Науково-дослідний інститут інформатики і права
Національної академії правових наук України

О.Д.Довгань, І.М.Доронін

ЕСКАЛАЦІЯ КІБЕРЗАГРОЗ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ УКРАЇНИ ТА ПРАВОВІ АСПЕКТИ КІБЕРЗАХИСТУ

Монографія

Київ 2018

АртЕк
видавничий дім

УДК 004.9:351.746.1(477)

Рекомендовано Вченою радою НДІІП НАПрН України,
протокол № 8 від 14 грудня 2017р.

Рецензенти :

О.А.Баранов завідувач наукової лабораторія теорії, історії та філософії інформаційного права Науково-дослідного інституту інформатики і права НАПрН України, доктор юридичних наук, старший науковий співробітник.

Н.А. Савінова декан факультету морського права та безпеки Національного університету «Одеська морська академія», доктор юридичних наук, старший науковий співробітник.

Автори монографії:

О.Д.Довгань, д.ю.н., с.н.с. – передмова (у співавторстві), розділ 1, розділ 2, післямова (у співавторстві)., ***І.М.Доронін,*** к.ю.н., доцент – передмова (у співавторстві), розділ 3, розділ 4, післямова (у співавторстві)

Довгань О.Д., Доронін І.М.
Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія/О.Д. Довгань, І.М.Доронін; НАПрН України, НДІІП – К.: Видавничий дім «АртЕк». – 2017. – 107с.

ISBN

У монографії запропоновано вирішення проблемних питань у сфері кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібридних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці.

Книга розрахована як на фахівців у сфері інформаційної та кібернетичної безпеки, так й всіх читачів, що цікавляться даною проблематикою.

ISBN

УДК 004.9:351.746.1(477)

ЗМІСТ

“Безпека завжди є надмірною, але лише до тих пір, поки її стає недостатньо”
(Роббі Сінклер)

ПЕРЕДМОВА

Сучасний період державотворення України відзначений поступовим формуванням комплексних підходів до національної безпеки, серед яких забезпечення інформаційної безпеки, складовою якої с кібербезпека, посідає одне з провідних місць.

На другу половину XX – початок XXI ст. припадають помітні здобутки людства в практичному впровадженні засобів ефективного управління інформацією, передусім, на базі впровадження нових електронних інформаційних технологій. Використання таких технологій, зростання значення інформаційних ресурсів у житті суспільства обумовило визначення характеристики нового, постіндустріального етапу розвитку людства як інформаційного.

Інтенсифікація глобалізаційних процесів у світі стала найважливішою ознакою сучасного розвитку цивілізації. Ці процеси спираються на все нові й нові здобутки науково-технологічного прогресу. З їх допомогою глобалізаційні впливи проникають в усі сфери людського життя. Інформаційна основа глобалізації розвивається, створює умови для розвитку глобального інформаційного простору. Відбувається розвиток процесів інформатизації, пов’язаний із розширенням доступу до інформаційних ресурсів та засобів їх виробництва всіх категорій населення, формування в людей на основі цієї інформації нових світоглядних і всіх інших стереотипів суспільної поведінки, корегування духовно-ціннісних орієнтирів, планів і перспектив.

Із вдосконаленням цих технологій розвиваються методики ведення інформаційних воєн, що вже в наш час нерідко за своїми результатами є більш ефективними від воєн традиційних. Удосконалюється здійснення спеціально орієнтованих впливів на інформаційний простір об’єкта агресії, враження інформаційної основи його діяльності, зростають масштаби кіберзлочинності.

Для України входження в новий етап суспільного розвитку означає безальтернативну ситуацію, за якої лише вдосконалення організації використання інформаційної основи розвитку української нації і держави – об'єднаної системи вітчизняних інформаційних баз, а також розвитку інформаційного виробництва та систем соціальних інформаційних комунікацій, що в сукупності складають ресурсну базу вітчизняного інформаційного простору, – може забезпечити належні позиції у міжнародному співробітництві. Запорукою цього розвитку є організація безпеки національного інформаційного суверенітету для України і як для об'єкта глобальних інформаційних впливів, і як для повноправного суб'єкта міжнародної діяльності, міжнародних інформаційних обмінів має надзвичайно велике значення. Гарантом існування і розвитку національних інформаційних ресурсів в умовах глобальних впливів є ефективна інформаційна безпека нашого суспільства.

Процеси глобалізації, каталізатором яких в останні десятиріччя стала інформатизація на основі електронних технологій, крім свого позитивного значення для розвитку прогресу зумовлюють появу нових викликів і загроз для інформаційної інфраструктури, для національного інформаційного суверенітету, самобутності, самосвідомості, а для цивілізації – багатоваріантних можливостей подальшого розвитку. І тому робота з нейтралізації кіберзагроз як важливої складової забезпечення інформаційної безпеки є запорукою ефективного використання і перспективного розвитку суверенних для кожної держави, нації масивів інформації. Розвиток ефективних інструментів забезпечення інформаційного суверенітету є важливою умовою суспільного розвитку і першочерговим завданням сьогодення.

Питання забезпечення кібернетичної безпеки є надзвичайно важливими для української держави на сучасному етапі, що, насамперед, обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України

є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення кібернетичної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам в інформаційній сфері.

Традиційно питання забезпечення кібербезпеки розглядались у вітчизняній науці насамперед у контексті технічних та організаційних проблем. Водночас ескалація загроз у кіберпросторі, широкомасштабне використання кібератак, а також стрімка зміна характеру суспільних відносин, пов'язаних із забезпеченням кібербезпеки зумовили необхідність вдосконалення інформаційного законодавства і формування спеціальних нормативно-правових актів з забезпечення кібербезпеки. Зазначені законодавчі новації, що мають предметом свого регулювання чітко визначене коло суспільних відносин, повинні знайти своє місце у системі вітчизняного законодавства. Ці питання на сьогодні майже не досліджено у вітчизняній правовій науці, окрім побіжних досліджень присвячених законодавчим новаціям та загальним аспектам інформаційного права. Окрім цього, необхідно проаналізувати співвідношення законодавчих новел із чинною нормативно-правовою базою насамперед у сфері забезпечення національної безпеки.

Ґрунтуючись на вищезазначених ключових моментах, автори монографії намагались насамперед окреслити загальне коло проблемних питань, дослідити ескалацію загроз та характер відповідей на них з боку держави, що здійснюється шляхом правової регламентації.

«Высшее искусство войны –
победить врага без схватки»
(Сунь Цзы, «Искусство войны»).

РОЗДІЛ 1
АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

Глобальний розвиток дистанційних комунікацій, інформаційних технологій та продуктів, ресурсів і послуг призвів до виникнення принципово нових суспільних відносин в інформаційній сфері, економіці й виробництві, став новим джерелом продуктивності праці й активізував процеси формування глобальної економіки. Інформація та інформаційні ресурси стають стратегічним ресурсом і найважливішими чинниками розвитку людини, суспільства і держави. Процеси, що відбуваються в глобальному інформаційному просторі характеризуються такими основними тенденціями та особливостями:

– сучасна інформаційна ера, як свідчать уроки інформаційної агресії проти України, змінює традиційні уявлення про символи могутності й способи досягнення світового панування. Розвиток інформаційної сфери не визнає національно-державних меж і веде до утворення глобальних інформаційних мереж та інформаційних ресурсів, що нав'язують свої стандарти поведінки й мислення;

– змінюється роль і місце військово-політичних механізмів забезпечення безпеки й оборони. Досягнення інформаційної переваги (домінування) забезпечує можливість випереджати суперника у прийнятті військово-політичних рішень і є основою успіху у воєнних діях. Нині світ стоїть на порозі нової сутички за контроль над інформаційним простором і «транспортуванням інформації»;

– з'являється низка проблем, пов'язаних комунікативно-психологічними проблемами в сучасному українському інформаційному просторі, зумовлених поточним військово-політичним становищем України, анексією Криму, антитерористичною операцією в Луганській та

Донецькій областях України, так й майбутніх викликів світовій спільноті – інформаційно-психологічної агресією, руйнуванням системи цінностей і контурів управління держав як основних технологій ведення гібридної війни.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Крім того, застосування країною-агресором по відношенню до України технологій гібридної війни, у першу чергу в інформаційній сфері, сформувало нові виклики та загрози інформаційній безпеці держави. Кібернетичні атаки на інформаційні ресурси держави стали невід'ємним компонентом такої гібридної війни.

Поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

В таких умовах актуальними нині залишаються питання необхідності створення цілісної та узгодженої системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів у інформаційній сфері, розбудови власних спроможностей надійних та достовірних державних комунікацій та створення тісної взаємодії між органами влади, формування інфраструктури національного інформаційного простору з метою створення умов для його інтегрування у світовий інформаційний простір, налагодження комунікаційного процесу між органами влади та споживачами інформації. Тому питання кібербезпеки, у т.ч. її правового забезпечення, у нашій державі має надзвичайно велике значення.

Оскільки, довгий час суспільний добробут і економічна стабільність спиралися на надійну роботу мереж передачі даних і обчислювальних сервісів. На функціонування ключових інформаційних систем загального

користування впливає багато факторів: Інтернет-атаки, порушення, викликані загрозою фізичної розправи, вихід з ладу програмного та апаратного забезпечення, людські помилки та ін. Перераховані явища наочно демонструють, наскільки сучасне суспільство залежить від стабільної роботи інформаційних систем. Аналогічна думку ми знаходимо і в німецькій стратегії кібербезпеки: «Забезпечення доступності кіберпростору, а також цілісності, достовірності та конфіденційності інформації в кіберпросторі стало однією з найважливіших проблем XXI-го століття. Саме тому захист кіберпростору стає головним завданням держави, економіки і суспільства, як на державному, так і на міжнародному рівні»[1].

Кібербезпека все частіше розглядається як стратегічна проблема державного рівня, зачіпає всі верстви суспільства. Державна політика кібербезпеки повинна служити засобом посилення безпеки та надійності інформаційних систем держави.

Все більш широке використання у найрізноманітніших сферах життєдіяльності соціуму комп'ютерних і телекомунікаційних технологій, у тому числі Інтернет-технологій, разом з великою кількістю переваг привнесло також і чималу кількість загроз. Реалізація цих загроз може завдати значної шкоди як на мікро, так і на макрорівні в рамках суверенних держав, а також і в світовому масштабі. Це призвело до розуміння необхідності вирішення проблеми нейтралізації або мінімізації цієї нової сукупності загроз. Одночасно з цим з'являється термін «кібербезпека». Вважається, що він вперше виник у середині 1990-х років, коли уряд Сполучених Штатів Америки став приділяти увагу цьому явищу і розпочав досліджувати цю тему[2].

З того часу проведено велику кількість міжнародних і національних форумів, конференцій, семінарів на різних рівнях, опубліковано багато наукових робіт, присвячених найрізноманітнішим аспектам кібербезпеки. Більшість країн прийняли або розробляють стратегії кібербезпеки

[1] http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

[2] Stubley D. What is Cyber Security? – Режим доступу : //www.7elements.co.uk/resources/blog / what-is-cyber-security

(США, Німеччина, Франція, Канада та багато інших)[3]. Частина з них активно створюють інституційні системи кібербезпеки. До прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (05.10.2017р.) в законодавстві було відсутнє визначення не тільки поняття «кібернетична безпека (кібербезпека)», а й таких понять, як «кібернетичний простір (кіберпростір)», «кібернетична загроза (кіберзагроза)», «кібернетична атака (кібератака)», «кібернетичний захист (кіберзахист)», «кіберзлочинність» тощо, про що правильно зауважував В.П.Шеломенцев[4].

Тоді поставала актуальною проблема визначення змісту терміна "кібернетична безпека". І на це було декілька причин. По-перше, класична причина – дефініція терміна дозволила вичерпно окреслити предмет досліджень і дискусій, коло проблем, які могли б бути при цьому підняті. По-друге, проблема кібербезпеки в силу своєї специфіки існувала, є і залишається глобальною і тому найбільш ефективно може бути вирішена лише за умови об'єднання зусиль найширших кіл міжнародних гравців як на державному рівні, так і на рівні приватних корпорацій і асоціацій. Тому для забезпечення ефективності взаємодії на міжнародному рівні необхідно узгоджене розуміння терміна кібербезпека.

Безсумнівно, ці та ряд інших факторів і визначили необхідність якомога найшвидшої «стандартизації» терміна «кібернетична безпека».

Деякі експерти, у т.ч. і Д. Франсело, вважали, що останнім часом термін cybersecurity все частіше і частіше використовується, але при цьому

---

[3] Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – Режим доступу : //www.publicsafety.gc.ca/cnt/rsrcs/ pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf ; Information systems defence and security: France's strategy. – French Network and Information Security Agency. – 2011. – С. 23. – Режим доступу : //www.gouvernement.fr/sites /default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf; The national strategy to secure cyberspace. – Washington, 2003. – 60 с. – Режим доступу : //www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf; Cyber Security Strategy for Germany. –Berlin : Federal Ministry of the Interior. – 2011. – 15 с. – Режим доступу : //www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_ download.pdf?__blob=publicationFile

[4] Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2012. – № 1. – С. 312-320.

багато керівників служб безпеки, експертів з інформаційної безпеки досі плутаються в тому, коли і як використовувати цей термін[5].

Тому, виходячи з наведеного виникла необхідність проведення аналізу дефініцій терміна "кібернетична безпека", які наведені в деяких національних стратегічних документах. У стратегії Франції, присвяченій питанням кібербезпеки, існує таке визначення: кібербезпека – це бажаний стан інформаційної системи, за якого вона може протистояти подіям з кіберпростору, що можуть поставити під загрозу доступність, цілісність або конфіденційність даних, які зберігаються, обробляються або передаються, і пов'язаних з ними послуг, які ці системи пропонують або роблять доступними[6]. Франція робить акцент на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту.

Насамперед, треба розуміти, що відповідно до цього визначення кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах. Крім того, завдяки включенню до переліку об'єктів, на які можуть діяти які небудь загрози з кіберпростору, послуг інформаційних систем це визначення терміна дозволяє мати на увазі наявність якихось загроз функціональності систем більш високого порядку, до яких в якості складових елементів входять інформаційні системи. Це положення має важливий методологічний зміст у розумінні місця і ролі проблеми кібербезпеки в контексті інших видів безпеки.

У німецькій стратегії під кібербезпекою розуміється деяка сукупність необхідних і відповідних заходів, в результаті реалізації яких досягається мінімізація ризиків[7]. В ній стверджується, що кібербезпека

---

[5] Franscella J. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term / J. Franscella. – Режим доступу : //www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

[6] Information systems defence and security: France's strategy. – French Network and Information Security Agency. – 2011. – С. 23. – Режим доступу : //www.gouvernement.fr/sites /default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf

7 Cyber Security Strategy for Germany. –Berlin : Federal Ministry of the Interior. – 2011. – 15 с. – Режим доступу: //www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

повинна базуватися на комплексному підході. Це досить прагматична точка зору, яка дозволяє розробляти практичні кроки щодо забезпечення кібербезпеки, проте вона не надає достатніх методологічних підстав для проектування та оцінки систем, що забезпечують цю безпеку. Про зазначене побічно свідчить зміст десяти стратегічних напрямів у стратегії забезпечення кібербезпеки, оголошених федеральним урядом Німеччини. Стратегія Німеччини закладає основу для безпеки критично важливих інформаційних систем. Німеччина зосереджена на запобіганні і кримінальному переслідуванні кібератак, а також на запобігання виходу з ладу ІТ-обладнання, викликаного випадковими чинниками. Особливо останнє стосується критично важливих інформаційних систем. У стратегії аналізується, чи потрібно проводити додаткові дії (і якщо так, то де саме) щодо захисту ІТ-систем шляхом надання основних функцій безпеки, сертифікованих державою, а також підтримкою малого і середнього бізнесу за допомогою створення нової робочої групи.

У Канаді стверджують, що з метою забезпечення найсучаснішого використання кіберпростору, який є стратегічним активом, необхідно передбачати і протистояти кіберзагрозам, що виникають[8]. У канадській стратегії кібербезпеки не міститься чіткого визначення того, що являє собою кібербезпека. Відповідно до цього документа під кібербезпекою можна розуміти захист кіберсистем від шкідливого неправильного використання та від інших деструктивних атак. З іншого боку, надано досить докладне визначення кібератаки, а кібербезпека – це засіб захисту від цих загроз.

Кібератаки включають ненавмисні або несанкціонований доступ, використання, маніпуляції, переривання або знищення (через електронні засоби) електронної інформації та/або електронної та фізичної інфраструктури, що використовується для обробки, зв'язку, та/або баз даних. При цьому рівень кібербезпеки визначається рівнем шкоди, що може бути завданий від кібератаки.

[8] Canada's Cyber Security Strategy: For a stronger and more prosperous Canada. – Her Majesty the Queen in Right of Canada, 2010. – 14 с. – Режим доступу : //www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

У цілому, канадська стратегія все ж таки розглядає основну шкоду від реалізації кіберзагроз як збиток, який можуть мати системи життєзабезпечення та підтримки діяльності всієї країни, бізнесу та окремого громадянина. Вона в цілому передбачає три напрями: захист урядових систем *(встановлення чітких ролей і відповідальності, посилення безпеки кіберсистем федерального рівня і підвищення інформованості уряду в області кібербезпеки)*; співпраця з метою захисту ключових кіберсистем, що знаходяться за межами федерального Уряду *(ряд партнерських проектів державного рівня із залученням приватного сектора і секторів критичних інфраструктур)* та забезпечення безпеки канадських громадян в онлайн-середовищі *(боротьба з кіберзлочинністю і захист канадських громадян в онлайн-середовищі. Також порушується проблема персональних даних)*.

Одна із останніх прийнятих за часом національних стратегій кібербезпеки (Турецька Республіка) містить наступне визначення: кібербезпека – захист інформаційних систем, що входять до складу кіберпростору, від нападів, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в цьому просторі, виявлення та протидія атакам і кіберінцидентам[9]. Водночас, під кіберпростором розуміється середовище, що складається з інформаційних систем, розподілених по всьому світу, в тому числі мереж, що з'єднують ці системи. Національний кіберпростір визначається як простір, який складається з інформаційних систем суб'єктів, що перебувають під юрисдикцією Турецької Республіки.

У Нідерландах також приділяють велику увагу наявності загроз інформаційній інфраструктурі в умовах широкого застосування цифрових (комп'ютерних) технологій. Національним координатором з безпеки та боротьби з тероризмом в 2013 році була опублікована Національна стратегія кібербезпеки. На думку авторів стратегії, кібербезпека – це сукупність

[9] National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. – С. 47. – Режим доступу : //www.ccdcoe.org/strategies/TUR_CyberSecurity.pdf

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[10]. До збоїв стратегія відносить зниження надійності ІКТ, обмеження доступності та порушення конфіденційності та/або цілісності інформації, що зберігається в системах ІКТ. Таке тлумачення робить дуже складним вирішення проблеми визначення критеріїв забезпечення кібербезпеки.

Однак у стратегії нідерландів зроблено вельми важливий в методологічному аспекті висновок – кібербезпека може бути досягнута тільки в системній кореляції з вирішенням проблем захисту та забезпечення основних прав, цінностей і соціально-економічних вигод членів соціуму.

