinnikova N. Axiological portrait of information society. *Схід: аналітично-інформаційний журнал*. 2019. № 5 (163). С. 13-19

290. Yoneji Masuda The Information Society as Post-industrial Society. World Future Society, 1981. P. 171

291. Toffler A. The Third Wave. / Alvin Toffler. New York: Bantam Books, 1980. P. 544

292. Тоффлер Э. Столкновение с будущим. (Отрывки из книги). *Иностранная литература*. 1972. № 3. С. 228-249

293. Мартин Дж. Организация баз данных в вычислительных системах. М.: Мир, 1980, 662 с.

294. Уебстер Ф. Теории информационного общества / Под ред. Е. Л. Вартановой / Пер. с англ. М.: Аспект Пресс, 2004. 400 с.

295. Drucker P.F. The Age of Discontinuity: Guidelines to our Changing Society. London: Published January 30, 1992 by Routledge 434 P.

296. К обществам знания: Всемирный доклад ЮНЕСКО 2005 URL: http//unesdoc.unesco (дата звернення 29.01.2021).

297. Дзьобань О. П., Жданенко С. Б. Від “інформаційного суспільства” до “інформаційної безпеки”: до проблеми концептуалізації сутності понять. *Інформація і право*. № 2(29)/2019. С. 60-73

298. Robertson R., Lechner F. Modernization, Globalization and the Problem of Culture in the World-Systems Theory // Theory, Culture & Society. - 1985. - № 3

299. Robertson R. Globalization Theory and Civilization Analysis. Comparative Civilizations Review. 1987. Vol.17; Robertson R. Globalization Theory and Civilization Analysis. Comparative Civilizations Review. 1987, Vol. 17

300. Burton J. World Society. Cambridge. Cambridge University Press. 1972.

301. Levitt T. The Globalization of Markets. Harvard Business Review. 1983. URL: https://hbr.org/1983/05/the-globalization-of-markets (дата звернення 29.01.2021).

302. Internet democracy. URL: http://en.wikipedia.org/wiki/Internet_democracy (дата звернення 29.01.2021).

303. Протоколи передачі даних. URL: http://ru.wikipedia.org/wiki/Сетевой_протокол (дата звернення 29.01.2021).

304. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

305. Стратонов В. «Комп'ютерні злочини»: окремі особливості та характеристики. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 2. С. 134-141

306. Хахановський В. Г., Гавловський В. Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. № 2(33)/2020. С. 99-108

307. Костенко О. В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. *Інформація і право*. № 3(30)/2019. С. 96-104

308. Eriksson J., Giacomello G. Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State. *International Studies Review*. 2009. Vol. 11(1). P. 20

309. Post D., Johnson D. The Great Debate – Law in the Virtual World First Monday. 2006. Vol. 11(2). P. 1230

310. Benkler Y. The Wealth of Networks, How Social Production Transforms Markets and Freedom. New Haven, Conn: Yale University Press, 2006.

311. Манифест киборгов: наука, технология и социалистический феминизм 1980-х / Автор: Харауэй Д., Издательство: Ад Маргинем Пресс, Серия: Minima 128 с.

312. Giacomello G. Technology and International Relations. Monograph. 2021. 224 p.

313. Management of government information systems, elements of strategies and policies. New York: United Nations, 1999. P. 174

314. Лессиг Л. Свободная культура/Пер. с англ. М.: Прагматика Культуры, 2007. 272 с.; Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books, 1999. 297 p.

315. Froehlich T. J. Survey and analysis of legal and ethical issues for library and information services, UNESCO Report (Contract № 401.723.4), for the International Federation of Library Associations. IFLA Professional Series. – Munich: G. K. Saur, 1997

316. Mayer P. Das Internet im offentlichen Recht. Unter Berucksichtigung europarechtlicher und volkerrechtlicher Vorgaben. Berlin: Duncker & Humblot, 1999

317. Goldsmith J., Wu T. Who Controls the Internet?: Illusions of a Borderless World. New York: Oxford University Press, 2006

318. Les dimensions internationales du droit du cyberspace. Publio sous la direction de Teresa Fuentes-Camacho. Editions UNESCO. 2000. P. 11

319. Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. URL: https://rm.coe.int/1680081580 (дата звернення 29.01.2021).

320. Electronic Frontier Foundation. URL: https://www.eff.org (дата звернення 29.01.2021).

321. Lü Y. Privacy and data privacy in contemporary China. In Ethics and Information Technology. 2005. P. 7-15

322. Hongladarom S. Analysis and Justification of Privacy from a Buddhist Perspective. *Information Technology Ethics: Cultural Perspectives*: Idea Group, 2007. P.122

323. Nakada M., Tamura T. Japanese conceptions of privacy: An intercultural perspective. *In Ethics and Information Technology*. 2005. P. 27-36

324. Фуко М. Археологія знання; пер. з фр. В. Шовкуна. К. : Основи, 1996. 326 с.