Політикою кібербезпеки австралійського уряду є підтримка безпечної, стійкої і надійної роботи електронного операційного середовища, яке підтримує національну безпеку Австралії та максимізує переваги цифрової економіки[11]. В опублікованій у 2009 році Стратегії під кібербезпекою розуміється забезпечення доступності, цілісності та конфіденційності ІКТ Австралії, а також захист людей, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і від використання ІКТ для цілей сексуальної експлуатації [10].

В українському законопроекті щодо кібернетичної безпеки України було запропоновано свій варіант визначення кібербезпеки, під якою розумілося стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі[12]. При цьому в законопроекті кіберпростір – середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами

---

[10] Национальная стратегия кибербезопасности (NCSS). От понимания к возможности. – Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. – Режим доступу : //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2 Engelseversie

[11] Cyber security strategy. – Commonwealth of Australia: Australian Government, 2009. – Режим доступу : //www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber %20 Security %20Strategy%20-%20for%20website.pdf

[12] Про внесення змін до Закону України "Про основи національної безпеки України": проект Закону України щодо кібернетичної безпеки України від 07.03.13 р. № 2483. – Режим доступу : //www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998

інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Це визначення має дуже низький методологічний потенціал і не дозволяє конкретизувати особливості кібербезпеки. Більше того, абсолютно необґрунтовано до кібербезпеки віднесені проблеми функціонування інформаційних систем в загальному сенсі, внаслідок чого до проблематики кібербезпеки можуть бути віднесені телебачення і радіо, а також навіть бібліотеки та архіви. Майже таким залишилося визначення «кібербезпеки» і в проекті Закону України «Про основні засади забезпечення кібербезпеки України»[13]. Зокрема, в ньому кібернетична безпека (далі – кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кібернетичному просторі.

Таким чином, визначення терміну «кібернетичної безпеки» ґрунтувалося на визначенні терміну «кібернетичний простір» під яким розумілося «середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем». Виходячи із наданого визначення під середовищем можна розуміти сукупність інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем.

Натомість, виникає питання щодо ідентифікації «життєво важливих інтересів людини і громадянина, суспільства та держави» в цьому середовищі. На нашу думку, в такому середовищі не відбуваються і не можуть в принципі відбуватись ніякі суспільні відносини між суб'єктами (людина, громадянин, суспільство, держава). Таким чином, на наше переконання та думку більшості фахівців у цій сфері, а також експертів[14] невдале визначення терміну «кібернетична безпека» логічно призводило до не зовсім неправильного визначення предмета зазначеного акту, його цілей, а, саме головне, до неправильного визначення комплексу заходів щодо його впровадження.

---

[13] Проект Закону України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] . – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657

[14] Аналітична записка щодо Законопроекту «Про основні засади забезпечення кібербезпеки України» http://inau.vds.colocall.com/52.3253.0.0.1.0.phtml

З урахуванням того, що проблема кібербезпеки має глобальний характер, вельми цікавою видається позиція міжнародних організацій. Так, Міжнародний телекомунікаційний союз (International Telecommunication Union, ITU) у своїй Рекомендації тлумачит визначення: кібербезпека – це набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача[15]. При цьому ресурси організації та користувача включають під'єднанні комп'ютерні пристрої, персонал, інфраструктуру, додатки, послуги, системи телекомунікацій і всю сукупність переданої та/або збереженої інформації в кіберсередовищі, а мета кібербезпеки полягає в спробі досягнення і збереження властивостей безпеки ресурсів організації або користувача, спрямованих проти відповідних загроз безпеки в кіберсередовищі. До загальних завдань забезпечення безпеки віднесено: доступність; цілісність, яка може включати автентичність і безвідмовність; конфіденційність.

У Європейському Союзі у зв'язку з розумінням важливості проблеми кібербезпеки ще у 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки[16]. У подальшому це Агентство у 2012 році оприлюднило огляд «Національні стратегії кібербезпеки. Практичний посібник з розвитку та виконання»[17]. Щодо визначення терміна «кібербезпека» в цьому огляді констатовано факт, що в національних стратегіях не існує загальноприйнятого та однозначного визначення кібербезпеки.

---

[15] Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : МСЭ, 2009. – С. 55. – Режим доступу : //www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru

[16] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) // Official Journal L 077, 13/03/2004P. 0001-0011. – Режим доступу : //www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[17] National Cyber Security Strategies. Practical Guide on Development and Execution. –ENISA, 2012. – Режим доступу : //www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

Таким чином, можна стверджувати, що на рівні національних та міжнародних стратегічних документів визначення кібербезпеки значно відрізняються. Тобто є відмінності до змісту відповідних стратегій та планів дій із забезпечення кібербезпеки. Однак транскордонний характер цієї проблеми настійливо диктує необхідність координації зусиль як на національному, так і на міжнародному рівні. Передусім, мова йде про осмислення суті кіберзагроз, змісту заходів щодо забезпечення кібербезпеки, чітке визначення цілей стратегії і власне визначення змісту самого терміна «кібербезпека».

З урахуванням того, що термін «кібербезпека» отримав значного поширення не тільки в середовищі фахівців, а й у різних міжнародних і національних документах, пропонується не розгортати дискусію власне про назву самого терміна, незважаючи на те, що вона викликає обґрунтовані нарікання у багатьох фахівців.

Оскільки, деякі західні фахівці запевняють, що слово «cyber» пов'язане з використанням інформаційних технологій і комп'ютерів[18]. Цю ж позицію займає і науковець[19], який обґрунтовуючи необхідність застосування в правовій науці терміна «кібернетичний простір», розуміє під ним сукупність суспільних відносин, що виникають в процесі використання функціонуючої електронної комп'ютерної мережі, що складається з приводу інформації, яка обробляється за допомогою ЕОМ, і послуг інформаційного характеру, що надаються за допомогою ЕОМ та засобів зв'язку комп'ютерної мережі.

З проведеного аналізу можна зазначити, що практично всі національні стратегії щодо забезпечення кібербезпеки і переважна більшість експертів пов'язують проблематику кібербезпеки саме з використанням у процесі людської діяльності комп'ютерних систем і телекомунікаційних мереж (до останніх належить і мережа Інтернет).

---

[18] Stubley D. What is Cyber Security? – Режим доступу : //www.7elements.co.uk/resources/blog / what-is-cyber-security

[19] Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : автореф. дис. на соискание ученой степени канд. юрид. наук : спец. 12.00.01 / Д.В. Грибанов. – Екатеринбург, 2003. – 23 с. – Режим доступу : http://law.edu.ru/book/book.asp?bookID=126348

Дійсно, саме з початку використання комп'ютерних технологій, особливо у сукупності із телекомунікаційними мережами, виникає особливий клас загроз інформаційній безпеці. Ситуація набуває ще більшого загострення разом з поширенням використання мережі Інтернет. Але широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів. Це пояснюється значним коефіцієнтом «корисної» дії цих загроз, тому що обсяг ресурсів, що витрачаються на реалізацію загроз, є набагато меншим, ніж результати, що отримуються.

Заслуговує на увагу й інша точка зору, яку висловив автор статті[20] таким чином: використання термінів, похідних від терміна «кібернетика», наприклад, таких як «кібернетична атака», «кібернетична безпека», «кіберпростір», «кіберсфері», «кіберзлочинність», «кібервійна», «кібероборони», є виправданим у разі опису явищ або фактів, безпосередньо пов'язаних із системами і процесами управління.

Дійсно, процеси управління нерозривно пов'язані з інформаційними процесами як у процесі підготовки управлінських рішень, так і безпосередньо у процесі управління. Сучасні системи управління, особливо великими територіально-розподіленими соціотехнічними системами (системи управління енергетичною інфраструктурою, повітряним і залізничним рухом, банківськими та фінансовими системами, великими промислово-виробничими комплексами тощо), неможливо уявити без використання комп'ютерних систем і телекомунікаційних мереж. Тому розуміння кібербезпеки як проблеми, пов'язаної із системами управління, не суперечить тим поглядам, які висловлюють більшість експертів за умови того, що ця проблема буде розумітися як часткова проблема у всій проблематиці кібербезпеки.

На підставі проведеного аналізу можливо зробити декілька узагальнюючих висновків. Автори цілком підтримують і поділяють

[20] Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право. – 2012. – № 1. – Режим доступу : http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099

думку Баранова О.А.[21]. Зокрема, можна зробити перший висновок про те, що основною кваліфікуючою ознакою віднесення до проблематики кібербезпеки є обов'язкова умова – використання комп'ютерних систем і телекомунікаційних мереж.

Українські дослідники пропонують своє бачення терміна кібербезпеки. Так деякі з них вважають, що в контексті нормативно-правового розуміння національної та інформаційної безпеки кібербезпека може визначатися як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем[22]. Цим визначенням автори визначають в якості об'єкта загроз – національні інтереси у сфері функціонування інформаційно-телекомунікаційних систем, що значно звужує поле можливих життєво важливих інтересів людини і громадянина, суспільства і держави. Крім того, пропозиція використовувати в якості критерію захищеності життєво важливих інтересів людини і громадянина, суспільства і держави критерій «стабільний розвиток суспільства» не дозволяє сформувати методологічну основу для оцінки рівня такої захищеності, оскільки важко дати кількісні оцінки «стабільного розвитку».

В.Н. Фурашев визначає кібербезпеку як стан здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації[23].

Методологічно важливим для визначення обсягу юрисдикції поняття кібербезпеки є знання об'єкта можливих загроз, а також видів і типів

[21] Баранов О.А. Про тлумачення та визначення поняття "кібербезпека"/О.А.Баранов// Правова інформатика. – 2(42). – 2014 [Електронний ресурс]. – режим доступу: http://ippi.org.ua/sites/default/files/14boavpk.pdf

[22] Мельник С.В.До проблеми формування понятійно-термінологічного апарату кібербезпеки/ С.В.Мельник, О.О.Тихомиров, О.С.Лєнков // : зб. матер. наук.-практ. конф. [Актуальні проблеми управління інформаційною безпекою держави], (Київ, 22 березня 2011 р.). – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 43-48.

[23] Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності/ В.М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162-169.

можливого збитку. Ці знання і розуміння мають високу практичну цінність, оскільки саме від них залежить зміст стратегій кібербезпеки, охоплення об'єктів, які підпадають під заходи щодо забезпечення кібербезпеки, рівень і перелік інституцій та органів, склад і обсяги ресурсів, які повинні бути при цьому задіяні.

Виходячи з цільового призначення систем, що містять в якості складових комп'ютерні системи та телекомунікаційні мережі, можна зробити висновок про те, що кіберзагрози насамперед спрямовані на порушення обігу інформації. При цьому мова може йти як про фундаментальні системні загрози, пов'язані з порушенням власне обігу інформації на будь-якому з його етапів – створенні, поширенні, використанні, зберіганні і знищенні інформації, так і про загрози, пов'язані з недостовірністю, несвоєчасністю і неповнотою інформації. Крім того, до цього класу загроз слід віднести загрози, пов'язані з несанкціонованим використанням та поширенням інформації, порушенням її цілісності та конфіденційності.

Таким чином, другий висновок полягає в тому, що проблематика кібербезпеки має відношення до обігу інформації, зокрема, до забезпечення суб'єктів інформаційних відносин достовірною, своєчасною та повною інформацією, а також до недопущення несанкціонованого використання і поширення інформації, порушення її цілісності та конфіденційності.

Широке використання в останні роки комп'ютерних систем і телекомунікаційних мереж для створення та розповсюдження інформації істотно підвищило ефективність цих процесів, а отже, і ефективність інформаційного впливу. Однак поряд з позитивом комп'ютерні системи та телекомунікаційні мережі також дозволили істотно підвищити ефективність негативного інформаційного впливу. Не проводячи детальний аналіз видів і типів таких впливів, скажемо тільки, що левова частка з них пов'язана з використанням інтернет-технологій. Тому протидія негативному інформаційному впливу іноді здійснюється не на контентному рівні, а на технологічному. Тобто у цьому випадку протидія може бути віднесена до заходів із кібербезпеки. Тому логічним для цієї

ситуації буде третій висновок, який полягає в тому, що з проблемою кібербезпеки пов'язана проблема нейтралізації негативних інформаційних впливів на технологічному рівні.

Непоодинокі випадки, коли функціонування соціальних і соціотехнічних систем повністю базується на використанні якихось технічних комплексів комп'ютерних систем і телекомунікаційних мереж. Тому досягнення цілей функціонування цих соціальних і соціотехнічних систем залежить від якості, надійності та стабільності роботи цих комплексів. Або іншими словами, порушення функціонування комп'ютерних систем і телекомунікаційних мереж може призвести до погіршення або навіть припинення роботи соціальних і соціотехнічних систем, елементами яких вони є. А це означає, що такі комплекси (комп'ютерні системи та телекомунікаційні мережі) зобов'язані належним чином проектуватися, будуватися, здаватися в експлуатацію, експлуатуватися, супроводжуватися проектантами і виробниками тощо. Недоліки в нормативно-правовому та нормативно-технічному забезпеченні цих процесів, прорахунки в їх організації та реалізації, які можуть призвести до порушення функціонування комп'ютерних систем і телекомунікаційних мереж у процесі їх експлуатації, становлять окрему групу кіберзагроз.

Крім того, при створенні соціальних та соціотехнічних систем, елементи яких знаходяться на різних територіях і на значній відстані, досить важливим фактором є забезпечення оптимального проектування топології територіально розподілених комп'ютерних систем та телекомунікаційних мереж з метою забезпечення їх інфраструктурної стійкості та достатності. Недотримання або невиконання вимог інфраструктурної стійкості та достатності територіально розподілених комп'ютерних систем та телекомунікаційних мереж може призвести до погіршення або навіть припинення роботи соціальних і соціотехнічних систем, елементами яких вони є. таким чином випливає четвертий висновок – серед проблем кібербезпеки є проблема забезпечення інфраструктурної безпеки соціальних та соціотехнічних систем, що використовують комп'ютерні системи та телекомунікаційні мережі, або іншими словами, проблема, пов'язана

з завданням можливого збитку через негативні наслідки використання інформаційних комп'ютерних технологій[24].

Деякі експерти при дослідженні об'єктів кібербезпеки не уникають спокуси перерахувати конкретні види або навіть типи технічних систем, що містять комп'ютерні та телекомунікаційні технології[25]. Але тоді в якості збитку доведеться розглядати тільки лише збої у функціонуванні цих технічних систем. Насправді технічні системи є лише складовими елементами систем більш високого порядку – соціальних та соціотехнічних систем і призначені для забезпечення їх функціонування чи діяльності. Прикладом можуть служити банківські автоматизовані системи «банк-банк» або «банк – клієнт», які являють собою сукупність комп'ютерних і телекомунікаційних технологій. Збої у функціонуванні цих автоматизованих систем призводять, насамперед, до порушення інформаційного обміну між банками та їх клієнтами. А вже системним збитком для банків є зрив фінансового обороту, для якого інформаційний обмін є необхідною умовою.

Наведений приклад, а також маса інших, свідчать про те, що, врешті-решт, всі можливі види і типи збитку, які можуть мати місце в результаті порушення кібербезпеки, зводяться до збитку, який безпосередньо несуть соціальні та соціотехнічні системи. Або для загального випадку можна стверджувати, що порушення кібербезпеки призводить до зниження рівня захищеності життєво важливих інтересів людини, суспільства і держави. Ця обставина знайшла відображення в багатьох національних стратегіях кібербезпеки або в частині, де надається обґрунтування, або в частині, в якій описуються напрями проведення заходів для забезпечення кібербезпеки. Таким чином, п'ятим висновком є: базова мета забезпечення кібербезпеки – це забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави.

---

[24] Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.

[25] 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.

Кібербезпека не є річчю в собі, замкнутої тільки на комп'ютерних системах та/або телекомунікаційних мережах. Із системних позицій заходи щодо забезпечення кібербезпеки насамперед спрямовані на збереження якості функціонування соціальних і соціотехнічних систем, до складу яких входять відповідні комп'ютерні системи та телекомунікаційні мережі. Тому основними критеріями ефективності заходів щодо забезпечення кібербезпеки повинні бути критерії, що базуються на оцінці якості функціонування соціальних і соціотехнічних систем. Наприклад, якщо реалізація кіберзагроз навіть і призводить до порушення роботи комп'ютерних систем, але це майже не позначається на якості функціонування відповідної соціальної або соціотехнічної системи, гострота проблеми забезпечення кібербезпеки різко падає. Отже, шостий висновок – проблема оцінки стану кібербезпеки повинна передусім розглядатися в нерозривному зв'язку з оцінкою можливих чи завданих збитків соціальним або соціотехнічним системам як системам більш високого порядку.

Похідним від цього останнього висновку є методологія визначення об'єктів критичної інфраструктури в контексті кібербезпеки. До об'єктів критичної інфраструктури в загальному випадку слід відносити ті інфраструктурні об'єкти, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави. А для випадку кібербезпеки: об'єкти критичної інфраструктури – це інфраструктурні об'єкти, що мають у своєму складі комп'ютерні системи та/або телекомунікаційні мережі, порушення функціонування яких призводить або може призвести до збитку для життєво важливих інтересів суспільства і держави.

В роботі[26] було обгрунтовано дефініцію терміна «інформаційна безпека», яка знайшла в подальшому законодавче закріплення у Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки». Інформаційна безпека – стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого запобігається

[26] Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.

завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації[27].

На основі зіставлення результатів аналізу проблем визначення терміна «кібербезпека», що були отримані вище, та законодавчого визначення терміна «інформаційна безпека» можливо зробити висновок про те, що кібербезпека – це окремий випадок інформаційної безпеки, поява якого обумовлена використанням комп'ютерних систем та/або телекомунікаційних мереж.

В такому випадку цікавим, на наш погляд, є надане визначення: кібербезпека – інформаційна безпека в умовах використання комп'ютерних систем та/або телекомунікаційних мереж. Або його розгорнуте визначення: кібербезпека – це такий 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[28]. Таким чином, надане визначення кібербезпеки засноване на діалектичному зв'язку категорій загального і одиничного у сфері інформаційної безпеки. Кібербезпека розглянута як одиничне стосовно інформаційної безпеки, яка виступає в якості загального. Крім того, запропонований підхід дозволяє розглядати проблеми кібербезпеки з позицій відносно напрацьованої теоретичної та практичної бази інформаційної безпеки та створювати несуперечливі моделі в цих сферах.

---

[27] Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102

[28] Баранов О.А. Про тлумачення та визначення поняття "кібербезпека"/О.А.Баранов// Правова інформатика. – 2(42). – 2014 [Електронний ресурс]. – режим доступу: http://ippi.org.ua/sites/default/files/14boavpk.pdf

Але законодавець в Законі України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 року[29] надає дещо інше визначення: кібербезпека – 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.

У цілому Закон створює засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами державного і приватного секторів та громадянського суспільства.

Ним визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження і обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки.

Документ також визначає основні об'єкти кіберзахисту, які в сукупності складають критичну інфраструктуру країни, принципи забезпечення кібербезпеки та національна система кібербезпеки. Прийняття цього Закону дозволяє впровадити комплексний підхід під егідою держави і у тісному співробітництві з приватним сектором і громадянським суспільством та створює умови для забезпечення кіберзахисту критично важливих інфраструктурних об'єктів України.

Крім цього, у законі йдеться про так звану «державно-приватну взаємодію» у сфері кібербезпеки. Документ зобов'язує держустанови, підприємства і навіть окремих громадян сприяти органам держбезпеки, повідомляючи, наприклад, про кіберзагрози.

[29] Про основні засади забезпечення кібербезпеки України: закон України [Електронний ресурс]. – режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19

Важливим у цьому законі є й те, що він запроваджує відповідальність, у тому числі кримінальну, за злочини, вчинені саме в кіберпросторі. І як раніше згадували у законі також тлумачаться самі поняття «кібербезпеки», «кіберзахисту» та «кіберзлочинності», які вже понад десятиліття використовують у юридичній практиці, у тому числі у зв'язку із вчиненими в мережі злочинами, але які досі не були ніде закріплені в документах.

Експерти загалом схвально відгукуються про його ухвалення – як базового документу, хоча у ньому є ціла низка недопрацювань. Водночас на думку аналітиків, ще завчасно говорити про ефективність цього закону для підвищення рівня кібербезпеки.

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.

Таким чином, питання кіберзахисту повинне набути системного характеру на державному рівні. Можливо багато говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому і приватного сектора; встановлення контролю над кіберзброєю, а також посиленням охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та вдосконалення освітніх напрямів підготовки фахівців цієї сфери діяльності тощо. Однак без системного та комплексного підходу всі зазначені підходи не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень.

РОЗДІЛ 2
ТРАНСФОРМАЦІЯ КІБЕРЗАГРОЗ В УМОВАХ ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

Кібербезпека все частіше розглядається, як стратегічна проблема державного рівня, яка охоплює всі верстви суспільства. Не виключенням є і нинішній етап розвитку України, як і багатьох держав світу, який характеризується максимальною інформатизацією всіх сфер її життєдіяльності. В той же час перенесення багатьох процесів, зокрема й тих, що стосуються критичної інфраструктури, у т.з. кіберпростір, несе в собі разом з позитивними, також й негативні наслідки: уразливість цих процесів перед численними кіберзагрозами. Забезпечення безпеки у кіберпросторі є на сьогодні актуальним для нашої держави з огляду на те, що проти неї ведеться гібридна війна, одним з проявів якої є кібератаки на українські державні органи та установи, а також об'єкти критичної інфраструктури. З огляду на це, державі слід приділяти питанню кібербезпеки максимальну увагу.

Не дивлячись на те, що розвиток технологій в сучасному світі не тільки дозволяє людству вирішувати безліч проблем його прогресивної еволюції, але одночасно з цим породжує нові виклики і загрози в області віртуального кібернетичного простору, яке в більшості випадків дослідники називають інформаційним і якими в більшості випадків віддається перевага терміну «інформаційна безпека». Про такі підходи нами зазначалося у попередньому розділі. Однак відмінності між кібернетичної безпекою і інформаційною безпекою, на думку авторів, цілком очевидні.

Аналіз робіт вітчизняних і зарубіжних дослідників дозволяє зробити висновок про те, що в зміст інформаційної безпеки включаються в тому числі аспекти забезпечення інформаційної безпеки Інтернету, що важливо як в цілому для держави *(боротьба з інформаційними загрозами, кіберзлочинами, в тому числі кібертероризмом)*, так і для кожної людини (проблема захисту персональних даних, кредитних карт і т. д.).

З огляду на розкриття суті питання, що розглядається в розділі, нам імпонує запропоноване автором[30] розширене визначення кіберпростору, під яким розуміється особливий інформаційний простір зі специфічними просторово-часовими характеристиками (транскордонність, екстериторіальність, децентралізованість, розгалуженість, багатоканальність, віртуальність, імітаційність та ін..); виник і функціонує за допомогою комп'ютерних та інших електронних пристроїв (мобільних засобів зв'язку, ігрових консолей, телевізійних пристроїв, супутників і т. д.), на базі інформаційно-телекомунікаційних мереж, переважно мережі Інтернет, в зв'язку з чим, як правило, володіє параметрами глобального інформаційного обсягу, яке виконує функції комунікації, розміщення і використання інформації, надання інформаційних та інших соціально значущих послуг, взаємодії інститутів державної влади, громадянського суспільства і окремої особистості, що є моделюючим фактором впливу на індивідуальну, групову і масову свідомість, соціально-політичну, економічну, духовну (культурну, релігійну, ідеологічну, наукову, освітню) і інші сфери життєдіяльності соціуму. Виходячи з цього визначення, кіберпростір може бути і об'єктом захисту (інформаційних ресурсів, апаратних і програмних засобів зв'язку і т. д.), і одночасно, при певних негативних умовах, джерелом загроз іншим об'єктам національної безпеки.

Розглянемо загрози, що виникають в кібернетичному просторі, традиційно класифікуючи їх за характером спрямованості: на внутрішні (мають джерелом свого зародження – простір Укрнета, або український сегмент глобальної інформаційно-комунікаційної мережі) і зовнішні (виникнення яких, перш за все, обумовлюється транскордонною мережою Інтернет).

Зауважимо, що, маючи один і той же характер, загрози можуть одночасно бути віднесені до внутрішніх, і до зовнішніх джерел, як, наприклад, хакерські атаки і їх підвид – кібертероризм, пропаганда соціальної, расової, національної, релігійної або мовної переваги, комп'ютерні шахрайства

[30] Тонконогов А. В. Кибернетическая безопасность: понятие и сущность феномена // Правовой Центр – «Правый Берег» (http://www.center-bereg.ru/h69.html).

і тощо. Інтернет, зважаючи на свою екстериторіальність, нівелює поняття джерела загрози, так як дозволяє реєструвати доменні імена сайту в одній країні, а поширювати інформацію (за рахунок дії пошукових систем, посилань, запитів і т. д.) – в іншій, в зв'язку з чим досить складно встановити винну в поширенні шкідливої інформації особи. Розмірковуючи про зовнішні загрози (в чистому вигляді) кібернетичної безпеки, перш за все необхідно виходити з того, що в даний час інформаційна сфера є справжній театр бойових дій[31]. Особливо це актуально, коли використання нових інформаційно-пропагандистських технологій призводить до досить швидкої зміни режимів в різних країнах.

Поразка в інформаційній, в тому числі кібернетичній, війні може неминуче призвести до розпаду будь-якої держави. У сучасних умовах багато важливих систем промислового і оборонного сектора економіки, наприклад система управління повітряним сполученням, підприємствами енергетичної й атомної галузі та електромережі, що працюють на основі інформаційно-комунікаційних технологій, становлять потенційні об'єкти ризику через уразливості їх для вторгнення ззовні. Таким чином, до зовнішніх загроз кібернетичному просторі відносяться і власне хакерські атаки, що здійснюються з територій інших держав, які мають на меті порушення роботи комп'ютерних систем, розкрадання інформації конфіденційного характеру та ін.

Як джерело загрози кібернетичної і в цілому національної безпеки України і інших країн слід розглядати і фактичне регулювання США мережі Інтернет. Це обумовлено розташуванням на її території організацій (зокрема, інтернет-корпорації ICANN), що забезпечують управління доменними іменами верхнього рівня, тобто практично всім адресним простором DNS (доменної системи імен) у мережі Інтернет, що дозволяє називати США генеральним «утримувачем» доступу в мережу Інтернет.

До внутрішніх загроз, багато з яких можна вважати, одночасно і зовнішніми загрозами кібернетичній безпеці, можна віднести наступні:

[31] Тонконогов А. В. Кибернетическая безопасность: понятие и сущность феномена // Правовой Центр – «Правый Берег» (http://www.center-bereg.ru/h69.html).

– технічна залежність інформаційної інфраструктури України від іноземних технологій, включаючи безпосередньо мережу Інтернет;

– низький рівень захищеності інформаційно-телекомунікаційних систем від несанкціонованого доступу (під цим мається на увазі і вразливість програмно-апаратного обладнання, і наявність людського фактора, що виражається у витоку важливої інформації про паролі і коди доступу);

– низька якість нормативно-правових актів, що розробляються та їх невідповідність нинішній ситуації в інформаційній сфері й в цілому відсутність послідовної державної політики в галузі забезпечення кібернетичної безпеки;

– низький рівень комп'ютерної грамотності у населення та знань в області інформаційно-комунікаційних технологій;

– відсутність кваліфікованих фахівців, що володіють необхідними професійними якостями, відповідних організаційно-функціональних структур, здатних на підставі ввірених державою повноважень здійснювати ефективну протидію розміщенню в кібернетичному просторі незаконної і небажаної (шкідливої) інформації;

– відсутність механізмів контролю та відповідальності учасників медіаспівтовариства мережі Інтернет, реєстраторів доменних імен, провайдерів, що функціонують в Інтернеті засобів масової інформації.

Нагальним залишається питання про правову неврегульованість простору Інтернет, про відсутність в арсеналі держави правових норм, що сприяють підвищенню відповідальності провайдерів і власників сайтів за розміщення недостовірної та завідомо шкідливої інформації, а також закріплюють механізм впливу на недобросовісних суб'єктів інформаційних правовідносин в кібернетичному просторі.

Кіберзлочинність – це наступний вид загроз, явище, характерне як для України окремо, так і для всього світового соціуму в цілому. У Європейській конвенції про кіберзлочинність[32] зроблено спробу нормативно закріпити і систематизувати правопорушення в кібернетичному

[32] Конвенція про кіберзлочинність [Електронний ресурс]. – режим доступу: http://zakon0.rada.gov.ua/laws/show/994_575

просторі за такими видами: фальсифікація з використанням комп'ютерних технологій; шахрайство з використанням комп'ютерних технологій; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторських та суміжних прав.

Розмірковуючи про спробу регламентувати і систематизувати види правопорушень, пов'язаних з використанням комп'ютерних засобів, мається на увазі, що за межами Конвенції про кіберзлочинність залишаються дії, які кваліфікуються як кримінальні, але вочевидь заподіюють в тій чи іншій мірі збиток інформаційним відносинам і їх суб'єктам в кібернетичному просторі. До них можна віднести: кіберсквотерство (придбання доменних імен з метою їх подальшого перепродажу або розміщення реклами); розсилку спаму; створення спеціальних наборів та інструментів для проведення хакерських атак, пошуку і використання вразливостей в інформаційних системах (при цьому більшість таких засобів не є шкідливим програмним забезпеченням).

Новим соціальним явищем, що вимагає детального правового опрацювання, стає кібердифамація (від латинського diffamatio – паплюжити), тобто поширення за допомогою засобів масової інформації в мережі Інтернет неправдивих відомостей, що ганьблять честь, гідність, ділову репутацію, добре ім'я. Від даного роду посягань добропорядні громадяни та держава фактично не захищені.

Наступна загроза кібернетичній безпеці: наявність правових колізій та прогалин в законодавстві, що тягне за собою несвоєчасне і неадекватне реагування правозастосовника на факти заподіяння шкоди інформації, інформаційно-телекомунікаційним мережам, репутації громадян та ін.

Слід також вказати і на ще одну важливу обставину. А саме, прив'язка поняття «кіберзлочинність» тільки до сфери функціонування комп'ютерів істотно збіднює дане поняття і не дозволяє оцінювати в якості кіберзлочину правопорушення, вчинені з використанням, наприклад, мобільних засобів зв'язку, зокрема, виражені у формі поширення дитячої порнографії за допомогою стільникового зв'язку і шахрайства з оплатою послуг зв'язку.

Тому автори поділяють думку тих дослідників, які вважають, що кіберзлочини включають в себе «не тільки діяння, вчинені в глобальній

мережі Інтернет, але і в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, техніка можуть виступати предметом злочинних посягань, середовищем, в якій вчинено правопорушення, і засобом або знаряддям злочину»[33]. Цей підхід є більш вдалим, оскільки більше відповідає суті кібернетичного простору, утвореного, як зазначалося раніше, на базі всіх можливих (локальних, глобальних) інформаційно-телекомунікаційних мереж, серед яких мережа Інтернет є переважною.

Таким чином, кібернетичні злочини по суті є правопорушеннями економічного, політичного і етнодискримінаційного характеру, що виражаються у формі незаконної політичної боротьби (кібертероризм, кіберекстремізм), здійснення шахрайських операцій у всіх сферах суспільної життєдіяльності, в тому числі у вигляді розміщення в Інтернеті, інших засобах електронної комунікації матеріалів, що пропагують радикальні ідеї національної та іншої переваги; інформації, що має свідомо шкідливий характер і стосується незаконної торгівлі зброєю, вибуховими речовинами, вибуховими пристроями, їх виготовлення; торгівлі людьми, людськими органами, наркотичними засобами, психотропними сильнодіючими речовинами, рецептами щодо їх виробництва.

У даному контексті в якості нових видів можливих внутрішніх і зовнішніх загроз в кібернетичної сфері можна виокремити: ініціювання кібернетичних революцій; поширення електронних вірусів, спаму, неліцензійних софт-програм, що не відповідає дійсності інформації; несанкціоноване проникнення на сайти; безконтрольність інформації кримінального характеру.

Враховуючи те, що ми живемо в країні, яка конкурує з іншими в світовій економіці, причому більшість громадян працюють в сфері послуг, для якої, вкрай важливі комп'ютерні технології. Один із наслідків цього – глобально взаємопов'язане суспільство, життєво важлива інфраструктура

[33] Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. М., 2002.

якого вразлива перед кібертероризмом. Одрі Курт Кронін[34] писав, що «ось уже років десять заколотники і терористи успішно використовують Інтернет для проведення своїх операцій. Засоби глобального зв'язку допомагають їм вирішувати завдання організації, набору нових членів, спілкування».

Терористичні групи, використовуючи Інтернет, порушили монополію держав і корпорацій, якою ті довго володіли. Стратегія терористів в швидкому поширенні своїх месиджів і насиченні ними кіберпростору. Інтернет-месиджі терористичних груп стають все більш складними, завдяки використанню фахівців, які працюють на серверах по всьому світу. Як визнав це екс-Президент США Обама, «кіберзагрози можуть нашкодити навіть міжнародному миру і безпеці, оскільки традиційні форми конфлікту розширюються вже і на Інтернет»[35].

Відомо, що держави, так само як окремі люди, сьогодні залежать від Інтернету, який потрібен їм для ведення бізнесу, планування відпустки, придбання товарів і послуг, зв'язку зі старими друзями, і навіть пошуку супутника життя. Твердження, що Інтернет став частиною життя це більше не перебільшення. Відомі в минулому і сьогодні політики зазначили: -«соціальні мережі це найгірше зло в суспільстві» (Тайіп Ердоган), екс-Президент США Обама сказав м'якше – Інтернет це «хребет, що підтримує процвітаючу економіку, сильну армію, відкритий і демократичний уряд». Екс-Держсекретар США Керрі назвав кібератаки проти життєво важливої інфраструктури США «еквівалентом ядерної зброї 21-го століття».

Нині тероризм – це потужні високооснащені структури. Важливою особливістю сучасного тероризму є його добре структурований та організований характер. Терористична діяльність у сучасних умовах характеризується суворою організаційною структурою, що складається з керівної та оперативної ланок, підрозділів розвідки і контррозвідки, матеріально-технічного забезпечення, бойових груп і груп прикриття;

---

[34] How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns [Електронний ресурс].– Режим доступу: https://www.amazon.com/How-Terrorism-Ends-Understanding-Terrorist/dp/069115239X

[35] International Strategy for Cyberspace, 2011 [Електронний ресурс].– Режим доступу: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

жорсткою конспірацією (що приводить до високої латентності цієї діяльності); потужним технічним оснащенням, яке конкурує, а то й перевершує забезпеченість урядових підрозділів.

Кібертероризм не має державних кордонів, кібертерорист здатний однаковою мірою загрожувати інформаційним системам, розташованим практично у будь-якій точці земної кулі. Виявити і нейтралізувати віртуального терориста дуже складно через занадто малу кількість слідів, що залишаються ним, на відміну від реального світу, де слідів вчиненого залишається все ж таки більше. Різноманіття існуючих визначень ускладнює розроблення стратегії боротьби з тероризмом, пов'язаним із інформаційними технологіями[36].

Уніфікованого визначення, закріпленого на законодавчому рівні, поки не існує, а різноманіття наявних дефініцій ускладнює розроблення стратегії боротьби з кібертероризмом. Враховуючи думку відомих фахівців із питань забезпечення інформаційної безпеки, візьмемо як робочу версію таку:

Кібертероризм – суспільно небезпечна діяльність, що здійснюється в кіберпросторі (або з використанням його технічних можливостей) із терористичною метою і полягає у свідомому, цілеспрямованому залякуванні населення та органів влади або вчиненні інших посягань на життя і здоров'я людей.

Кібердиверсія – це суспільно небезпечні діяння у кіберпросторі, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження стратегічних об'єктів шляхом втручання у роботу ІТС.

Кібератака – цілеспрямовані дії, що реалізуються в кіберпросторі (або за допомогою його технічних можливостей), та призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян)[37].

[36] Голубєв В.О. Кібертероризм, як нова форма тероризму [Електронний ресурс] / В.О.Голубєв. – Режим доступу : http://www.crimeresearch.org/library/Gol_tem3.ht.– 10.04.0.

[37] Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В.Дубов, М.А.Ожеван. – К. : НІСД, 2011. – 30 с.

Нова форма тероризму суттєво відрізняється від інших типів: вона діє в кіберпросторі і породжує новий різновид насильства. Саме тому глобальний характер технічної бази кібертероризму та її доступність визначили особливі риси цього виду тероризму: висока ефективність кібератак, наслідки яких можуть мати глобальний характер; невизначеність джерела кібератаки у просторі; тимчасова невизначеність у часі як самої кібератаки, так і процесу її підготовки; можливість організації складних кібератак одночасно на різні об'єкти із різних напрямів; анонімність злочинця (для здійснення терористичного акту зловмиснику немає необхідності перетинати межі держав і знаходитися безпосередньо на місці злочину); зниження рівня морально-психологічного тиску на суб'єкт кібератаки, пов'язане з просторово-часовою віддаленістю від об'єкта кібератаки (усі дії для суб'єктів кібератаки відбувається у віртуальному кіберпросторі)[38].

Кіберзлочинність не обмежується межами злочинів, вчинених у глобальній мережі Інтернет. Вона поширюється на всі види злочинів, вчинених в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, інформаційна техніка можуть бути предметом (метою) злочинних посягань, середовищем, в якому скоюються правопорушення, і засобом чи знаряддям злочину. Характерною особливістю кібертероризму і його відмінністю від кіберзлочинності є його відкритість, коли умови терориста широко висвітлюються мас-медіа.

Спектр проявів кібертероризму досить широкий, від незаконного впливу на прийняття невиправданих рішень, поширення паніки і безладу, до проникнення в канали і системи супутникового зв'язку, навігації, управління енергетикою, транспортом, банківським сектором тощо. На відміну від звичайного терориста, який для досягнення своїх цілей використовує вибухівку або стрілецьку зброю, кібертерорист використовує для досягнення своїх цілей сучасні інформаційні технології, комп'ютерні системи і мережі, спеціальне програмне забезпечення, призначене для несанкціонованого

[38] Іксар В.К. Комп'ютерні злочини [Електронний ресурс] / В.К.Іксар. – Режим доступу : http://www.comprice.ru/pravo/.2001–20_2.phtml.

проникнення в комп'ютерні системи й організації дистанційної атаки на інформаційні ресурси об'єкта нападу.