325. Lessig L. Code and Other Values of Cyberspace. New York: Basic Books, 1999. P. 89

326. Клятва Гіппократа. Національний медичний університет ім. О. О. Богомольця. URL: http://nmuofficial.com/zagalni-vidomosti/klyatva-gippokrata/ (дата звернення 29.01.2021).

327. McQuail D. McQuail's Mass Communication Theory. London. 2010. 534 p. URL: http://docshare04.docshare.tips/files/28943/289430369.pdf (дата звернення 29.01.2021).

328. Gotterbarn D., Rogerson S. Responsible Risk Analysis for Software Development: Creating the Software Development Impact Statement. Communications of the Association for Information Systems. 2005. № 15(40)

329. R Rubin, TJ Froehlich Ethical aspects of library and information science. Encyclopedia of library and information sciences, 2010. P. 1743-1757

330. Кириченко М. О. Інформаційна антропологія й інформаційна етика як складники формування ідеології інформаційного суспільства. *Актуальні проблеми філософії та соціології*. 2017. №3. С. 51-53

331. Информационная этика. ЮНЕСКО. URL: http://www.dlab.irtc.org.ua/IFAP_UA/programu.html (дата звернення 29.01.2021).

332. Програма «Інформація для всіх» Офіційний сайт. URL: http://www.dlab.irtc.org.ua/IFAP_UA/programu.html (дата звернення 29.01.2021).

333. Трофименко О. Г., Прокоп Ю. В., Логінова Н. І., Задерейко О. В. Моніторинг рівня кібербезпеки України у світових рейтингах. *Інформаційна безпека людини, суспільства, держави*. К. : Національна академія Служби безпеки України. 2019. №3(27). С. 100–107

334. Bynum T. The Development of Computer Ethics as a Philosophical Field of Study. *The Australian Journal of Professional and Applied Ethics*. 1999. № 1(1).

335. Лук'янчук Р. В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції. *Вісник Національної академії державного управління при Президентові України*. 2015. № 3. С. 110-117

336. Advancing Technology for Humanity. URL: https://www.ieee.org/ (дата звернення 29.01.2021).

337. ACM Invites You to Celebrate #WomensHistoryMonth by Sharing Your Stories. URL: https://www.acm.org/ (дата звернення 29.01.2021).

338. Brody R. Information ethics in the design and use of metal. IEEE Technology and Society Magazine. 2003. Vol. 22(2). P. 34

339. Обшуки в Яндекс: за ким шпигувала російська компанія. URL: https://politeka.net/uk/news/443162-obyski-v-yandeks-za-kem-shpionila-rossijskaya-kompaniya-video (дата звернення 29.01.2021).

340. EUSIDIC. Офіційний сайт. URL: http://www.eusidic.org (дата звернення 29.01.2021).

341. Thomas J. Froehlich Philosophical Musings on the Underbelly of Information Age. *Informatio. Revista del Instituto de Información de la Facultad de Información y Comunicación*. V.1 2021. P. 132-177

342. Creative Commons. URL: http://creativecommons.org (дата звернення 29.01.2021).

343. In search of a code of global information ethics:the road travelled and new horizons. Rafael Capurro and Johannes B. Britz. URL: http://www.capurro.de/britz.html (дата звернення 29.01.2021).

344. Тарасюк А. В. Місце концепції «суспільства знань» у процесах забезпечення кібернетичної безпеки. *Юридичний науковий електронний журнал*. 2020. № 6. С. 156–169. URL: http://www.lsej.org.ua/6_2020/40.pdf. (дата звернення 29.01.2021).

345. Тарасюк А. В. Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях. *Вісник Запорізького національного університету. Юридичні науки*. 2020. № 4. Т. 1. С. 168–173.

346. Тарасюк А. В. Теоретико-правове підґрунтя інформаційної етики у системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52.

347. Тарасюк А. В. Окремі аспекти соціального чинника в забезпеченні кібербезпеки суспільства. KELM (Knowledge, Education, Law, Management). 2020. № 3 (31). С. 206–211.

348. Тарасюк А. В. Окремі аспекти співпраці державного та приватного секторів безпеки у забезпеченні кібербезпеки. *Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні*: зб. мат. міжн. наук.-практ. конф. м. Запоріжжя, 24–25 квіт. 2020 р. С. 77–81.