«Зламуючи» сайти, кібертерористи дістають доступ до різного роду інформації, зокрема значущої. При цьому загроза полягає не просто в отриманні доступу до закритих інформаційних ресурсів державних органів – спеціальні служби досить успішно протидіють вказаним спробам. Найбільшу небезпеку становлять зломи відкритих сайтів і комп'ютерних мереж.

Зокрема, на деяких сайтах місцевих органів влади присутні дані щодо розташування підземних комунікацій, місць знаходження техногенно небезпечних об'єктів, можливої їх охорони, графіки чергувань відповідних служб тощо.

Атакуючи їх, кібертерористи можуть досягти своєї цілі – отримати доступ до чутливої інформації. Водночас злочинці можуть дістати доступ до особистих даних багатьох користувачів мережі – починаючи від їх адреси, номера телефону і закінчуючи детальною інформацією щодо особи, включаючи її хобі і розпорядок життя.

Наслідки злочинних посягань на тісно пов'язані між собою об'єкти критичної інфраструктури держави можуть бути руйнівними як в економічному, так і соціальному плані. Нині багато елементів критичної інфраструктури держави знаходяться у сфері володіння приватного сектору і не є державною власністю. Тому вкрай важливим моментом в організації системи забезпечення безпеки держави є створення відповідної системи координації, до складу якої б входили як урядові, так і громадські організації із залученням комерційних структур, які працюють у ключових секторах критичної інфраструктури держави. Тісний взаємозв'язок між державним і приватним сектором країни є невід'ємною умовою безпеки держави[39].

Ця взаємодія повинна ґрунтуватись на обізнаності щодо загроз критичній інфраструктурі держави; зосередженні уваги спецслужб і виробників програмного забезпечення на безпеці захищеності комп'ютерної техніки; своєчасному і швидкому реагуванні на інциденти,

[39] Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави /О.Д. Довгань, В.Г. Хлань / Інформаційна безпека людини, суспільства, держави. – 2011. – №3(7). – С.49 – 53.

пов'язані з втручанням у роботу автоматизованих систем; наявності системи формального і неформального обміну інформацією щодо загроз комп'ютерної злочинності і кібертероризма.

Вирішення проблеми протидії кібертероризму ґрунтується на комплексному підході та має такі складові:

– *правову* – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;

– *організаційну* – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності у сфері захисту інформації;

– *психологічну* – передбачає формування морально-етичних норм у співробітників, які працюють з інформаційними системами, що забезпечують критичну інфраструктуру держави;

– *технічну* – ґрунтується на створенні і постійному вдосконаленні системи забезпечення інформаційної безпеки на об'єктах інформатизації та попередження нападу.

Звернемо увагу на технічну складову. Проблема розробки і вибору ефективних методів і засобів забезпечення інформаційної безпеки залежить від ресурсів, на які спрямовані атаки, рівня їх захищеності та інших взаємопов'язаних чинників. Ефективність вирішення вказаного завдання передусім полягає у визначенні того, на які класи кібератак розраховані певні методи і засоби протидії.

Враховуючи, що спектр кібератак досить різнорідний, то найбільш доцільно їх класифікувати за такими базовими ознаками, як: інструментальний засіб, що використовується при їх проведенні; специфіка реалізації; міра складності; умова ініціалізації; дистанційність; процес автоматизації; зовнішній прояв; спрямованість кінцевого результату та специфіка порушення базових характеристик системи інформаційної безпеки.

За допомогою такої класифікації можна формалізувати необхідні можливості системи забезпечення кібернетичної безпеки, а також значно

підвищити ефективність їх вибору у ході подальшого проектування та розробки.

З огляду на те, що кібератаки зазнають постійних змін, їх складно прогнозувати та відстежувати у реальному часі, гостро постає питання вдосконалення системи забезпечення кібернетичної безпеки. Досягнення поставленої мети потребує наукового опрацювання та подальшого супроводження таких напрямів, як: розвиток захищених телекомунікаційних систем; підвищення надійності спеціального програмного забезпечення; розробка адекватних методів контролю ефективності засобів захисту інформації; виявлення технічних пристроїв і програм, що становлять небезпеку для штатного функціонування інформаційно-комп'ютерних систем; запобігання перехопленню інформації технічними каналами; формування системи моніторингу показників якості захисту інформації тощо.

Як зазначалося вище, сучасні інформаційно-комп'ютерні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні веб-сайти в мережі Інтернет.

Згідно з озвученими положеннями щорічної доповіді про глобальні ризики у світі «Global Risks Report 2017», підготовлену експертами Всесвітнього економічного форуму в Давосі, на третьому місці за важливістю для світової спільноти перебувають технологічні ризики – крадіжки персональних даних, махінації з ними, масштабні кібератаки та кіберзлочинність[40].

Свідченням щодо останнього є оприлюднені дані із звіту американської компанії «Symantec» «2016 Norton Cyber Security Insights Report», світового лідера в галузі прогресивних рішень інформаційної безпеки. Так, за їх

[40] Эксперты Давоса назвали главные риски для человечества в 2017 [Електронний ресурс].– Режим доступу:http://www3.weforum.org/docs/GRR17_Report_web.pdf

даними у 21 країні світу в 2016 році зазнали збитків від кіберзлочинності понад 689 мільйонів чоловік. Злочинна діяльність у кіберпросторі стала настільки поширеним явищем, що чимало користувачів однаково побоюються як он-лайн, так і реальних посягань[41]. Однією з типових особливостей кіберзлочинності є її глобальний міжнародний характер – кібератака може плануватися в одній країні, поширюватися з декількох інших, а жертвами можуть стати як громадяни, так і приватні й державні установи на різних континентах світу.

Дедалі частіше об'єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.

2017 рік виявився також не простим. Оскільки питанням безпеки було приділено значну увагу з боку суспільства, бізнесу і IT-фахівців, а також фахівців в області безпеки. Виявилося безліч проблем, пов'язаних з шкідливими програмами, а саме спалахами WannaCry і Petya. Так, відповідно до хронології порушень конфіденційності даних Privacy Rights Clearinghouse (PRC), зафіксовано 301 відоме порушення, в результаті яких були скомпрометовані і опубліковані 5 338 608 критичних записів. З цих порушень 166 були пов'язані зі зломом і шкідливими програмами. Масштабна вірусна атака «WannaCry», яка мала місце 12-13 травня 2017 року, вразила десятки тисяч комп'ютерів по всьому світу. У результаті кібернападу у Великій Британії низка медичних закладів по всій країні була змушена відмовляти пацієнтам у наданні послуг навіть в екстрених випадках в наслідок виходу із ладу більшості комп'ютерних систем[42]. В Іспанії атаки зазнало міністерство енергетики, а також телекомунікаційна компанія

[41] 2016 Norton Cyber Security Insights Report [Електронний ресурс]. Режим доступу: https://us.norton.com/cyber-security-insights-2016

[42] ЗМІ: Мільйони комп'ютерів уразливі перед WannaCry [Електронний ресурс]. Режим доступу: http://ua.korrespondent.net/world/3850634-zmi-miliony-kompuiteriv-urazlyvi-pered-WannaCry

«Telefonica». У Німеччині були заражені комп'ютери диспетчерських центрів залізничного концерну, внаслідок чого вийшли з ладу системи диспетчерського управління. Інші комп'ютери було вирішено відключити з метою припинення розповсюдження вірусу[43]. У Франції масштабній кібератаці піддався автовиробник «Renault», у зв'язку з чим у терміновому порядку було вжито всіх необхідних превентивних заходів[44]. У Португалії постраждав найбільший провайдер телекомунікаційних послуг «Portugal Telecom». За інформацією неурядової організації «JPCERT» в Японії, удар хакерів уразив принаймні дві тисячі комп'ютерів. Серед них виявилася заблокованою комп'ютерна мережа однієї з лікарень. За даними видання, у Південній Кореї здійснили кібератаку на найбільшу в державі мережу кінотеатрів. Повідомляється також, що у Китаї від атаки кібершахраїв постраждало приблизно 15% мереж в освітніх закладах. Окрім того, зазнали атак комп'ютерні системи торговельних та офісних центрів, мережі лікарень і заправок, поштової служби, залізничних вокзалів, а також урядові установи[45].

За повідомленням глави компанії KnowBe4 С.Сьювермана, ймовірний збиток, завданий вірусом «WannaCry» за перші чотири дні, перевищив 1 млрд доларів. Зазначається, що в загальну оцінку збитку увійшли втрата даних, зниження продуктивності праці, простої в роботі, судові витрати, репутаційні збитки та інші фактори[46].

Не є винятком з правил й наша держава. Розповсюдження комп'ютерних вірусів, атаки на українські об'єкти фінансового та енергетичного секторів, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем – це далеко

---

[43] Вірус WannaCry вразив системи основного залізничного оператора Німеччини [Електронний ресурс]. Режим доступу: http://nv.ua/ukr/world/countries/virus-wanna-cry-vraziv-sistemi-osnovnogo-zaliznichnogo-operatora-nimechchini-1137166.html

[44] Компанію Renault атакували хакери [Електронний ресурс]. Режим доступу: https://www.vectornews.net/news/world/24688-kompanyu-renault-atakuvali-hakeri.html

[45] Нова хвиля кібератаки. Вірус WannaCry вразив тисячі комп'ютерів у країнах Азії [Електронний ресурс]. Режим доступу: http://tyzhden.ua/News/192285

[46] Вірус WannaCry: збиток оцінили в мільярд доларів [Електронний ресурс]. Режим доступу: http://ua.korrespondent.net/world/3855174-virus-WannaCry-zbytok-otsinyly-v-miliard-dolariv

не повний перелік кіберзлочинів, які відомі в Україні. У 2014 р. наслідки кіберзлочинів коштували українцям 39 млн. грн. А протягом 2015-2016 рр. кількість кіберзлочинів в Україні збільшилася більш ніж на тисячу випадків.

Україна у 2015 році стала абсолютним лідером за внутрішніми і зовнішніми кіберзагрозами в Європі. Що не дивно – за останні роки наша країна неодноразово ставала мішенню не тільки для дрібних шахраїв, але і для наймасштабніших кібероперацій.

Так, Україна посіла п'яте місце в світі (і перше в Європі) за ризиками зіткнення з веб-погрозами в третьому кварталі 2015 року. За даними, Kaspersky Security Network за липень-вересень 2015 третина (33,7%) українських користувачів мережі зіткнулися з погрозами, що поширюються через інтернет.

За тим же показником, за період з січня по вересень 2015 р. Україна посідає третю сходинку рейтингу країн з найбільшим ризиком зараження через інтернет: 35,7% користувачів зіткнулися з веб-погрозами за звітний період.

За результатами другого кварталу 2015 року, Україна опинилася на 9 сходинці рейтингу країн з найбільшим ризиком зараження мобільними зловредами (8,39%). Досить високий для українців і ризик зіткнення з локальними погрозами (54,5%). Сюди потрапляють об'єкти, які проникли на комп'ютери шляхом зараження файлів або знімних носіїв або спочатку потрапили на комп'ютер не у відкритому вигляді (наприклад, програми в складі складних інсталяторів, зашифровані файли і т.д.).

В Україні було відзначено велику кількість спрацьовування антивіруса на програми-вимагачі і шифрувальники – шкідливі програми, мета яких – заблокувати пристрій або браузер або зашифрувати файли користувача, зробивши їх недоступними без спеціального ключа, за який потрібно заплатити викуп.

Серед жертв Turla – однієї з найскладніших кібершпіонських кампаній, яка діє вже більше 8 років, були виявлені комп'ютери українських чиновників. Угруповання, яке стоїть за Turla, заразило сотні комп'ютерів більш ніж в 45 країнах світу, що належать, зокрема, державним установам,

посольствам, військовим, дослідницьким центрам і фармацевтичним компаніям. Метою кіберзлочинців був збір необхідних або конфіденційних даних з комп'ютера жертви[47].

З урахуванням зазначеного та тих даних, якими оперували фахівці в IT-сфері було зроблено прогноз стосовно кіберзагроз у 2016 році. Експерти передбачали, що повністю зміниться структура кібероперацій і те, як вони проводяться. Вони стануть більш непомітними для систем виявлення і фаєрволом. Мотивом атак буде не стільки демонстрація хакерської мощі, скільки повернення інвестицій для держав-замовників, цілі яких не настільки тривіальні. Вони також передбачали, що у перспективі область кібершпіонажу поповниться новими учасниками. Чим більший попит, тим більше пропозиція і такі послуги будуть доступні всім, хто здатний їх оплатити. У мережі зацікавленим особам продаватимуть доступ до конфіденційної інформації високопоставлених жертв. Так з'явиться AaaS – або Access-as-a-Service.

Під загрозою також будуть приватні особи. Очікувалося, що в 2016 році сильно зросте кількість троянських програм, які будуть атакувати банківські акаунти користувачів. Їх поширення пророкують на раніше не схильних загрозам платформах, зокрема на пристроях з OS X або IoT-платформах. Тим часом, кібершахраї шукатимуть нові способи «розводити» жертв на гроші. Слід також очікувати, що популярними мішенями для фінансових кібератак стануть платіжні системи на зразок Apple Pay і Android Pay.

У квітні цього року міністром оборони України Степаном Полтораком у ході брифінгу в Отаві за результатами зустрічі з їхнім міністром національної оборони було озвучено інформацію, що за останні три роки Росія здійснила понад сім тисяч кібератак на Україну. Зважаючи на такі обставини оборонному відомству доведеться посилювати свої позиції в питаннях обізнаності кіберзахисту, об'єднуватися задля співпраці

[47] Кібербезпека в Україні: У 2015 році наша країна – «найгарячіша» точка Європи [Електронний ресурс]. – режим доступу: https://news.finance.ua/ua/news/-/363836/kiberbezpeka-v-ukrayini-u-2015-rotsi-nasha-krayina-najgaryachisha-tochka-yevropy

з країнами-партнерами для спільної оборони кіберпростору. На щастя, вже є втішні результати щодо попередніх домовленостей, та налагоджено співпрацю з Канадою у питаннях, пов'язаних з кіберзахистом. У Конгресі США нещодавно представили законопроект щодо підсилення кібербезпеки України. Документ визначає, що політикою США у даному питанні є надання допомоги урядові України в удосконаленні власної стратегії кібербезпеки.

Також на початку 2017 року стало відомо, що Міністерство фінансів України має намір витратити у п.р. 51,9 млн. грн. на забезпечення кібербезпеки державних інформаційних ресурсів. Виділені кошти планують залучити на закупівлю серверного та комутаційного обладнання, систем зберігання даних, антивірусного програмного забезпечення, послуг з технічного захисту інформації, послуг з надання захищеного доступу до мережі Інтернет.

Таким чином, ми бачимо, що кібертероризм це реальність XXI століття, яку більше не можна ігнорувати. Одрі Курт Кронін[48] говорив, що «Інтернет, це зручний засіб для розширення громадянського суспільства і демократичних ідей, але це також і засіб поширення шкідливих ідеологій, координування злочинної діяльності, відпрацювання її тактики, розробки руйнівної зброї, і підриву сил правопорядку». М.Демпсі сказав інакше: «поширення цифрових технологій не пройшло без наслідків. Воно породило нові загрози нашій безпеці». Ігнорувати їх – це не піде нам на користь. Терористична кібератака проти інфраструктури країни, проведена організацією або терористом-одиночкою, що засіли десь у недосяжній для закону глушині, може привести нас до нового «цифрового Перл-Харбору»[49].

Тому враховуючи викладене та у зв'язку зі зростанням рівня терористичної загрози в розвинутих країнах світу, а також достатньо високою кваліфікацією спеціалістів інформаційних підрозділів спецслужб РФ та вже проведеними кібератаками на об'єкти критичної інфраструктури України слід суттєво підвищити рівень їх інформаційної безпеки. Особливо

[48] Хосе де Ариматейя да Круз. Терроризм, война и кибер(не)безопасность [Електронний ресурс]. – режим доступу: // (http://dialogs.org.ua/ru/cross/page34457.html). – 2014. – 23.09.

[49] Там само

небезпечними є кібератаки на об'єкти енергетичної інфраструктури, оскільки добре скоординована кібератака, особливо при наявності «каскадного» ефекту, може завдати набагато більший збитків, ніж фізична атака та спричинити максимальний громадський резонанс.

Таким чином, боротьба з кіберзлочинністю повинна носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Системна боротьба з кіберзлочинністю потребує об'єднання зусиль правоохоронних органів, громадськості, приватного сектору та ін. з метою вироблення та вдосконалення ефективного механізму взаємодії та співробітництва у питаннях боротьби з кіберзлочинністю, інформаційного забезпечення відповідних процесів з метою упередження нових способів вчинення злочинів. Ефективність заходів у сфері боротьби з кіберзлочинністю повинно досягатися завдяки здійсненню оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики у кіберпросторі.

РОЗДІЛ 3.
ІНФОРМАЦІЙНО-КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ (ІНТЕРНЕТ РЕЧЕЙ, DL-ТЕХНОЛОГІЇ, GRID-ОБЧИСЛЕННЯ, БЛОКЧЕЙН І КРИПТО-ТЕХНОЛОГІЇ ВІДКРИТОГО ДОСТУПУ) ТА ЗАГРОЗИ У СФЕРІ КІБЕРБЕЗПЕКИ

Технологія, на основі якої у подальшому виник Інтернет речей, передбачає можливість підключення до мереж різноманітних речей матеріального світу, а не тільки електронно-обчислювальних машин різної конфігурації. При цьому навіть попередній перелік таких можливих пристроїв скласти неможливо з огляду на стрибкоподібний характер розвитку технології. Таким чином, питання забезпечення безпеки (у широкому розумінні) щодо застосування цієї технології набуває надзвичайної ваги. У ЗМІ в основному акцентується увага на забезпеченні збереження інформації приватного характеру, що пов'язано з масовим використанням мережевих роутерів, маршрутизаторів, мережевих відеокамер та систем відеоспостереження.

Інші фактори небезпеки були визначені свого часу технічними фахівцями з забезпечення національної безпеки і зводяться до наступного.

У загальному вигляді у мережі (у т.ч. глобальній мережі Інтернет) перебувають різноманітні пристрої, значна частина яких зумовлює пряму взаємодію на рівні «машина-машина» (M2M), хоча окремі з таких пристроїв і перебувають під контролем людини[50]. Пряма взаємодія може утворювати різні системи, включаючи системи із застосуванням елементів «штучного інтелекту» та обмеженим використанням управління з боку людини. Але можлива побудова складних систем, створених з пристроїв M2M.

[50] Chou T. Security Threats on Cloud Computing Vulnerabilities. International Journal of Computer Science & Information Technology. 2013. Vol. 5 № 3. P 79-88. URL: http://airccse.org/journal/jcsit/5313ijcsit06.pdf (Last assessed 28.11.2017 p.); Abomhara M., Koien G. Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal Of Cyber Security. 2015. Vol. 4. P. 65-88; Costigan C., Lindstrom G. Policy and The Internet of Things. Connections. 2016. № 2. P. 9-18. URL: https://connections-qj.org/system/files/15.2.01_costigan_lindstrom.pdf (Last assessed 28.11.2017 p.); Rhodes Q., Twist J. Army Cyber Institute Trends and Predictions 2017 Report. May, 2017. URL: http://cyber.army.mil/Portals/3/Documents/publications/threat_reports/ACI_Cyber_Security_Threat_Predictions_2017.pdf?ver=2017-05-22-120747-653 (Last assessed 28.11.2017 p.).