349. Довгань О. Д., Тарасюк А. В. Національні інтереси України в кібернетичній сфері. *Інформація і право*. 2021. № 1. С. 134-142

350. Тарасюк А. В. Забезпечення кібербезпеки України як пріоритетне завдання цифрової дипломатії. Кібербезпека в Україні: правові та організаційні питання» : зб. мат. ІІ Міжнародної наук.-практ. конф. м. Одеса, 26 листоп. 2020 р. С. 23–24.

351. Тарасюк А. В. Питання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : мат. наук.-практ. конф., м. К., 10 груд. 2020 р. / упоряд О. А. Баранов, В. М. Фурашев, С. О. Дорогих. К. : Фенікс, 2020. С. 241–246

352. Сегеда О. О. Цифрова дипломатія України як елемент нової публічної дипломатії. *Науковий журнал «ПОЛІТИКУС»*. Випуск 3. 2020. С. 139-147

353. Global Risks 2012 Seventh Edition. Insight Report. URL: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf (дата звернення 29.01.2021).

354. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці. *Серія: Державне управління*, 2019 р., № 2 (66). С. 191-197

355. Носач А. В. Загрози національній безпеці як обов'язкова ознака злочинності, що посягає на державний суверенітет і територіальну цілісність України. *Право і суспільство*. 2019. №3. С. 50–56

356. Okinawa Charter on the Global Information Society. United Nations Economic and Social Commission for Western Asia. URL: https://www.unescwa.org/okinawa-charter-global (дата звернення 29.01.2021).

357. Jeffrey A. Hart The Digital Opportunities Task Force: The G8's Effort to Bridge the Global Digital Divide. 26 p. URL: https://www.researchgate.net/publication/228852360_The_Digital_Opportunities_Task_Force_The_G8's_Effort_to_Bridge_the_Global(дата звернення 29.01.2021).

358. Coronavirus underscores urgency to bridge digital divide. DW. URL: https://www.dw.com/en/coronavirus-underscore (дата звернення 29.01.2021).

359. Урочисте засідання, присвячене 20-ій річниці підписання Хартії про особливе партнерство між Україною та НАТО. URL: https://www.rada.gov.ua/preview/anons_acred/146596.html (дата звернення 29.01.2021).

360. 12 червня 2020 року Україна отримала статус члена Програми розширених можливостей НАТО. Урядовий портал: URL: https://www.kmu.gov.ua/news/ukrayina-otrimala-status-chlena-programi-rozshirenih-mozhlivostej-nato (дата звернення 29.01.2021).

361. Баровська А. В. Понятійно-категоріальний апарат інформаційної сфери: правовий аспект. Національний інститут стратегічних досліджень. URL: http://old2.niss.gov.ua/articles/532/ (дата звернення 29.01.2021).

362. Литвин Н. А. Наукові підходи щодо визначення поняття державної інформаційної політики в Україні. *Наука і правоохорона*. 2019. № 1(43). С. 253–261

363. Furtak A. et al. Bios and secure boot attacks uncovered. The 10th ekoparty Security Conference. 2014

364. Herala A. et al. Strategy for Data: Open it or Hack it? *Journal of Theoretical and Applied Electronic Commerce Research*. 2019. Т. 14. № 2. С. 33-46

365. Василенко М. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. *Юридичний вісник*. 2018. № 3. С. 17-24

366. Богуславська О. Г. Формування іміджу як конкурентної переваги в сучасному інформаційному суспільстві: теоретико-методологічні засади та практичні рекомендації. *Гуманітарний вісник ЗДІА*. 2017. Вип. 71. С. 149-157

367. Грущинська Н. М. Геоекономічна стратегія в умовах міжнародної конкуренції. *Науковий вісник Ужгородського національного університету*. Випуск 9. 2016. С. 30-33

368. Соснін О. Управління сучасною державою: роль цифрових технологій. *Юридичні новини України*. LexInform. 06.05.2020 URL: https://lexinform.com.ua/dumka-eksperta/upravlinnya-suchasnoyu-derzhavoyu-rol-tsyfrovyh-tehnologij-2/ (дата звернення 29.01.2021).

369. Проблема PGP. ХАБР. 21 июля 2019. URL: https://habr.com/ru/post/460827/ (дата звернення 29.01.2021).

370. Євсеєв С. П., Йохов О.Ю., Король О.Г. Гешування даних в інформаційних системах : монографія. Х. : Вид. ХНЕУ, 2013. 312 с.

371. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів. № 4004 від 01.09.2020. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення 29.01.2021).