Така ситуація зумовлює уразливість інформації, що перебуває у пристроях, які знаходяться у мережі Інтернет, і пов'язані між собою.

Існуючий стан речей склався під впливом тієї обставини, що спочатку взаємодія між приладами відбувалась у їх власних (локальних або внутрішніх) мережах, і лише потім розробники приладів звернулись до можливостей відкритих мереж. Подальша розробка пристроїв такого типу відбувалась практично без врахування необхідності забезпечення безпеки інформації від витоку та знищення. Наприклад, загроза пристроям Інтернету речей, що відома під назвою «Диявольський плющ» (Devil's Ivy Problem) не є наслідком дій зловмисників, а викликана недоліками в архітектурі побудови зберігачів інформації[51]. Загрози такого типу є суто технічними і викликають збої у роботі пристроїв або впливають на їх робочий стан. Але розповсюдженість технології Інтернету речей, наявність великої кількості пристроїв M2M та інші подібні фактори значно підвищують руйнівний вплив від таких технічних помилок. У випадку з проблемою «Диявольського плюща» негативні наслідки були викликані розповсюдженістю відеокамер одного виду в системах відеоспостереження та технічного управління, побудованих на основі M2M.

Іншим типом загроз є втрати контролю над пристроями внаслідок збоїв управління на рівні M2M, на рівні конкретного пристрою або ж як прояв цілеспрямованих деструктивних дій. В першу чергу мова йде про пристрої сфери транспорту, зв'язку та управління.

Зрозуміло, що пристрої, які постійно перебувають в мережі Інтернет є мішенню для деструктивних дій. У засобах масової інформації наводяться досить численні факти хакерських дій в мережах GSM (*GSM sniffing*), перехоплення в GPRS та втручання через Bluetooth, Wi-Fi або інфрачервоні порти з різною метою. У такому разі пристрій або захоплюються під управління іншим суб'єктом, або виходить з-під контролю оператора. У випадках більш простих атак мова може йти про

[51] Experts in Lather Over 'gSOAP' Security Flaw: Published 17.07.2017. URL: https://krebsonsecurity.com/2017/07/experts-in-lather-over-gsoap-security-flaw (Last assessed 28.11.2017 p.); Roberts P. A Study of IOT-Connected Product Security. URL: https://lmistatic.blob.core.windows.net/document-library/xively/pdf/xively-whitepaper-securityledger.pdf (Last assessed 28.11.2017 p.)

ускладнення управління пристроєм або про технічні збої в його функціях передачі інформації, або ж про підміну даних геолокації пристрою. Унаслідок різноманітності пристроїв Інтернету речей зазначені вище небезпеки є надзвичайно серйозними. Особливо якщо мова йде про медичні пристрої[52]. Технології Інтернету речей широко застосовуються у апаратурі медичного призначення, яка пов'язана із забезпеченням життя (штучні клапани серця і тому подібні пристрої), у зв'язку з цим вплив на управління таким пристроєм є смертельно небезпечним для конкретної фізичної особи.

Під загрозою також перебувають безпілотні літальні апарати (БПЛА, аеродрони), при цьому окрім впливу на їх управління можливий опосередкований вплив на M2M пристрої, що передають дані геолокації. Зазначене також може призвести до критично негативних наслідків. Звичайно така проблема досить давно відома у військовій справі і тому БПЛА військового призначення розробляються з урахуванням сучасних можливостей засобів радіо-електронної боротьби (РЕБ). Але пропозиції і експерименти щодо використання БПЛА в містах з комерційною метою (в основному для постачання товарів, проведення фото-відеозйомки, тощо). При цьому небезпека у застосуванні пов'язана із застосуванням технології взагалі. Тобто пристроїв у належному технічному стані і без їх стороннього впливу. У випадках з БПЛА найбільш яскраво проявляються потенційні конфлікти застосування технологій із реальним суспільним життям. У дослідженнях Інституту Інтернету речей (*Internet of Things Institute, США*) проаналізовані загальні загрози використання комерційних БПЛА. Зокрема, це їх вторгнення у повітряний простір у зонах орієнтирів, ризик зіткнення або падіння на людей, зрив публічних заходів, негативний вплив на застосування пожежної техніки, загроза польотам авіації, можливість обривів ліній електропостачання, використання з протиправної метою

[52] Balasingam I., Abie N. Risk-Based Adaptive Security for Smart IOT in eHealth: SETIT Workshop. 26/09/2012, Oslo, 2012. 25 p. URL: http://asset.nr.no/asset/images/0/01/SeTTIT_2012_Abie_Balasingham.pdf (Last assessed 02.12.2017 p.); Medical Devices and the Internet of Things: Defending against cyber threats. Helpnet Security. 16.08.2017. URL: https://www.helpnetsecurity.com/2017/08/16/medical-devices-iot/ (Last assessed 21.11.2017 p.)

(зокрема, для контрабанди, постачання наркотиків, передача заборонених предметів у в'язниці тощо)[53].

Під загрозами негативного впливу в зв'язку з використанням технологій Інтернету речей перебувають також транспортні засоби та об'єкти критичної інфраструктури[54]. Найбільш актуальними є загрози, що пов'язані з застосуванням безпілотних пристроїв у наземному транспорті. Зокрема, безпілотні автомобілі фактично є M2M пристроєм оскільки їх управління пов'язано з наданням даних геолокації, а отже із глобальної мережею Інтернет.

Загроза, що виходить від так званих «безпілотних автомобілів» для інших учасників дорожнього руху є очевидною. Хоча технічні спеціалісти і вважають, що проектування зазначених пристроїв від самого початку відбувалось з урахуванням можливості перехоплення управління ними, а отже питанням кібербезпеки приділено значну увагу, водночас отримання даних геолокації та напружений характер дорожнього руху зумовлює значний рівень загальної небезпеки технології[55].

Проблема збереження інформації на ранній стадії розвитку пристроїв Інтернету речей особливо не турбувала розробників, оскільки вважалось, що вони передають лише технічну інформацію. Але у подальшому при зміні підходів до правових проблем «великих даних» та необхідності збереження персональних даних в Інтернеті було звернуто увагу і на цю проблему для безпеки в епоху Інтернету речей[56].

Занепокоєння небезпекою розповсюдження зазначених загроз зумовило досить різку реакцію у деяких країнах. У цьому випадку найбільш невідкладною була реакція державних органів США.

---

[53] Buntz B. 10 of the Top Drone Security Worries. IOT Institute Revue, October, 30. 2017. URL: http://www.ioti.com/security/10-top-drone-security-worries (Last assessed 21.11.2017 p.).

[54] Simon T. Critical Infrastructure and the Internet Of Things. Global Commission on Internet Governance. 2017. No 46. URL: https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf (Last assessed 02.12.2017 p.).

[55] West D. Moving Forward: Self-Driving vehicles in China, Europe, Japan, Korea and the United States. Center for Technology Innovation at Brookings Institute, 2016. URL: https://www.brookings.edu/wp-content/uploads/2016/09/driverless-cars-2.pdf (Last assessed 02.12.2017 p.).

[56] Ziegeldorf J-H., Marchon O., Wehrle K. Privacy in the Internet of Things: Threats and Challenges. Aachen Rheinisch-Westfälische Technische Hochschule, 2013. URL: https://www.comsys.rwth-aachen.de/fileadmin/papers/2013/2013-ziegeldorf-scn-privacy-in-the-iot.pdf (Last assessed 02.12.2017 p.).

Зокрема, у своїй доповіді від 25.02.2016 для Комітету Конгресу США з питань розвідки директор Національної розвідки Дж.Клепер зазначив, що проблема забезпечення безпеки у сфері Інтернету речей належить до глобальних загроз, оскільки такі прилади розроблялись із мінімальними вимогами до безпеки і тому їх розповсюдженість насамперед у діяльності державних органів та установ становить небезпеку[57].

Реагування на такі загрози уповноваженими державними органами США відбувалось відповідно до компетенції шляхом підготовки рекомендацій або інших актів реагування.

Зокрема, Міністерство внутрішньої безпеки США (*DHS*) визначило низку стратегічних принципів у забезпеченні безпеки в сфері Інтернету речей. Вказані принципи повинні бути розповсюджені на діяльність розробників, виробників, постачальників послуг, а також державних і комерційних споживачів. Система стратегічних принципів зумовлена необхідністю належного державного реагування на загрози, що виникають у сфері Інтернету речей і визначені наступним чином:

– упровадження вимог безпеки на етапі розробки приладу,

– забезпечення своєчасного оновлення засобів безпеки та управління вразливостями;

– слідування визнаним практикам у сфері забезпечення безпеки;

– надання пріоритету вимогам безпеки відповідно до потенційного впливу;

– забезпечення поінформованості стосовно приладів у сфері Інтернету речей;

– обережне та обдумане під'єднання до мережі[58].

Цей розроблений фахівцями документ встановлює загальні засади політики і не є директивним приписом або нормативно-правовим актом.

---

[57] Clapper J. Worldwide Threats Assessment of the US Intelligence Comminity: Statements for the record. February, 25, 2016. US Congress' House Permanent Select Committee on Intelligence. 33 p. URL: https://www.dni.gov/files/documents/Newsroom/Testimonies/HPSCI_Unclassified_2016_ATA_SFR-25Feb16.pdf (Last assessed 02.12.2017 p.).

[58] US Department of Homeland Security: Strategic Principles for Securing the Internet of Things. Version 1.0. November, 15.2016. Washington: DHS. 22 p.

Шляхи впровадження зазначених стратегічних принципів мають уникати директивного державного впливу на бізнес, а лише рекомендувати кращі практики забезпечення безпеки, які відомі на сьогодні, окрім сфер державного регулювання (телекомунікації, платіжні системи тощо).

Міністерство оборони США (*DOD*) розробило обов'язкові для керування власними службовцями «рекомендації», що визначають як загальні вимоги до використання приладів у сфері Інтернету речей в підпорядкованих установах, організаціях, військових частинах так і конкретні заходи безпеки для користувачів[59].

Законодавчі пропозиції стосовно регулювання безпеки у сфері Інтернету речей у США знайшли своє відображення у законопроекті сенаторів М. Уарнера, К. Гарднера, Д. Фішера і Р. Уайдена – «Акт щодо впровадження кібербезпеки стосовно Інтернету речей» 2017 року[60]. Проте зазначений проект викликав досить серйозну критику з боку прихильників громадянських свобод та фахівців у сфері інформаційних технологій[61].

Найбільш неоднозначними є пропозиції ведення державними органами обліку приладів, що можуть під'єднуватися до мережі Інтернет, регламентація порядку продажу таких пристроїв у роздрібній мережі, обмеження придбання таких приладів державними установами.

В Європейському Союзі загрози у сфері Інтернету речей є предметом уваги Європейського агентства з мережевої та інформаційної безпеки (ENISA) та Європейської групи кібербезпеки. Хоча можливо констатувати

---

[59] US Department of Defense: Policy Recommendations for The Internet of Things (IoT). December 2016. Washington: DHS. 24 p.

[60] S. 1691: Internet of Things (IoT) Cybersecurity Improvement Act of 2017. Bill. URL: https://www.govtrack.us/congress/bills/115/s1691/text (Last assessed 02.12.2017 p.).

[61] Dellinger A. IOT Security: Senate Bill Proposes Safeguard for Government Internet-Connected Devises. International Business Times. August, 01, 2017. URL: http://www.ibtimes.com/iot-security-senate-bill-proposes-safeguards-governments-internet-connected-devices-2573207 (Last assessed 02.12.2017 p.); Teitler K. Will the Latest (Proposed) Legislation Make a Differense? MISTI. August, 03, 2017. URL: http://misti.com/infosec-insider/will-the-latest-proposed-iot-legislation-make-a-difference (Last assessed 02.12.2017 p.); Joyce S. The next stage in the evolution of the Internet of things? PWC Next In Tech. August, 04, 2017. URL: http://usblogs.pwc.com/emerging-technology/evolution-of-iot-is-security (Last assessed 02.12.2017 p.); Buntz B. US Congress' proposed IOT security requirements: A balancing act. IOT Institute Revue. August, 14, 2017. URL: http://www.ioti.com/security/us-congress-proposed-iot-security-requirements-balancing-act (Last assessed 02.12.2017 p.).

менший рівень занепокоєності станом проблеми з боку відповідних урядових функціонерів. Зокрема, у доповіді для Європейської наради з питань кібербезпеки 2016 року, підготовленою ENISA, зазначено, що значне розповсюдження Інтернету речей буде знижувати рівень безпеки попри на застосування неналежних методів захисту та людський фактор, який негативно впливає на стан безпеки[62].

Слід зазначити, що напрями державної політики стосовно забезпечення кібербезпеки у зв'язку з використанням технології Інтернету речей визначені в ЄС менш детально аніж у США і ще не стали значним трендом для державних органів або міждержавних агентств.

На відміну від ЄС у КНР досить значна увага приділяється заходам з вдосконалення державної політики у сфері регуляції питань застосування технології Інтернету речей, в першу чергу на технічному рівні[63]. При цьому на думку деяких дослідників, враховуючи значний вплив китайських виробників на ринок приладів, заснованих на технології Інтернету речей, не можна виключити можливість цілеспрямованих дій з боку влади КНР щодо використання таких приладів в інтересах китайської держави[64]. Значна увага питанню забезпечення кібербезпеки в умовах використання технології Інтернету речей приділяється урядами Японії та Кореї. Зокрема, в Японії заходи з забезпечення такої безпеки визначаються на рівні документів державного стратегічного планування[65].

---

[62] European Foresight Cyber Security Meeting 2016. URL: https://www.cybersecurityraad.nl/binaries/Report%20European%20Foresight%20Cyber%20Security%202016_tcm56-102235.pdf (Last assessed 13.11.2017 p.).

[63] Müller B. Cyber Security Made in China. Pictures of the Future. September, 12, 2017. URL: https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/it-security-it-security-in-china.html (Last assessed 28.11.2017 p.).

[64] Lowmaster K. China Insidious Surveillance Army: The Internet of Things. The Hill. 21/11/2017. URL: http://thehill.com/opinion/cybersecurity/361300-chinas-insidious-surveillance-army-the-internet-of-things

(Last assessed 28.11.2017 p.).

[65] Yamauchi T. Cybersecurity Strategy in Japan. NISC, April, 24, 2017. URL: https://project.inria.fr/FranceJapanICST/files/2017/05/TYamauchi_presentation_2017.pdf (Last assessed 18.11.2017 p.); Kim K., Park S., Lim J. Changes of cybersecurity legal system in East Asia: Focusing on comparison between Korea and Japan // Lecture Notes in Computer Science. Vol. 9503 Springer Verlag, 2016. P. 348-356.

Разом із цим заходи реагування передбачають інформування суб'єктів використання приладів Інтернету речей, обмін інформацією між державними органами та впровадження кращих практик. Доречно зазначити, що фахівці з кібербезпеки визначають за необхідне унормування відповідних технічних стандартів у цій сфері шляхом відкритої сертифікації[66], хоча відкрита сертифікація не є обов'язковою і не вирішують багатьох організаційних і правових проблем.

Стан державного реагування на загрози, пов'язані з застосуванням технології Інтернету речей в Україні може бути охарактеризований лише негативно, попри на зафіксований різними спеціалістами стан небезпеки. Серед прикладів фахового обговорення варто зазначити науково-практичну конференцію «Інтернет речей: проблеми правового регулювання та впровадження», що відбулася 24 жовтня 2014 року[67]. Співорганізаторами цього заходу виступили Комітет з питань інформатизації і зв'язку Верховної Ради України, Науково-дослідний інститут інформатики і права Національної академії правових наук України та факультет соціології і права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Водночас, документи стратегічного планування з питань забезпечення кібербезпеки, що ухвалені останнім часом в Україні, оминають проблематику забезпечення безпеки у сфері Інтернету речей, хоча деякі із визначених заходів державної політики одночасно і опосередковано стосуються проблематики Інтернету речей.

Підсумовуючи викладені вище загрози у сфері розповсюдження технології Інтернету речей, доцільно узагальнити з урахуванням кращих світових практик й відповідних звітів фахівців з питання кібербезпеки наявні загрози безпеці у сфері Інтернету речей та відпрацювати прогнозні

---

[66] Spiegelmock M. IoT Security Through Open Certification. URL: https://spiegelmock.com/2017/08/14/iot-security-through-open-certification/ (Last assessed 28.11.2017 р.).

[67] Інтернет речей: проблеми правового регулювання та впровадження : Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петрячев. Київ: Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. 238 с.

показники на рівні технічних спеціалістів. З урахуванням існуючої в Україні моделі забезпечення кібербезпеки зазначене скоріш за все належить до компетенції Національного координаційного центру з питань кібербезпеки. Окрім цього, на нашу думку вітчизняні законодавчі та нормативно-правові новації у цій сфері мають ґрунтуватись на відповідних рекомендаціях, що мають бути підготовлені фахівцями (аналогічно до рекомендацій державних органів США) і враховувати кращі зразки світової практики. Пропозиції щодо стандартизації у сфері Інтернету речей на міждержавному рівні , попри на існуючі складнощі.

У контексті розгляду питань забезпечення кібербезпеки та ескалації відповідних загроз доцільно розглянути вплив на це технології розподіленої обробки даних. Мова йде про розподілену обробку даних та відповідні технології – **«хмарні технології», grid, DLT та блокчейн**, що мають багато спільного.

Розвиток технології розподіленої обробки даних відбувався паралельно з розвитком інших технологій побудови і використання комп'ютерних мереж. Особливості існування зазначених технологій та вирішення різного роду технічних завдань тривалий час не створювали якихось особливих проблем правового характеру, оскільки суто технічна специфіка, не здійснюючи прямого впливу на суспільні відносини, не викликала необхідності у відповідному нормативно-правовому регулюванню цієї діяльності.

У подальшому при технічному розвитку сфери комп'ютерних технологій виникла технологія розподілених реєстрів (*Distributed Ledger Technology, DLT*), одним із напрямків якої є «блокчейн» – технологія розподіленої системи даних, що закладена в основу «криптовалют» (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента), найвідомішою з яких на сьогодні є система «Біткойн».

Упровадження та стрімке розповсюдження технології «блокчейн» викликає зміни у суспільних відносинах, що потребує правового регулювання. Останні пропозиції щодо розширення сфери застосування технології «блокчейн» на різні сфери суспільного життя – банківську справу,

фінанси, оподаткування, державні реєстри, виборче законодавство, земельні відносини тощо викликає і нові соціальні та правові проблеми.

Сама по собі «DL-технологія» (одним із підвидів якої є «блокчейн»-технологія) на сьогодні однозначно термінологічно не визначена в українській мові. В основі скорочення DLT лежить термін «ledger», який, починаючи з XIX сторіччя розуміється як «основна бухгалтерська книга» або гросбух, а походить від співзвучного застарілого і скоріш за все запозиченого з голландської мови терміну «leg[g]er» – «річ, що знаходиться в основі чогось»[68]. Слід зазначити, що важливість цього терміну для розуміння суті технології підкреслюється обраною для першого академічного журналу з DL-технологій, який видається Бібліотекою Університету Пітсбурга, назвою «Ledger»[69].