372. Ризики використання готівки. Державна служба фінансового моніторингу України. 2017. URL: https://www.ipay.ua/media/files/tipolog_gotivka2017.pdf (дата звернення 29.01.2021).

373. Міжнародний досвід законодавчого регулювання питання функціонування криптовалют, криптовалютних бірж, майнінгу та виводу в фіат. Інформаційна довідка. URL: https://radaprogram.org/sites/default/files/infoc.pdf (дата звернення 29.01.2021).

374. Прогнозы о рынке криптовалют URL: https://legalhub.online/tse-po-roboti/tradytsijni-groshi-vykorystovuyutsya-dlya-vidmyvannya-u-800-raziv-chastishe-za-bitkoyiny-doslidzhennya (дата звернення 29.01.2021).

375. The RAND Corporation is a nonprofit institution that helps improve policy and decision making through research and analysis. URL: http://www.rand.org/about. (дата звернення 29.01.2021).

376. Аналіз державної політики у сфері національної безпеки і оборони України. К. 2015. Коаліція Реанімаційний Пакет Реформ. URL: https://rpr.org.ua/wp-content/uploads/2018/02/Analiz-polityky-NB-pravl-final.pdf (дата звернення 29.01.2021).

377. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. URL: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (дата звернення 29.01.2021).

378. Department of Defense, Strategy for Operation in Cyberspace (2011). URL: https://fas.org/irp/eprint/dod – cyber.pdf

379. Пашунин И. США милитаризируют Интернет. «Таллинское руководство» по ведению кибервойны. URL: http://d-russia.ru/ssha-militariziruyut-internet-tallinnskoe-rukovodstvo-po-vedeniyu-kibervojny.html; (дата звернення 29.01.2021).

380. Проект Закону про критичну інфраструктуру та її захист. № 10328 від 27.05.2019. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3(дата звернення 29.01.2021).

381. Еннан Р. Є. Правове регулювання відносин у мережі Інтернет. IT ПРАВО: *Проблеми і перспективи розвитку в Україні*. URL: http://aphd.ua/publication-173/ (дата звернення 29.01.2021).

382. Новицький А. М. Міжнародний досвід правового регулювання Інтернет. *Юридичний вісник. Повітряне і космічне право*. 2014. No 2. С. 52–58

383. Гуцу С.Ф. Правове регулювання мережі інтернет: міжнародний і вітчизняний досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. Випуск 2 (38) 2018. С. 114-118

384. Лесько Н. В., Гулак Л. С. Правові засади управління інтернетом. *Порівняльно-аналітичне право*. №8. 2020. С. 140-143

385. Указ Президента Республики Беларусь от 4 февраля 2010 г. № 60 «О переводе всех участников интернет-отношений в белорусскую зону». URL: http://pravo.by/main.aspx?Guid=3871&p0=P31000060&p2={NRPA} (дата звернення 29.01.2021).

386. Zekos G. I., Amvrosia-Komotini T. Cyberspace and Globalization. *Law, Social Justice & Global Development* (LGD). 2002. P. 65.

387. Резолюция, принятая Генеральной Ассамблеей 21 декабря 2009 года [по докладу Второго комитета (A/64/422/Add.3)] 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур. URL: https://undocs.org/ru/A/RES/64/211 (дата звернення 29.01.2021).

388. Browse Privately. Explore Freely. URL: https://www.torproject.org/ (дата звернення 29.01.2021).

389. Probabilistic Analysis of Onion Routing in a Black-box Model [Extended Abstract], WPES'07: Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, ACM Press, October 2007, pp. 1--10 URL: https://www.onion-router.net/Publications/wpes08 (дата звернення 29.01.2021).

390. Deploying Low-Latency Anonymity: Design Challenges and Social Factors", IEEE Security & Privacy, September/October 2007 (Vol. 5, No. 5), pp. 83-87

391. Японская полиция формирует спецотряд для борьбы с киберпреступностью и кражей криптовалют. URL: https://bitnovosti.com/2018/04/03/yaponskaya-politsiya-formiruet-spetsotryad-dlya-borby-s-kiberprestupnostyu (дата звернення 29.01.2021).

392. Ball J., Schneier B., Greenwald G. NSA and GCHQ target Tor Network that Protects Anonymity of Web Users // URL: https://www.schneier.com/essays/archives (дата звернення 29.01.2021).

393. National Security Agency Central Security Service. URL: https://www.nsa.gov (дата звернення 29.01.2021).

394. Коопс Б.- Ж. (Koops B.- J.), Хоепман Ж.- Х. (Hoepman J.- H.), Линес Р. (Leenes R). Open – source intelligence and privacy by design. *Computer Law & Security Review*. 2013. № 29. P. 676 – 688

395. Уголовные кодексы. Legislationline.org. URL: https://www.legislationline.org/ru/documents/ section/criminal-codes/country (дата звернення 29.01.2021).

396. Response to the public consultation on a review of the functioning of regulation (EC) NO 544/2009 11 February 2011. URL: http://ec.europa.eu/information_society/activities pdf (дата звернення 29.01.2021).

397. TECHWORM. URL: https://www.techworm.net/2017/06/the – pirate – bay – can – be – blocked – rules (дата звернення 29.01.2021).

398. COMPARE & RESEARCH THE LAW. *Worldwide*. URL: https://iclg.com/practice – areas/copyright – laws – and – regulations/Germany

399. Марушева О. Г. Міжнародне право: навч. посіб. Х. : ХДУХТ, 2015. 243 с.

400. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces. URL: https://repository.law.umich.edu (дата звернення 29.01.2021).

401. Послание по случаю Всемирного дня электросвязи и информационного общества. Генеральный секретарь ООН. URL: https://www.un.org/ru/sg/messages (дата звернення 29.01.2021).

402. Тарасюк А. В. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights*. 2020. № 1. С. 167–172

403. Тарасюк А. В. Актуальні питання правового забезпечення кібербезпеки України. *Recht der Osteuropäischen Staaten*. 4/2019. С. 164–168

404. Тарасюк А. В. Пріоритети забезпечення кібербезпеки: досвід окремих країн. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. 4. С. 42–49.

405. Тарасюк А. В. Місце та роль України у глобальних інформаційних процесах: питання кібербезпеки. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. XI (43). С. 46–52.

406. Тарасюк А. В. Онтологічні засади поняття «кібербезпека». *Управління інформаційною безпекою* : зб. мат. наук.-практ. конф. НА СБУ. К., С. 197-199

407. Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : *моногpаф*. Х. : Вид-во «ФІНН», 2011. 192 с.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці в яких опубліковані основні наукові результати дисертації:

1. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи; Одеса : Фенікс, 2020. 404 с.

2. Тарасюк А.В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монограф. Х. : Вид-во «ФІНН», 2011. 192 с.

3. Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с., підр. 5.2.

4. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

5. Довгань О.Д., Тарасюк А.В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності *Інформація і право*. 2018. № 2 (25). С. 51–61.

6. Тарасюк А.В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. 4(31)/2019. С. 73–82.

7. Тарасюк А.В. Досвід забезпечення кібербезпеки у зарубіжних країнах. *Науковий вісник публічного та приватного права* : зб. наук. праць. 2019. № 4. С. 204–209.

8. Тарасюк А.В. Понятійно-категоріальний синтез правового забезпечення кібербезпеки України. *Порівняльно-аналітичне право*. С. 296-298. URL : http://www.pap.in.ua/5_2019/77.pdf.

9. Тарасюк А.В. Стан правового забезпечення кібербезпеки в Україні. *Наукові записки ЛУБП*. Серія «Право». 2019. Вип. 23. С. 201–206.

10. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки Таврійського національного університету імені В.І. Вернадського.* Серія «Юридичні науки». 2020. Т. 31 (70), № 2. – С. 119–124.

11. Тарасюк А.В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. № 1. С. 133–136.

12. Довгань О.Д., Тарасюк А.В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*. 2020. № 2. С. 85–98.

13. Тарасюк А.В. Системний підхід у дослідженні правових основ кібербезпеки. *Прикарпатський юридичний вісник*. 2020. № 2. С. 108–111.

14. Тарасюк А.В. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254–258.

15. Тарасюк А.В. Забезпечення кібернетичної безпеки людини: міжнародно-правовий аспект. *Юридичний вісник*. 2020. № 3. С. 254–261.

16. Тарасюк А.В. Місце концепції «суспільства знань» у процесах забезпечення кібернетичної безпеки. *Юридичний науковий електронний журнал*. 2020. № 6. С. 156–169. URL : http://www.lsej.org.ua/6_2020/40.pdf.

17. Тарасюк А.В. Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях. *Вісник Запорізького національного університету.* Юридичні науки. 2020. № 4. Т. 1. С. 168–173.

18. Тарасюк А.В. Теоретико-правове підґрунтя інформаційної етики у системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52.

19. Довгань О.Д., Тарасюк М.В. Національні інтереси України в кібернетичній сфері. *Інформація і право*. 2021. № 1. С. 134-142

20. Тарасюк А.В. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights*. 2020. № 1. С. 167–172.