Питанням соціальних, організаційних, інформаційних, технічних аспетів використання «біткойну» та «блокчейн»-технологій присвячені численні публікації в основному в англомовній науковій літературі останніх років, у т.ч. і монографічного характеру.

Слід також згадати огляди та звіти державних органів, аналітичних і дослідницьких установ, присвячені окремим питанням використання та розвитку DL-технологій в основному з точки зору аналізу економічного впливу розповсюдження криптовалют. При цьому практично відсутні публікації стосовно правових аспектів використання DL-технологій та інших (альтернативних «біткойну») криптовалют («альткойни»). Роботи аналітичних підрозділів державних органів різних країн мали на меті насамперед проведення дослідження суті відносин, пов'язаних з застосуванням DL-технологій та їх проявів у різних сферах людської діяльності, враховуючи рівень потенційної небезпеки від таких технологій. Спочатку небезпека розумілась в основному з точки зору забезпечення фінансової безпеки держав, впливу на їх валютний ринок, необхідності

[68] Більш детальне дослідження щодо походження та історії вжиття термінології DLT викладено у роботі: Доронін І.М. Використання сучасних технологій розподіленої обробки даних: право та функції держави. Інформація і право. 2017. № 2 (21). С. 52.

[69] URL: https://ledgerjournal.org/ojs/index.php/ledger/about/editorialPolicies#focusAndScope (Last assessed 28.11.2017 р.).

вжиття заходів боротьби з фінансовими правопорушеннями та легалізацією грошових коштів здобутих злочинним шляхом. Окремою метою була необхідність забезпечення технічної безпеки сучасних електронних платежі них систем.

Якщо розглядати розвиток DL-технологій у загальному вигляді, то використання систем розподіленої обробки даних для вирішення різного роду технічних завдань застосовується досить давно. Перші програми використання потужностей електронно-обчислювальних машин для проведення спільних обчислень з'явились понад 40 років тому практично одночасно зі створенням комп'ютерних мереж. Застосування технологій було обумовлено вирішенням суто технічних завдань та економічними потребами – перші розробники зазначених технологій забезпечували проведення обчислень на електронно-обчислювальних машинах, які не використовувались у неробочий час та у вихідні, або не були задіяні у вирішенні інших завдань. Розвиток зазначеного типу технологій зумовив застосування GRID (більш вдалим є термін «грід-обчислення», оскільки GRID не є абревіатурою, а походить від англійського слова «grid» – решітка, а у вигляді абревіатури термін став вживатись у нормативно-правових актах, зокрема, в розділі 3 Основних засад розвитку інформаційного суспільства в Україні на 2007-2015 роки, затверджених Законом України від 09.01.2007 № 537-V[70], а в Основних напрямах та найважливіших проблемах фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009-2013 роки, затверджених наказом Міністерства освіти і науки України та НАН України від 26.11.2009 № 1066/609, термін Grid вживається не як абревіатура, що є більш вірним[71]).

Розвиток технології розподіленого обчислення відбувався паралельно з розвитком технологій побудови і використання комп'ютерних мереж,

[70] Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. Голос України. 06.02.2007. № 21

[71] Про затвердження Основних напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009-2013 роки: наказ МОН України та НАН України від 26.11.2009 № 1066/609. Офіційний вісник України. 2010. № 40. С. 25. Ст. 1326.

а також передачі інформації у таких системах, особливо значний вплив на їх розвиток спричинили «пірінгові» мережі, які дозволили відійти від традиційної побудови за принципом «клієнт-сервер»[72]. Особливості існування цих технологій тривалий час не створювали якихось специфічних проблем правового характеру за винятком захисту прав інтелектуальної власності при розповсюдженні інформації у «пірингових» мережах, що призвело до юридичної «війни проти торентів» і є значною проблемою правового регулювання до цього часу. Питання забезпечення безпеки також не виходили за рамки загальних загроз, що традиційно існували для комп'ютерних мереж.

У подальшому з'явилась технологія розподілених реєстрів (Distributed Ledger Technology, DLT) і, нарешті технологія «блокчейн», яка стала на сьогодні трендом в гуманітарних науках, що вивчають аспекти інформаційних технологій. За 2017 рік термін «блокчейн» можливо вже сприймати як медіа-вірус, який перебуває у загальносуспільному дискурсі, характеризуючи свій зміст як «прояв реформ» апріорі і тому досить широко застосовується в політичній рекламі та промоцій ній діяльності. На нашу думку, створенню і розповсюдженню DL-технологій сприяло технічне вирішення двох проблем – передачі інформації за відсутності централізованого серверу і взагалі відхід від побудови мереж за принципом «клієнт-сервер». Відома американська дослідниця філософських і соціологічних проблем впровадження нових технологій М. Свон вважає одноранговий «піринговий» обмін основою для технології «блокчейна»[73]. Погоджуючись із цим, слід зазначити, що іншою технічною проблемою, яка вирішена, це проблема захисту інформації від впливу, тобто криптозахисту на рівні кожної операції обміну інформацією. На сьогодні саме такий захист зумовив надзвичайну популярність криптовалют в інвесторів, насамперед інформаційної сфери, оскільки криптозахист зробив з таких валют по суті «цифрове золото», недарма саме таку назву для своєї книги,

[72] Kshemkalyani A., Singhal M. Distributed Computing. Principles, Algorithms And Systems. Cambridge: University Press.2008. 756 p.; Coulouris G., Dollimore J., Kindberg T., Blair G. Distributed Systems: Concepts and Design. Fifth Edition. Boston: Pearson-Addison-Wesley, 2012.1008 p.

[73] Swan M. Blockchain: Blueprint for a New Economy. Sebastopol CA: O'Reilly Media, 2015. P 3

присвяченій історіям ключових постатей біткойн-індустрії обрав репортер-розслідувач Н.Поппер. Водночас обраний для технології метод криптозахисту зумовлює збереження всієї історії змін інформації (за загальним правилом, якщо не рахувати окремі підвиди технології). Не вдаючись в технічні тонкощі, можливо стверджувати, що сутність DL-технології полягає у відсутності якогось одного фізичного носія інформації (сервера чи системи серверів), що зберігає усю інформацію, або її частину. Інформація, яка зберігається, перебуває одночасно у всіх учасників системи, при цьому жоден з них не контролює ані усю інформацію, ані якусь критично важливу частину. Саме таке розуміння суті технології вбачається критично важливим для правового погляду на суспільні відносини в цій сфері з метою вирішення проблем юридичного характеру, а також для розуміння суті загроз, що можуть виникнути для безпеки інформації в комп'ютерних мережах. Існують різні технічні рішення зазначеного вище завдання щодо розподіленої інформації. З огляду на критичну важливість для такої системи проблеми захисту інформації перспективними для прикладного використання поза сферою наукових обчислень є системи, які використовують криптографічний захист і конструювання блоків. Зазначена технологія наразі відома як «блокчейн» (від англомовного терміну block chain – ланцюг блоків) і використовується насамперед як розподілена система даних, що закладена в основу «криптовалют» (віртуальних валют, які не мають фізичного аналогу і, як правило, одного емітента, а здобуваються шляхом використання обчислювальних можливостей учасників системи), найвідомішою з яких на сьогодні є система «Біткойн». На сьогодні досить часто у популярній літературі та засобах масової інформації ці поняття використовують як синоніми. Хоча, звичайно, увага суспільства (а останнього часу і держав в особі їх органів) більше зосереджена на «біткойні», оскільки цифрові показники є більш ніж красномовними. Починаючи з січня 2017 року капіталізація «біткойн»-індустрії збільшилась вдвічі і станом на травень поточного року становить близько 35 мільярдів доларів США, а на листопад того ж року – вже більше 500 мільярдів.

І хоча таке зростання дозволяє окремим аналітикам зробити висновки про спекулятивний характер торгівлі «біткойн» і її розуміння як чергової інвестиційної «мильної бульбашки», яка неодмінно закінчиться падінням

та кризою, економічне значення введення і розповсюдження грошової одиниці, яка не емітується централізовано, але є об'єктом для вільної торгівлі на біржах і обміну на інші валюти, важко переоцінити. Основні аналітичні звіти, що були підготовлені різноманітними науково-дослідними та аналітичними установами стосувались насамперед економічних питань – від глобального впливу на стан світової економіки до питань кримінальної (тіньової) економіки та ухилення від сплати податків.

В основі традиційного сприйняття «біткойн»-індустрії знаходяться багато факторів – як економічних, так і геополітичних – наприклад, окремі дослідники приділяють значну увагу ролі Китаю на глобальних ринках «біткойн» та взаємозв'язку характеру внутрішніх китайських ринків із ціною криптовалюти. З іншого боку «біткойн» став трендом і породив певну суспільну субкультуру, нерідко і без якогось економічного підґрунтя. На нашу думку, питання глобальних впливів на світову економіку слід розглядати окремо, а в рамках цієї роботи доцільно зосередитись на проблематиці впливу проявів технології «блокчейн» на стан кібербезпеки.

Як вбачається з самого терміну «криптовалюта», в основі її існування знаходиться безпека, яку забезпечують методи захисту, побудовані на криптографії. Попри досить невелику історію використання криптовалют, з часу впровадження їх вільного обміну на звичайні грошові кошти та введення котирування на деяких валютних біржах, різного роду атаки на систему є постійними. Особливо, коли вартість одного біткойну стала перевищувати 1 000 доларів США.

В основному, звичайно, кібератаки робляться для викрадання криптовалют. Такі атаки бувають і успішними у випадках, коли об'єктом є не уся система або її частина під час функціонування, а конкретний визначений користувач, що «зберігає криптовалюту» (яка так би мовити «існує» тільки у віртуальному вигляді) на власних носіях інформації. Іншою метою атак є намагання встановити контроль над емісією криптовалют одним користувачем (або групою, що об'єднана змовою). Зазначені випадки мали місце шляхом змови великих груп, які займаються здобуванням «біткойну», але успішними не були завдяки закладеним в алгоритм системи запобіжникам.

На цей час питання картельного управління системою з боку осіб, що здійснюють вплив на систему через недержавний орган (Bitcoin Foundation) залишається відкритим з часу кримінального переслідування Ч.Шрема в США[74].

Оскільки в основі системи є розподілення інформації та криптографічний захист усіх транзакцій на усіх етапах система є стійкою за умови, якщо електронно-обчислювальні машини, які її складають, продовжують роботу. У випадку, якщо система створена і використовується для обігу криптовалют, її робота зумовлена необхідністю здобування нових одиниць криптовалюти, яка виробляється внаслідок проведення обчислювальних операцій учасниками усієї системи. Таким чином учасників системи тримає у ній їх власний економічний інтерес. Слід зазначити, що кількість криптовалют, які є альтернативою «біткойн», уже обчислюється сотнями. Серед них є і валюти з різними видами підтримки державами, а також ті, які покращили алгоритм програми таким чином, що виключають генерацію у промислових масштабах.

З аналітичних оглядів, підготовлених фахівцями у сфері фінансів та регулювання[75], попри нібито мінімальність державного впливу в цій сфері

---

[74] Biddle S. Bitcoin Cartel Seizes Enough Power to Spend Money Twice. ValleyWag. 16.06.2014. URL: http://valleywag.gawker.com/bitcoin-cartel-seizes-enough-power-to-spend-money-twice-1591601615 (Last assessed 28.11.2017 p.); Raymond N. Bitcoin backer gets two years prison for illicit transfers. Reuters Technology News. December, 19, 2014. URL: https://www.reuters.com/article/us-usa-crime-bitcoin/bitcoin-backer-gets-two-years-prison-for-illicit-transfers-idUSKBN0JX2CW20141219 (Last assessed 28.11.2017 p.).

[75] Murphy E., Murphy M., Seitzenger M. Bitcoin: Questions, Answers and Analysis of Legal Issue. Report by Congressional Research Service. October, 13. 2015. Washington. US Congerss Research Service. – 2015. – 36 p.; Shcherbak S. How Should Bitcoin be Regulated? European Journal Of Legal Studies. 2014.Vol. 7. No 1. P. 42-83; Walport M. Distributed Ledger Technology: beyond block chain. December 2015. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (Last assessed 28.11.2017 p.) Whitepaper On Distributed Ledger Technology. Commissioned by Hong Kong Monetary Authority. URL: http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf (Last assessed 27.05.2017 p.); Mills D., Wang K., Malone B., Ravi A., Marquardt J., Chen C., Badev A., Brezinski T., Fahy L., Liao K., Karnegian V., Ellithorpe M., Baird M. Distributed ledger technology in payments, clearing, and settlement. URL: https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf (Last assessed 27.05.2017 p.); Casey M., Dahan M. Blockchain Technology: Redefining Trust for a Global Digital Economy. URL: https://medium.com/mit-media-lab-digital-currency-initiative/blockchain-technology-redefining-trust-for-a-global-digital-economy-1dc869593308 (Last assessed 27.05.2017 p.)

і, навіть, практичну неможливість статутного правового регулювання таких суспільних відносин, основними проблемами вбачаються такі:

1. Необхідність ліцензування (або будь-якого іншого дозволу з боку держави в особі її уповноважених органів) для такої діяльності взагалі. У демократичних державах усяка діяльність приватних осіб, що не порушує закон, є легальною. Таким чином, відповідні операції з криптовалютами (купівля-продаж та інші угоди) ніяких дозволів не потребують оскільки здійснюються між приватними особами. Метою зазначеної діяльності державних органів є протидія вчиненню злочинів (насамперед, шахрайства) щодо приватних осіб, а також легалізації доходів, отриманих злочинним шляхом, фінансуванню тероризму, ухиленню від сплати податків. Основним проблемним питанням для правової регламентації цих відносин є необхідність дотримання правил про так звану банківську ідентифікацію вкладників, що не завжди можливо в умовах проведення операції з криптовалютою.

2. Оподаткування операцій з криптовалютами. Безумовно, що під час проведення операцій отримується прибуток, який підлягає оподаткуванню. При цьому такий прибуток може виникнути і як пасивний дохід внаслідок збільшення вартості криптовалюти по відношенню до валюти, емітованої державою, протягом часу. У деяких державах існують також окремі податки на майно, до складу якого також можуть бути віднесені криптовалюти внаслідок наявності у них відповідної вартості. На сьогодні у більшості держав із розвиненою фінансовою системою та деталізованим податковим законодавством, проблема належної правової регламентації оподаткування таких операцій та вдосконалення відповідного законодавства є актуальним. Тим більше, що інвестування в криптовалюти може здійснюватись з метою мінімізації податків.

3. Також важливим питанням є визначення статусу криптовалют саме як грошей. Ще два роки тому щодо криптовалют застосовувався термін «сурогат грошей». А в деяких державах були підготовлені законодавчі пропозиції стосовно заборони таких «сурогатів». Нині з різних причин криптовалюти (або окремі види) заборонені у деяких країнах (Бангладеш, Болівія, В'єтнам, Таїланд), проте операції з ними не криміналізовано,

а ці обмеження стосуються адміністративних заборон у діяльності банків та інших фінансових установ. Така заборона пов'язана, як правило, з іншими численними забороняючими та регламентуючими вимогами. Інші випадки (Ісландія, Гонконг) стосувалися досить складної державної політики та наявності певних преференцій у цій сфері. Як правило, спірні питання виникають в першу чергу при валютообмінних операціях (з огляду на відсутність централізованого емітента, криптовалюта розглядається як аналог дорогоцінного металу, а операції юридично вважаються бартерними), а також при використанні криптовалют як засобу платежу за товари чи послуги (при цьому невирішеними залишаються спірні питання у цивільно-правовому статусі такої угоди і оподаткуванні відповідної операції).

4. Необхідність дотримання вимог міжнародно-правових актів щодо боротьби з тероризмом та легалізацією доходів, отриманих злочинним шляхом. Імплементація зазначених положень у національне законодавство викликає правову колізію з огляду на зазначені вище властивості криптовалюти. Звичайно, що криптовалюти з огляду на удавану анонімність цілком можуть використовуватись для фінансування різних видів протиправної діяльності.

При цьому дослідники проблематики протидії фінансуванню тероризму та іншої протиправної діяльності зазвичай розглядають криптовалюти як аналог історичних систем безготівкових операцій з веденням децентралізованого обліку. У такому разі виникає необхідність у вжитті відповідних заходів щодо застосування визначених міжнародно-правовими актами механізмів насамперед у питанні ідентифікації в режимі реального часу не тільки суб'єктів проведення операцій, а і всіх транзакцій. Пов'язаним із цим питанням є необхідність дотримання вимог законодавства щодо обмеженості використання криптографії недержавними органами та приватними особами, що до цього часу існує в США та деяких інших країнах. Така обставина може впливати на правове регулювання використання криптовалюти, оскільки застосування криптографічних методів її захисту є неодмінною властивістю криптовалюти. Натомість, анонімізація платежів є досить удаваною.

Річ у тім, що технологія блокчейн не забезпечує анонімізацію, навпаки для участі у системі необхідна цифрова ідентифікація користувача, яка розповсюджується на усі його дії. У випадку поєднання такої технології зі сферою «інтернет-речей» можлива повна ідентифікація дій особи, фіксація інформації стосовно таких дій, а також вплив на ці дії зовні. До речі, на двоякий характер технології і здатність використання її ідентифікаційних можливостей в інтересах правоохоронної діяльності вже звернуто увагу окремих дослідників[76].

На нашу думку, питання правового регулювання суспільних відносин, які виникають у ході обігу криптовалют, мають розглядатись у контексті реалізації функцій держави, що знаходить свій прояв у відповідному впливі та правовій регламентації. У правовій регламентації обігу криптовалют реалізується економічна функція держави, яка зумовлена потребами ринкової економіки. Інша річ це застосування технології «блокчейн» у тих напрямках життєдіяльності, що прямо не пов'язані із обігом криптовалют.

За останні два роки зазначений вид технологій розподіленої обробки даних став дуже популярним в основному в сфері вітчизняних мас-медіа. З огляду на таку популярність, імідж «блокчейн» став використовуватись у політичних цілях та у рекламній компанії деяких продуктів, у т.ч. ніяк не пов'язаних з цими технологіями.

Особливим напрямом є застосування технологій розподіленої обробки даних в системах електронного урядування та ведення державних реєстрів. Це зумовлено, насамперед, вимогами боротьби з корупцією, що досягається прозорістю дій держави.

Використання «блокчейн» та інших подібних DL-технологій для ведення державних реєстрів та у діяльності державних органів визнана перспективною фахівцями з державного стратегічного планування провідних країн світу. Починаючи з 2016 року, у вітчизняній пресі

[76] Everdell C., Mandell D. The Promise of Blockchain Technology To Combat Money Laundering. New York Law Journal.2017. Vol. 257. № 62. https://www.cohengresser.com/assets/publications/070041703_Cohen_Gresser.pdf (Last assessed; 27.05.2017p)

згадувалось принаймні про два проекти застосування технології «блокчейн» саме для ведення різного роду державних реєстрів України. Попри досить активну кампанію в ЗМІ саме «блокчейн»-технології ще ніде в світі не реалізовано в рамках більш-менш великого проекту у сфері державних реєстрів. Значна популярність ідеї застосування «блокчейн»-технології для державних реєстрів зумовлена насамперед недовірою суспільства до діяльності державних органів, а також іншими соціальними факторами впливу (медійна популярність теми, недовіра до закритості інформації, приналежність активної частини користувачів соціальних мереж і ЗМІ до субкультури «блокчейну» та криптовалют, лібертаріанські ідеї тощо).