21. Тарасюк А.В. Актуальні питання правового забезпечення кібербезпеки України. *Recht der Osteuropäischen Staaten*. 4/2019. С. 164–168.

22. Тарасюк А.В. Пріоритети забезпечення кібербезпеки: досвід окремих країн. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. 4. С. 42–49. URL : https://doi.org/10.25313/2520-2308-2020-4-5818.

23. Тарасюк А.В. Окремі аспекти соціального чинника в забезпеченні кібербезпеки суспільства. *KELM (Knowledge, Education, Law, Management)*. 2020. № 3 (31). С. 206–211.

24. Тарасюк А.В. Місце та роль України у глобальних інформаційних процесах: питання кібербезпеки. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. XI (43). С. 46–52. URL : https://doi.org/10.25313/2520-2308-2020-11-6528.

25. Тарасюк А.В. Пріоритети національної політики України у сфері забезпечення міжнародної кібербезпеки. *Visegrad Journal on Human Rights*. 2021. № 1. С. 48-53.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

26. Тарасюк А.В. Актуальні питання протидії кіберзлочинності в сучасних умовах. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.-практ. Семінару. м. Харків, 26 жовт. 2018 р. 2018. С. 251–254.

27. Тарасюк А.В. Кібербезпека – один із важливих напрямків захисту держави. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.- практ. семінару, м. Харків, 23 трав. 2019 р. / редкол.: С.О. Гриненко (голов. ред.) та ін. Х. : Право, 2019. Вип. 10. С. 44–47.

28. Тарасюк А.В. Законодавчі підходи до кібернетичної безпеки України. *Актуальні проблеми правових наук в євроінтеграційному вимірі* зб. мат. Міжнародної наук.-практ. конф. м. Харків, 20–21 груд. 2019 р. 2020 р.. С. 87–90.

29. Тарасюк А.В. Пріоритетні питання забезпечення кібербезпеки України. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку* : зб. мат. ІІІ Міжнародної наук.-практ. конф., м. Острог, 14 черв. 2019 р. / упорядн.: С.О. Дорогих, І.М. Доронін, О.Д. Довгань, О.В. Лебединська, В.Г. Пилипчук, О.Г. Радзієвська, М.С. Романов ; НУОА, НДІІП НАПрН України. К. : ТОВ «Вид. дім «АртЕк», 2019. С. 181–185.

30. Тарасюк А.В. Новації у сфері кібербезпеки великої Британії. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. Х Всеукраїнської наук.-практ. конф. м. Київ, 4 квіт. 2019 р. С. 217–218.

31. Тарасюк А.В. Окремі питання політики європейських країн щодо правового забезпечення кібербезпеки. *Теоретичні та практичні проблеми правового регулювання суспільних відносин* : зб. мат. Міжнародної наук.-практ. конф. м. Харків, 17–18 січ. 2020 р. С. 61–64.

32. Тарасюк А.В. Теоретико-правові конструкції правового забезпечення кібербезпеки України. *Реформування національного та міжнародного права: перспективи та пріоритети : зб. мат. Міжнародної наук.-практ. конф.* м. Одеса, 17–18 січ. 2020 р. С. 107–110.

33. Тарасюк А.В. Кіберпростір як об’єкт кібербезпеки держави. *Нові завдання та напрями розвитку юридичної науки у XXI столітті* : зб. мат. Міжнародної наук.-практ. конф. м. Одеса 21–22 лют. 2020 р. С. 115–118.

34. Тарасюк А.В. Окремі питання забезпечення кібербезпеки: досвід Європейського Союзу. *Міжнародне та національне законодавство: способи удосконалення* : зб. мат. Міжнародної наук.-практ. конф. м. Дніпро 3–4 квіт. 2020 р. С. 159–163.

35. Тарасюк А.В. Онтологічні засади поняття «кібербезпека». *Управління інформаційною безпекою* : зб. мат. Науково-практичної конф. НА СБУ. К., С.

36. Тарасюк А.В. Окремі питання функціональних завдань суб'єктів забезпечення кібербезпеки. *Міжнародні та національні правові виміри забезпечення стабільності* : зб. мат. Міжнародної наук.-практ. конф. м. Львів, 17–18 квіт. 2020 р. С. 72–76.

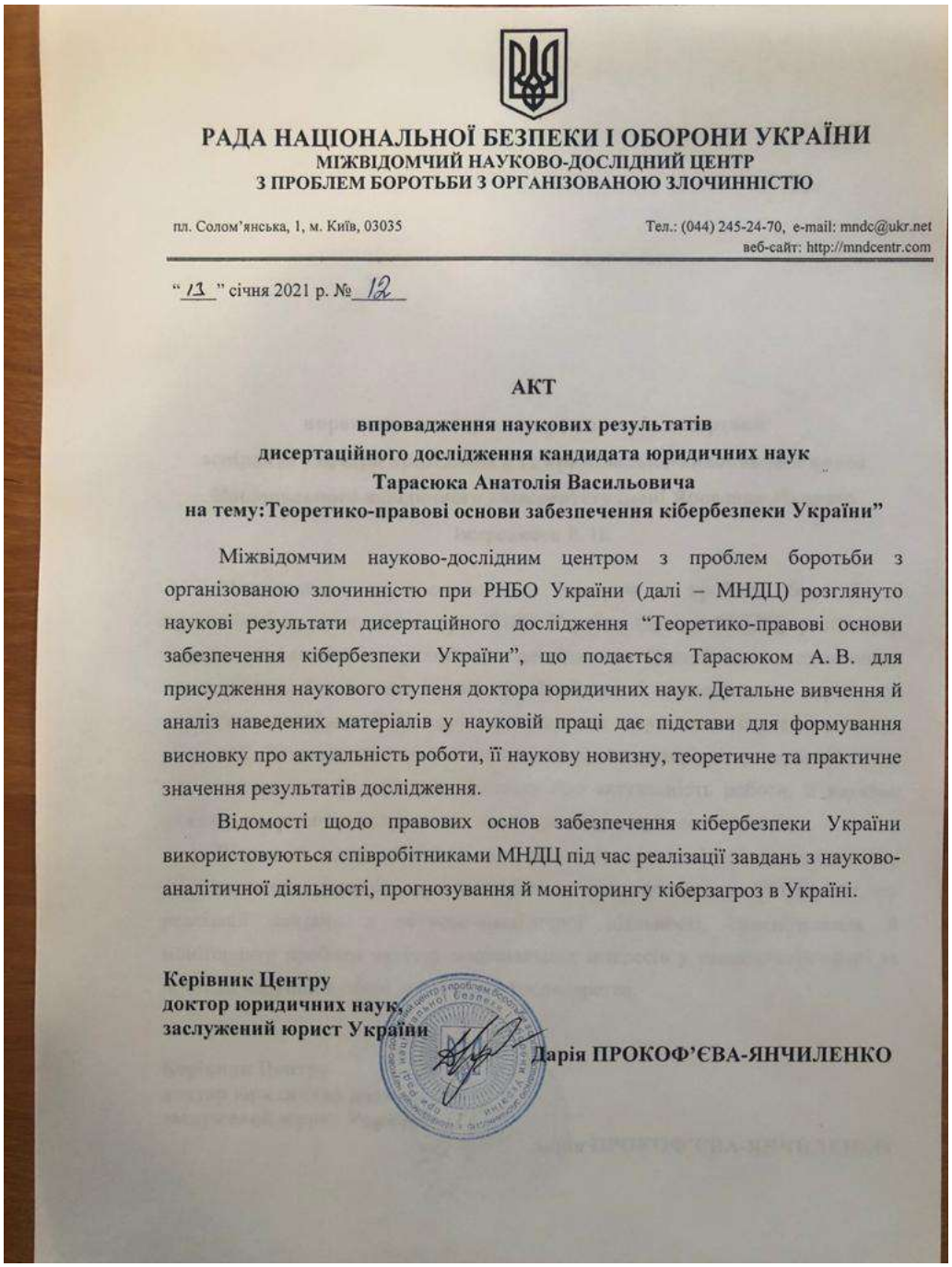
37. Тарасюк А.В. Окремі аспекти співпраці державного та приватного секторів безпеки у забезпеченні кібербезпеки. *Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні* : зб. мат. Міжнародної наук.-практ. конф. м. Запоріжжя, 24–25 квіт. 2020 р. С. 77–81.

38. Тарасюк А.В. Міжнародно-правові засади протидії кіберзагрозам *Розбудова правової держави в Україні: реалії та перспективи* : зб. мат. Міжнародної наук.-практ. конф. Одеса, 29 трав. 2020 р. С. 133–135.

39. Тарасюк А.В. Забезпечення кібербезпеки України як пріоритетне завдання цифрової дипломатії. *Кібербезпека в Україні: правові та організаційні питання» :* зб. мат. II Міжнародної наук.-практ. конф. м. Одеса, 26 листоп. 2020 р. С. 23–24.