До речі, застосування технологій на основі «блокчейн» в адмініструванні різних державних реєстрів звичайно не скасовує визначених законодавством України вимог до захисту інформації в мережах. Тому усі випадки побудови реєстрів на основі технології «блокчейн» поки що носять характер проектів та експериментів.

На наш погляд, при використанні сучасних технологій розподіленої обробки даних (DLT, блокчейн) у сферах державного регулювання та державної реєстрації інформації неодмінно рано чи пізно доведеться вирішити ряд проблем насамперед правового характеру до числа яких слід віднести: – питання відповідальності держави за функціонування системи (у випадку класичної «блокчейн»-технології ніхто не контролює всю систему), – питання стимулів для підтримки функціонування системи користувачами (у випадку «криптовалют» таким стимулом є економічний); – питання захищеності інформації (насамперед від втрати і спотворення та забезпечення довготривалого (практично довічного) зберігання у відкритому для користування стані). У будь-якому разі впровадження технологій розподіленої обробки даних для потреб управління державою потребуватиме значного оновлення законодавства і вирішення дуже серйозних правових проблем.

На наш погляд, ескалація загроз у кіберпросторі протягом останніх двох років зумовлена в першу чергу особливим характером комп'ютерних

технологій, що мають значне розповсюдження у суспільстві. Мова йде про певний клас таких технологій, який пропонується розглядати під умовним терміном «емерджентні технології». Про що саме йде мова?

Насамперед, слід визначитись які саме технології, що є новітніми у хронологічному сенсі, здійснюють істотний вплив на суть і характер суспільних відносин сучасного суспільства. У науковій літературі останніх п'ятдесяти років для цих явищ вживаються насамперед терміни «науково-технічна революція», «науково-технічний прогрес», «новітні технології», «інновації». Термінологічна багатоманітність стосувалась практично ідентичних явищ, а вектор їх розгляду багато у цьому був аналогічним. Останнім часом став у науковій літературі найбільш часто вживається термін «інновації».

Зокрема, стаття 1 Закону України «Про інноваційну діяльність» визначає інновації як «новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери», а інноваційну діяльність як «діяльність, що спрямована на використання і комерціалізацію результатів наукових досліджень та розробок і зумовлює випуск на ринок нових конкурентоздатних товарів і послуг»[77].

Якщо проаналізувати приписи статті 4 Закону України «Про пріоритетні напрями інноваційної діяльності в Україні», що безпосередньо визначає стратегічні пріоритетні напрями на період до 2021 року, то інноваційну діяльність по суті можливо визначати як створення та використання певних технологій[78].

Для англомовної наукової літератури більш розповсюдженим є термін «emerging technologies». Зазначений термін зазвичай перекладається як

[77] Про інноваційну діяльність: Закон України від 04.07.2002 № 40-IV. Дата оновлення: 05.12.2012. URL: http://zakon3.rada.gov.ua/laws/main/40-15 (дата звернення: 26.11.2017).

[78] Про пріоритетні напрями інноваційної діяльності: Закон України від 08.09.2011 № 3715-VI. Дата оновлення: 05.12.2012. URL: http://zakon3.rada.gov.ua/laws/show/3715-17 (дата звернення: 26.11.2017).

«новітні технології», що безумовно не відображає його зміст. На думку сучасних дослідників зазначені технології мають наступні основні властивості – радикальну новизну, відносно швидке зростання, узгодженість, значний вплив та невизначеність[79].

Тобто для такої технології характерна стрибкоподібність – вона з'являється нібито нізвідки, хоча і ґрунтуються на відповідних наукових концепціях.

Викладене можливо проілюструвати наступним прикладом.

Якщо провести аналіз ситуації навколо розвитку технологій, пов'язаних із використанням графену, то легко встановити, що такі дослідження провадились хіміками та фізиками протягом 100 років, допоки у 2004 році не відбувся прорив у науці – винайдення методу отримання графену науковцями Манчестерського університету А.Геймом та К.Новосьоловим, за що у 2010 році вони отримали Нобелівську премію по фізиці. Їхні праці створили теоретичне підґрунтя для численних наукових досліджень прикладного характеру та розвитку технологій застосування графену в промисловості та енергетиці. Таким чином, за останні 10 років відбувається стрибкоподібне зростання технологій використання графену в різних сферах.

Значний вплив емерджентної технології зумовлює її використання у найрізноманітніших сферах людської діяльності. При цьому доволі часто первинне призначення технології змінюється і передбачити напрями застосування тих чи інших особливостей технології неможливо.

Наприклад, запропонований свого часу вид технології розподіленої обробки даних, що став відомий як «блокчейн», може бути використаний не лише для створення і застосовування альтернативних грошових одиниць, які не емітує держава, але і для зберігання різноманітної критично важливої інформації з гарантією захисту від знищення, втручання та змін, що має значення для різноманітних сфер – від державних реєстрів до генних досліджень.

[79] Rotolo D., Hicks M., Martin B. What Is Emerging Technology? Working Paper of Science Policy Research Unit. Falmer: University of Sussex, 2015. 46 p.

На нашу думку, у вітчизняній науковій літературі також доцільно використовувати термін «емерджентний» стосовно найменування таких технологій.

Під «емерджентною технологією» у контексті розгляду питань правового регулювання відповідних суспільних відносин пропонується розуміти таку технологію що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед.

За таких умов існуюча у державі правова регламентація планування у цій сфері зводиться до правового забезпечення державної політики стосовно науково-технічного розвитку і навряд чи буде адекватною стану суспільних відносин.

З урахуванням стрибкоподібного характеру розвитку, що притаманний для емерджентних технологій, на сьогодні можливо лише визначити доволі приблизний перелік таких технологій. Зокрема, зазвичай до них відносять «мікро-літальні апарати» (MAV, різновид некерованих літальних апаратів малих та над-малих розмірів), «об'ємний друк» (комп'ютерний 3D-друк, клейтроніка, наноассемблер), технології на основі використання фулеренів та графену, біометрія, «гнучка електроніка» тощо.

Що стосується правового регулювання суспільних відносин у контексті застосування емерджентних технологій, то зазначене розглядалось насамперед з точки зору відповідного урядування та державного регулювання.

Потреба в державному регулюванні цієї сфери виникає насамперед як відповідь суспільному запиту на безпеку. Першим питанням, яке потребує невідкладного вирішення, є питання безпеки (заборони на заподіяння шкоду та ефективне і швидке відшкодування), а отже з точки зору теорії права мова йде про юридичну відповідальність. У другій частині питання у повному обсязі можуть бути застосовані загальні положення цивільного права. Що стосується державних заборон, то ситуація у цій сфері не настільки однозначна.

Емерджентна технологія ґрунтується на вже існуючих і має безпосереднє призначення, але має стрибкоподібний характер, що призводить до неможливості визначати наперед сферу застосування, а це обмежує заходи регламентації. У сучасних економічно розвинутих країнах мета регуляторного впливу держави полягає у досягненні насамперед мети належного функціонування вільного ринку та вільної економіки, що стосується фінансової, банківської сфери, біржової торгівлі, зв'язку, транспорту, тощо. При цьому регуляторні органи, як правило, не є органами державного управління, що прямо підпорядковані урядам, а формуються на паритетних засадах за законодавчо визначеною процедурою. Беручи до уваги таку схему державного регулювання, питання його традиційного здійснення у фінансовій сфері або у біржовій торгівлі не викликає складнощів, оскільки відповідним фахівцям відома уся можлива інформація стосовно технологій, які застосовуються, та інші відомості, що здійснюють вплив на ринок. Інша річ – це новітні технології у фінансовій сфері. Очевидно, що у питанні застосування криптовалют регуляторний вплив у більшості країн здійснюється із значним запізненням оскільки складність проблем, які породжені застосування емерджентної технології «блокчейн», виходить далеко за традиційні рамки уявлень про фінансовий ринок, а стрибкоподібний характер технології зводить нанівець усі існуючі механізми регулювання станом «на сьогодні». Водночас дії державних органів по регуляторному впливу особливо у випадках коли вони здійснюють пряме управління у цій сфері не передбачають динамічний характер технологій.

Наприклад, у ситуації із державними обмеженнями стосовно криптографічного захисту інформації мета таких обмежень з боку Уряду США полягала у недопущенні використання криптографії терористичними та організованими злочинними угрупованнями. При цьому державна політика ґрунтувалась ще на законодавстві 1950-70-х років, що містило заборони для експорту товарів та технологій до СРСР і його союзників.

Розповсюдження відкритих програмних засобів складного шифрування призвело до того, що зашифровані повідомлення не могли бути відкриті та прочитані правоохоронними органами. Намагання встановити

певні обмеження щодо вільного розповсюдження таких програм призвело до бурхливої дискусії у засобах масової інформації, а також судових процесів між громадськими активістами у сфері захисту приватності та державними органами. Як зазначила одна із громадських організацій – Фундація досліджень інформаційної політики (FIPR) у своєму маніфесті від 25 травня 2005 року «криптографічна війна» з урядом вважається закінченою у зв'язку із прийняттям Урядом США відповідних заходів з послаблення режиму обмежень доступу до криптографічних засобів.

Суть спору, який тривав з початку 1970– років полягала у обмеженні стосовно проведення досліджень у сфері стійких криптографічних ключів недержавними установами та приватними особами, а також щодо розповсюдження таких технологій поза межами державних органів і установ. Зазначена проблема виникла після вільного розповсюдження у глобальній комп'ютерній мережі першої програми стійкого шифрування PGP, що викликало подальший судовий процес американських правоохоронних органів щодо її розробника Ф.Ціммермана та кампанії захисників громадянських прав прихильників приватності. Зазначене завершилось ослабленням державного впливу, а самі події увійшли в історію під назвою «криптографічних воєн»[80]. Сама собою криптографічна технологія стійких шифрів не є емерджентною, але саме вона стала підґрунтям для справді емерджентної технології – «блокчейну». При цьому фахівці, що займалися розробкою такої технології не уявляли можливості її використання, які з'явились у зв'язку зі створенням DL-технолгій.

Повертаючись до державного регулювання емерджентних технологій у контексті реалізації функції держави слід визначити низку основних ключових моментів.

По-перше, мова повинна йти про забезпечення реалізації основної функції держави – загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії насамперед стосовно заздалегідь деструктивних технологій. Основна проблема полягає у неочевидності

[80] Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: АСТ-Астрель, 2007.

деструктивності і можливих помилок в оцінці суті технологій. Так на сьогодні, досить неоднозначна ситуація із правовими обмеженнями у сфері використання технологій генної модифікації. Широка кампанія проти генно-модифікованих організмів спирається на не до кінця встановлені факти, а уявно випереджувальна функція правових норм заборони може лише загальмувати технологічний прогрес в окремих державах.

По-друге, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції.

По-третє, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності. На жаль у чинному вітчизняному законодавстві норми стосовно розвитку інноваційної діяльності, а також відповідні заохочення багато у чому мають суто декларативний характер.

Зазначене дозволяє прийти до наступних загальних висновків стосовно загального впливу комп'ютерних технологій на кіберзагрози.

По-перше, серед інформаційно-компютерних технологій можливо виділити певну їх частину під умовною назвою «емерджентні технології», які проявляються у багатьох галузях науки і техніки. Під «емерджентною технологією» у контексті розгляду питань правового регулювання відповідних суспільних відносин пропонується розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед. Досить значна кількість технологій, що застосовуються в інформаційній сфері зумовлює виникнення і розвиток таких «емерджентних технологій» та їх стрибкоподібний і глобальний вплив.

По-друге, найбільш яскраво зазначені вище фактори проявляються у таких прикладах як: технології Інтернету речей, технології розподіленої

обробки (грід-технології, «хмарні технології», DL-технології), технології криптографії. Для емерджентних технологій, що застосовуються в інформаційній сфері і діють у кіберпросторі характерні тісний взаємозв'язок та взаємний вплив.

По-третє, загрози, що існують у кіберпросторі за весь час його існування модифікуються та інтенсифікуються за умови використання емерджентних технологій, при цьому такі технології мають потенціал їх збільшення.

По-четверте, у питанні правового регулювання як реалізації функцій держави, зокрема щодо забезпечення кібербезпеки та протидії кіберзагрозам слід виходити насамперед з загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії – зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій. Основна проблема полягає у неочевидності деструктивності і можливих помилок в оцінці суті технологій, тому пошук можливих шляхів вирішення зазначеної низки проблем є перспективним для подальших досліджень у галузі правової науки.

Окрім цього, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. Водночас, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності.

РОЗДІЛ 4.
РОЗВИТОК ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ КІБЕРБЕЗПЕКИ

Після ухвалення 20 грудня 2002 року Генеральною асамблею ООН резолюції 57/239 «Елементи для створення глобальної культури кібербезпеки»[81] термін «кібербезпека» почав активно використовуватись у вітчизняній правовій термінології. До цього поняття кібербезпеки у понятійному апараті нормативно-правових актів не використовувалось і в основному сприймалось як технічний термін у контексті заходів технічного захисту інформації.

Слід зазначити, що ситуація з правової регламентацією у сфері кібербезпеки, як і ситуація з правовою безпекою у кіберпросторі взагалі нагадувала правовий стан, що існував у період «фронтиру» (прикордоння) Дикого Заходу США у XIX сторіччі, а сам по собі кіберпростір сприймався як «новий фронтир»[82]. Такий правовий стан не означає, що право як регулятор відносин відсутнє як таке, або не діє узагалі. Скоріше мова йде про намагання пристосувати для потреб, що складаються або динамічно змінюються, вимоги чинного законодавства, яке створене для регламентації дещо інших суспільних відносин, або здійснювати спроби саморегуляції відносин їх учасниками (переговорами у режимі реального часу, намаганням створити приписи-рекомендації, або формуванням приписів, що можуть розглядатись як перед-право). Інколи намагались регламентувати відносини суто індивідуально та у залежності від конкретних ситуацій, не вдаючись до необхідності зовнішнього регулятора у вигляді права.

Для того щоб дослідити питання імплементації положень резолюції ООН варто більш детально проаналізувати її зміст.

Зокрема, Генеральна асамблея ООН констатувала, що стрімкий розвиток інформаційної технології означає зміну підходів державних органів,

[81] Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 27.11.2017).

[82] Kamal Ahmad. The Law Of Cyber-Space. Geneve: UNITAR, 2005.269 p. – P.3

організацій та індивідуальних користувачів до питання кібербезпеки. Звичайно, що комп'ютерна злочинність виникла одночасно із розповсюдженням комп'ютерних мереж, тому протидія комп'ютерній злочинності (та кіберзлочинності) було предметом міжнародного співробітництва, починаючи з 1990-х років[83]. Але питання забезпечення кібербезпеки вийшло далеко за межі діяльності правоохоронних органів із протидії злочинності, оскільки загрози у цій сфері не обмежуються лише злочинною діяльністю. У термінології, яку використовує ООН, мова йде про глобальну культуру кібербезпеки.

Після короткої констатації стану справ визначено дев'ять взаємопов'язаних елементів, яких потребуватиме глобальна культура кібербезпеки, а саме:

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

– *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі);

– *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявленню та реагуванню, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективні співробітництво з попередження, виявлення та реагування таки інцидентів);

– *етика* (врахування законних інтересів інших);

– *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; відкритість та гласність);

– *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації, яка захищається);

[83] Волеводз А.Г. Противодействие компьютерным преступлениям. Правовые основы международного сотрудничества. М.:Юрлитинформ, 2002.496 с. – С. 9-11.

– *проектування та впровадження засобів забезпечення безпеки*;

– *переоцінка* (належні та своєчасні заходи з внесення змін в політику, практику забезпечення безпеки з врахуванням нових та зміни існуючих загроз).

На 58-й сесії Генеральної асамблеї ООН 23 грудня 2003 року в розвиток раніше ухвалених положень прийнято резолюцію 58/199 «Створення глобальної культури кіберпростору і захист найважливіших інформаційних інфраструктур», що містить як додаток документ під назвою «Елементи для захисту найважливіших інформаційних інфраструктур»[84]. Зазначений документ фактично містить вимоги до систем забезпечення кібербезпеки у напряму захисту найважливіших інформаційних інфраструктур. Резолюція «Створення глобальної культури кібербезпеки та оцінка національних зусиль про захист найважливіших інформаційних інфраструктур», ухвалена на 64-й сесії Генеральної асамблеї ООН 21 грудня 2009 року[85], має на меті оцінити ефективність заходів, що вживались на виконання зазначених вище резолюцій Генеральної асамблеї. Для цього було обрано метод проведення самооцінки на підставі доданого документу – «Інструменту національної самооцінки національних зусиль щодо захисту найважливіших інформаційних інфраструктур». Окрім цього, технічні питання заходів із забезпечення кібербезпеки були викладені у Глобальній програмі кібербезпеки Міжнародного союзу електрозв'язку 2007 року[86].

В Україні правова регламентація питань ужиття заходів з кібербезпеки (окрім деяких суто кримінально-правових аспектів) в основному було зумовлено вимогами євроатлантичної інтеграції держави і випливало з доктрин, стратегій та настанов НАТО і Євросоюзу. Як було зазначено

---

[84] Резолюция Генеральной Ассамблеи ООН 58/199, принятая на 78 пленарном заседании 58-й сессии. 23 декабря 2003 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement (дата звернення: 27.11.2017).

[85] Резолюция Генеральной Ассамблеи ООН 64/211, принятая на 66 пленарном заседании 64-й сессии. 21 декабря 2009 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement (дата звернення: 27.11.2017).

[86] Global Cybersecurity Agenda (GCA). 17.09.2007 URL: https://www.itu.int/ITU-D/cyb/events/2007/Geneva/docs/kitaw-global-cybersecurity-agenda-geneva-17-sept-07.pdf (дата звернення: 27.11.2017).

вище, питання забезпечення кібербезпеки далеко не вичерпані кримінально-правовими аспектами, тому доцільно проаналізувати стан регламентації цих питань на рівні документів стратегічного планування у сфері національної безпеки України.

Відповідно до ст. 2 чинної редакції Закону України «Про основи національної безпеки України»[87] цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обстановці з метою своєчасного виявлення, відвернення і нейтралізації реальних, і потенційних загроз національним інтересам України визначаються Стратегією національної безпеки України і Воєнною доктриною України. Ці документи є документами, обов'язковими для виконання і основою для розробки конкретних програм за складовими державної політики національної безпеки.

До прийняття Закону України «Про основи національної безпеки України» питання державної політики у сфері забезпечення національної безпеки регламентувались Концепцією (основами державної політики) національної безпеки України, схваленою постановою Верховної Ради України від 16 січня 1997 року № 3/97[88]. Оскільки статус зазначеного документа у правовій системі держави був неоднозначним, а п. 17 ст. 92 Конституції України містить прямий припис, що основи національної безпеки повинні визначатись виключно законами України, Концепція втратила чинність одночасно із прийняттям 19 червня 2003 року Закону України «Про основи національної безпеки України».

Слід зазначити, що положення цього Закону оминули питання регламентації забезпечення кібербезпеки. Серед загроз національній безпеці України у сфері інформаційної безпеки ст. 7 Закону було визначено комп'ютерну злочинність та комп'ютерний тероризм.