40. Тарасюк А.В. Питання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : мат. наук.-практ. конф., м. Київ, 10 груд. 2020 р. / упоряд.: О.А. Баранов, В.М. Фурашев, С.О. Дорогих. К. : Фенікс, 2020. С. 241–246.

Додаток Б



РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ
МІЖВІДОМЧИЙ НАУКОВО-ДОСЛІДНИЙ ЦЕНТР
З ПРОБЛЕМ БОРОТЬБИ З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ

пл. Солом'янська, 1, м. Київ, 03035 Тел.: (044) 245-24-70, e-mail: mndc@ukr.net
веб-сайт: http://mndcentr.com

"13" січня 2021 р. № 12

АКТ

впровадження наукових результатів
дисертаційного дослідження кандидата юридичних наук
Тарасюка Анатолія Васильовича
на тему:Теоретико-правові основи забезпечення кібербезпеки України"

Міжвідомчим науково-дослідним центром з проблем боротьби з організованою злочинністю при РНБО України (далі – МНДЦ) розглянуто наукові результати дисертаційного дослідження "Теоретико-правові основи забезпечення кібербезпеки України", що подається Тарасюком А. В. для присудження наукового ступеня доктора юридичних наук. Детальне вивчення й аналіз наведених матеріалів у науковій праці дає підстави для формування висновку про актуальність роботи, її наукову новизну, теоретичне та практичне значення результатів дослідження.

Відомості щодо правових основ забезпечення кібербезпеки України використовуються співробітниками МНДЦ під час реалізації завдань з науково-аналітичної діяльності, прогнозування й моніторингу кіберзагроз в Україні.

Керівник Центру
доктор юридичних наук,
заслужений юрист України **Дарія ПРОКОФ'ЄВА-ЯНЧИЛЕНКО**

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки

"5" березня 2021 року

АКТ

впровадження результатів дисертаційного дослідження кандидата юридичних наук Тарасюка Анатолія Васильовича на тему: "Теоретико-правові основи забезпечення кібербезпеки України" в практичну діяльність Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (далі – ДКІБ) СБ України розглянуто наукові результати дисертаційного дослідження Тарасюка А. В. для здобуття наукового ступеня доктора юридичних наук.

Грунтовне вивчення та аналіз наданих матеріалів дає підстави для формування висновку про актуальність дослідження, її наукову новизну, теоретичне та практичне значення результатів наукової праці.

Матеріали дисертаційного дослідження, які стосуються правових засад забезпечення кібербезпеки України використовуються співробітниками ДКІБ СБ України під час реалізації завдань з контррозвідувального захисту інтересів держави у сфері інформаційної безпеки України.

Заступник начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України **Вадим ШВИДКИЙ**

«ЗАТВЕРДЖУЮ»
Директор Науково-дослідного інституту
інформатики і права НАПрН України,
доктор юридичних наук, професор
_____ В. Пилипчук
«16» грудня 2020 року

АКТ
впровадження результатів дисертаційного дослідження Тарасюка А.В. на тему:
«Теоретико-правові основи забезпечення кібербезпеки України»

Комісія у складі: керівника Науково-дослідного центру правового забезпечення інформаційної і національної безпеки НДІІП НАПрН України, доктора юридичних наук, професора Скулиша Є.Д., ученого секретаря кандидата юридичних наук Беланюк М.В.; провідного наукового співробітника, кандидата юридичних наук, старшого дослідника Радзієвської О.Г. склала цей акт про те, що результати дослідження на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07. – адміністративне право і процес; фінансове право; інформаційне право (081 – «Право») Тарасюка Анатолія Васильовича на тему: «*Теоретико-правові основи забезпечення кібербезпеки України*», використані у науковій діяльності Інституту в рамках планових НДР на тему "*Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні*" *(№ державної реєстрації 0116U007745), "Теоретичні та інформаційно-правові засади забезпечення національної безпеки в умовах євроінтеграції України" (№ державної реєстрації 0117U007744)* у частині надання авторських пропозицій щодо концептуальних засад правового забезпечення кібернетичної безпеки України, зокрема щодо розвитку державно-приватного партнерства; удосконалення нормативно-правового забезпечення протидії використанню інтернету в терористичних цілях; захисту національних інтересів України в інформаційній сфері та кіберпросторі; розвитку міжнародно-правих аспектів в контексті євроатлантичної інтеграції України, а також підготовки пропозицій до Стратегії кібербезпеки України (2021 – 2025 роки).

Члени комісії:

доктор юридичних наук, професор _____ Є. Д. Скулиш
кандидат юридичних наук _____ М. В. Беланюк
кандидат юридичних наук, ст. дослідник _____ О. Г. Радзієвська