---

[87] Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV: Дата оновлення 30.11.2017. URL: http://zakon3.rada.gov.ua/laws/main/964-15 (дата звернення: 03.12.2017).

[88] Про Концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16.01.1997: Дата оновлення 22.07.2003. URL: http://zakon3.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80 (дата звернення: 03.12.2017).

У подальшому у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12 лютого 2007 року № 105[89], стан безпеки інформаційно-комп'ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій охарактеризовано як такий, що *«наближається до критичного»*. Таким чином на підставі проведеного аналізу РНБО України було зроблено висновок про стан справ і щодо реального рівня небезпеки, оскільки висновок про критичний стан систем було зроблено не тільки із врахуванням їх вразливості перед проявами комп'ютерної злочинності, а й виходячи із усього спектра питань підтримання зазначених систем у належному технічному стані, що дає змогу адекватно та ефективно виконувати поставлені завдання.

Окрім цього, у п. 4.1 зазначеної Стратегії з метою реалізації державної політики було визнано за необхідне розробку та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність. Варто зазначити, що запропонований у першій редакції Стратегії національної безпеки підхід, який з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов'язань та вимог гармонізації законодавства до європейських стандартів, був цілком адекватним тодішній обстановці та повністю відповідав елементам для створення глобальної культури кібербезпеки, визначеним резолюцією Генеральної асамблеї ООН.

У подальшому Указом Президента України від 8 червня 2012 року № 389 було затверджено нову редакцію Стратегії національної безпеки

[89] Стратегія національної безпеки України: затв. Указом Президента України від 12.02.2007 № 105. Офіційний вісник України. 2007. 23.02.2007. № 11. С. 7. Ст. 389.

України «Україна у світі, що змінюється»[90]. Прийняття нової редакції Стратегії було зумовлено в основному політичними причинами, зокрема призупиненням поступу до євроатлантичної інтеграції.

Зазначений документ доктринального характеру, характеризуючи безпекове середовище, серед чинників впливу на національну безпеку визначав і нездатність держави протистояти викликам, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. При цьому на той час залишалась без змін і редакція ст. 8 Закону України «Про основи національної безпеки України», яка серед загроз в інформаційній сфері визначала такі:

«– прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації».

Отже, визначені на рівні документу стратегічного планування новітні виклики та загрози фактично не імплементовано на рівні спеціального законодавчого акту, що регламентує основи національної безпеки, оскільки комп'ютерна злочинність та комп'ютерний тероризм далеко не повністю охоплюють такі загрози.

Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково також було зазначено наступні:

«– стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

[90] Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України»: Указ Президента України від 08.06.2012 № 389. Офіційний вісник України. 2012. 22.06.2012. № 45. С. 104. Ст. 1749.

– забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;

– створення національної системи кібербезпеки».

Отже, мова йшла про низку реальних заходів організаційного характеру, у тому числі і створення національних систем управління у цій сфері.

У сучасних умовах фактичної гібридної війни, яка ведеться проти України в активній фазі з весни 2014 року, питання забезпечення кібербезпеки має надзвичайно важливе значення.

Доречно, що у такій гібридній війні значне місце мають бойові дії у кіберпросторі. Йдеться про «кібератаки», які вочевидь здійснювались та підтримувались іноземними державами, і за своєю суттю мали характер агресії. Можна стверджувати, що застосування існуючих категорій війни до таких дій відбулося після так званих «естонських кіберінцидентів» 09.05.2007.

«Естонськими кіберінцидентами» називають масштабні дії, сплановані та скоординовані з Росії, стосовно державних органів та об'єктів інфраструктури Естонії, які відбувались у кіберпросторі і полягали у нанесенні шкоди зазначеним об'єктам[91]. «Естонські кіберінциденти» були першими такими діями і за своїми наслідками призвели до збитків для інфраструктури держави, хоча і в менших масштабах ніж кібератаки проти України 2015-2017 років. Але реагування на зазначені інциденти з боку НАТО відбувалось в декількох сферах, однією з яких була сфера застосування положень міжнародного права, а саме права війни, до кібервійни, яка відбувається у кіберпросторі, інші стосувались реформування системи протидії загрозам воєнного характеру і кіберпросторі та технічне удосконалення існуючих систем кіберзахисту[92].

---

[91] Czosseck C., Ottis R, Taliharm A-M. Estonia after 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security// Proceedings of the 10th European Conference on Information Warfare and Security: 10th European Conference on Information Warfare and Security, Tallinn, 7-8 July 2011. Ed. Ottis, R. Reading, UK: Academic Publishing Limited, P. 57−64.

[92] Ilves L., Evans T., Ciluffo F., Nadeau A. European Union and NATO Global Cybersecurity Challenges. URL: http://cco.ndu.edu/LinkClick.aspx?fileticket=HVj82hUX7_s%3D&portalid=96 (дата звернення: 03.12.2017).

Питання забезпечення кібербезпеки виділені у чинній редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року № 287[93]. Зокрема, серед загроз інформаційній безпеці визначено:

«– ведення інформаційної війни проти України;

– відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства».

Перша з окреслених загроз констатує факт наявності інформаційної війни проти нашої держави як продовження бойових дій специфічними методами. Друга визначає умови, за яких методи інформаційної війни, що застосовуються противником, досягають поставлених ним цілей.

Загрозами кібербезпеці і безпеці інформаційних ресурсів згідно з положеннями Стратегії є:

«– уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

– фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом».

Таким чином, у чинній Стратегії національної безпеки України характеристика загроз кібербезпеці обмежена, а фактично її зведено лише до проведення кібератак щодо державних інформаційних ресурсів та застарілості системи охорони інформації з обмеженим доступом, хоча дещо застаріла система зберігання інформації з обмеженим доступом переважно на паперових носіях інформації робить таку систему досить стійкою з точки зору загроз саме у сфері кібербезпеки. З іншого боку визначення Стратегією як окремої загрози ведення інформаційної війни проти України розширило поле, що характеризує загрози у кіберпросторі.

Формулюючи основні напрями державної політики щодо забезпечення кібербезпеки та інформаційної безпеки, внаслідок розділення цих сфер безпеки, не вдалося уникнути певного дуалізму і у формулювання напрямів політики. Зокрема, створення інтегрованої системи оцінки інформаційних

[93] Стратегія національної безпеки України: затв. Указом Президента України від 26.05.2015 № 287. Офіційний вісник України. 09.06.2015. № 43. С. 14. Ст. 1353.

загроз та оперативного реагування на них і моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації є багато у чому пов'язаними заходами. До того ж розвиток інформаційної інфраструктури держави стосується не тільки забезпечення кібербезпеки, а й інформаційної безпеки також.

У подальшому основні напрями державної політики забезпечення саме кібербезпеки було окреслено у Стратегії кібербезпеки України, яку затверджено Указом Президента України від 15 березня 2016 року № 96[94]. Метою цієї Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Як показує аналіз пріоритетів та напрямів державної політики щодо забезпечення кібербезпеки, що визначені у розділі 4 Стратегії кібербезпеки, переважна більшість з них стосуються організаційних заходів, які є взаємопов'язаними і повинні складати відповідну систему забезпечення кібербезпеки. Що стосується заходів правового регулювання питань забезпечення кібербезпеки, то Стратегією визнано за доцільне проведення гармонізації вітчизняного законодавства у відповідність до вимог НАТО та ЄС, комплексне вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, подальшого розвитку кримінально-правової охорони суспільних відносин у цій сфері, боротьбу з кіберзлочинністю.

На виконання Стратегії кібербезпеки України розпорядженням Кабінету Міністрів України від 24 червня 2016 року № 440-р було затверджено план заходів на 2016 рік з реалізації зазначеної Стратегії[95]. У цьому розділі неможливо провести аналіз здійснення державними органами положень зазначеного плану, проте скоріше за все його виконання було незадовільним. Тому рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року, введеним в дію Указом Президента України від 13 лютого 2017 року № 32 акцентовано увагу на необхідності термінової підготовки законодавчих пропозицій щодо кіберзахисту об'єктів критичної

[94] Стратегія кібербезпеки України: затв. Указом Президента України від 15.03.2016 № 96. Офіційний вісник України. 29.03.2017. № 23. С. 69. Ст. 899.

[95] План заходів на 2016 рік з реалізації Стратегії кібербезпеки України: затв. Розпорядженням Кабінету Міністрів України від 24.06.2016 № 440-р. Урядовий кур'єр. 05.07.2016. № 123.

інформаційної інфраструктури, посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах та законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України, а також щодо запровадження відповідальності за невиконання законних вимог посадових осіб Служби безпеки України, а також розробки низки правових новел у сфері кібербезпеки[96].

Ужиття заходів, визначених Стратегією національної безпеки України, затвердженою Указом Президента України від 26 травня 2015 року № 287 та Стратегією кібербезпеки, затвердженою Указом Президента України від 15 березня 2016 року № 96, зумовило зміни у чинному законодавстві, насамперед з метою подальшого унормування суспільних відносин, пов'язаних з реалізацією таких функцій держави, як оборона та забезпечення державної безпеки.

На розвиток цього ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14 березня 2016 року № 92, Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 6 червня 2016 року № 240, Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242, Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23 серпня 2016 року № 563 та низка інших.

Переважна більшість з них встановлює загальні засади державної політики і визначає окремі підходи до унормування питань забезпечення кібербезпеки. Водночас, деякі заходи та стратегічні підходи не повною мірою базуються на науковому підґрунті, що неодмінно призведе до виникнення спірних питань стосовно правової регламентації.

---

[96] Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: рішення Ради національної безпеки і оборони України, уведено в дію Указом Президента України від 13.02.2017 № 32. Урядовий кур'єр. 16.02.2017. № 30.

Окремо слід згадати спеціальний законодавчий акт з питань кібербезпеки – «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, що досить тривалий час розглядався Верховною Радою України і був неоднозначно сприйнятий суспільством та бізнес-спільнотою. Згідно п. 1 його Прикінцевих та перехідних положень Закон набуває чинності через 6 місяців після його опублікування. Офіційне опублікування тексту законодавчого акту відбулось у газеті «Голос України» 9 листопада 2017 року, тому він набирає чинності 9 травня 2018 року – рівно через 11 років після «естонських кіберінцидентів».

Як визначено у його преамбулі, цей Закон *«визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки»*[97].

Отже, згідно задекларованих у преамбулі положень законом фактично встановлюються можливість та засади регулювання за допомогою норм вітчизняного права у кіберпросторі з метою забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, а також національних інтересів України.

Частина 1 стаття 2 Закону містить виключення щодо його дії. Зокрема, Закон не поширюється на:

«1) відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

[97] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)»[98].

Зазначені правові дефініції потребуватимуть у майбутньому роз'яснення і не виключено, що призведуть до подальших змін у чинному законодавстві. Аналіз приписів, що містяться у пунктах 1 та 4 частини 1 статті 2 дозволяє зробити висновок про їх тотожність у багатьох аспектах. Узагальнюючи зазначене, можливо зробити висновок, що дія Закону не розповсюджуватиметься на внутрішні (локальні) комп'ютерні мережі, що не взаємодіють (не підключені) до глобальних комп'ютерних мереж. Обмеження щодо інформації, яка становить державну таємницю, діятимуть відповідно до приписів актів спеціального законодавства у цій сфері. Водночас, відносини, що складаються при використанні соціальних мереж, а також «приватних» інформаційних електронних ресурсів (однак, судячи з усього мова йде про недержавні ресурси) не регламентуються Законом «Про основні засади забезпечення кібербезпеки в Україні» за певних умов – відсутності інформації, необхідність захисту якої встановлено законом. Зазначене положення викликатиме певні труднощі оскільки приписи чинної редакції Закону України «Про інформацію»[99](ст. 10) визначає 9 видів інформації і цей перелік не є вичерпним. Згідно ст. 11 цього ж Закону обмеження встановлені щодо інформації про фізичну особу (персональні дані), а щодо інших визначено наявність особливостей правового режиму щодо кожного виду, який встановлюватиметься законодавчими актами.

[98] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

[99] Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 01.01.2017. URL: http://zakon3.rada.gov.ua/laws/main/2657-12 (дата звернення: 03.12.2017).

Щодо обмеженості доступу до інформації, то відповідно до ст. 21 Закону «Про інформацію» встановлено 3 види інформації з обмеженим доступом – конфіденційна, таємна та службова. Конфіденційною при цьому вважається інформація про фізичну особу, а також інформація доступ до якої обмежено фізичною чи юридичною особою за умови неналежності цієї інформації до публічної. Таким чином, визначення належності чи неналежності функціонування тих чи інших «приватних» електронних ресурсів та соціальних мереж до сфери дії Закону «Про основні засади забезпечення кібербезпеки України» є складним питанням, що потребуватиме додаткових роз'яснень.

Слід зазначити і дещо ускладнену конструкцію з визначенням принципів забезпечення кібербезпеки. Річ у тім, що Закон встановлює два види принципів.

Зокрема, частина 2 статті 2 визначає, що застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням таких принципів:

«1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб'єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

2) об'єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов'язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб'єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб'єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов'язків особи, який є:

відмінним від обсягу прав та обов'язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов'язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об'єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції»[100].

Частина із цих принципів є теоретичними положеннями щодо загального предмету правового регулювання та законодавчої техніки і мають застосовуватись до усіх актів законодавства. Окрім цього, стаття 7 Закону визначає окремо і «принципи забезпечення кібербезпеки», відносячи до них наступні:

«1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

[100] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки»[101].

Деякі з визначених принципів корелюються із принципами, встановленими щодо інших правовідносин у спеціальних законодавчих актах. Частина ж приписів статей 2 та 7 Закону корелюються одне з одним, хоча й уникаючи протиріч.

Закон встановлює перелік об'єктів кібербезпеки та кіберзахисту. Під кібербезпекою розуміється *«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*

[101] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а під кіберзахистом – *«сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»* (пункти 5 та 7 частини 1 статті 1 Закону). Таким чином деякі об'єкти можуть бути одночасно об'єктами і кібербезпеки, і кіберзахисту.

Зокрема, об'єктами кібербезпеки є:

«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».

Останній з об'єктів кібербезпеки (як об'єкт критичної інформаційної інфраструктури) є одночасно і об'єктом кіберзахисту. Законодавець до їх числа відносить зокрема:

«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»[102].

[102] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

Зазначений перелік є вичерпним хоча і зумовлює необхідність у додаткових роз'ясненнях. Зокрема, встановлено, що перелік об'єктів критичної інформаційної інфраструктури визначає Кабінет Міністрів України та Національний банк України. З об'єктами критичної інфраструктури ситуація не така однозначна. Зокрема, постановою Кабінету Міністрів України від 23 серпня 2016 року № 563 затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Зазначений перелік затверджується Кабінетом Міністрів України на підставі погоджених з СБУ пропозицій державних органів, що подаються до Адміністрації Держспецзв'язку України. Слід зазначити, що чинне законодавство містить дещо неузгоджені терміни оскільки за буквальним тлумаченням приписів нормативно-правових актів одночасно Кабінет Міністрів України вестиме переліки об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури та інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави[103].

Питання визначення таких об'єктів на жаль попри на очевидну важливість для забезпечення національної безпеки дещо розпорошується у сучасних умовах, оскільки у літературі та деяких нормативно-правових документах вживаються терміни щодо об'єктів критичної інфраструктури у різних сферах, а переліки таких об'єктів по суті несформовані.

Окрім цього виникатиме питання і щодо суб'єктів, підстав та порядку прийняття рішень стосовно належності конкретних комунікаційних систем до об'єктів кіберзахисту в розумінні Закону України «Про основні засади забезпечення кібербезпеки України». Тим більше, що ужиття терміну «комунікаційна система» не спирається на законодавчу дефініцію.

У питанні визначення суб'єктного складу забезпечення кібербезпеки законодавець визначив окремо перелік власне суб'єктів її забезпечення (ст. 5) та суб'єктів Національної системи кібербезпеки (ст. 8).

---

[103] Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: затв. Постановою Кабінету Міністрів України від 23.08.2016 № 563. Урядовий кур'єр. 08.09.2016. № 168.

Згідно приписів ч. 1 ст. 5 Закону координацію діяльності у сфері кібербезпеки здійснює Президент України. Таке повноваження ґрунтується на законодавчому розумінні кібербезпеки як складової національної безпеки і випливає із положень статті 106 Конституції України, згідно яких Президент України забезпечує національну безпеку. Зазначене повноваження реалізується через очолювану Президентом України Раду національної безпеки і оборони України. Отже, законодавець встановив і певний механізм реалізації повноважень Президента України щодо здійснення ним повноважень із координації діяльності у сфері кібербезпеки, що ґрунтується на визначеному ст. 107 Конституції України статусі Ради національної безпеки і оборони України як координаційного органу при Президентові України. Окрім цього, згідно з вимогами ст. 3 Закону України «Про Раду національної безпеки і оборони України» до її функцій належить, окрім іншого, координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони.

Указом Президента України від 7 червня 2016 року № 242/2016 (тобто ще до прийняття Закону України «Про основні засади забезпечення кібербезпеки України») затверджено Положення про Національний координаційний центр кібербезпеки[104], керівником якого є секретар Ради національної безпеки і оборони України. Склад центру визначено п. 5, зокрема до його складу входять секретар РНБО України, як керівник Центру за посадою, секретар Центру, яким за посадою є керівник структурного підрозділу з питань кібербезпеки у складі Апарату РНБО України, а також перші заступники (або заступники) Міністра оборони України, начальника Генерального штабу Збройних Сил України, Голови Служби безпеки України, Голови Служби зовнішньої розвідки України, Голови Національної поліції України, Голови Національного банку України (за згодою), до відання яких належать питання кібербезпеки, а також начальник Головного управління розвідки Міністерства оборони України, начальник Управління розвідки Адміністрації Державної прикордонної служби України, Голова Державної

[104] Про національний координаційний центр кібербезпеки: затв. Указом Президента України від 07.06.2016 № 242. Офіційний вісник України. 21.06.2016. № 46. С. 8. Ст. 1665.

служби спеціального зв'язку та захисту інформації України. Формою роботи зазначеного Центру є засідання, що відповідно до п. 8 Положення про нього проводяться за потреби, але не рідше одного разу в квартал.

Компетенція Національного координаційного центру кібербезпеки визначена ч. 2 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема Центр 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.

До числа завдань Кабінету Міністрів у сфері забезпечення кібербезпеки згідно Закону належить забезпечення *«формування та реалізації державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьба з кіберзлочинністю»*.

Окрім цього, Кабінет Міністрів України *«організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України)»*[105]. Останнє завдання визначено для Національного банку України. Такий подвійний характер завдань щодо Кабінету Міністрів України та Національного банку України може зумовити у подальшому і виникнення питання щодо розмежування компетенції у цій сфері між Кабінетом Міністрів України та іншими органами влади зі спеціальним статусом (Верховна Рада України та її апарат, судові органи, прокуратура, національні комісії, що здійснюють державне регулювання, Антимонопольний комітет України, державні органи при Верховній Раді України, а також державні органи, що за чинним законодавством не входять до системи центральних органів виконавчої влади, зокрема Служба безпеки України, Служба зовнішньої розвідки України та Управління державної

[105] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

охорони, антикорупційні органи). У будь-якому разі це ускладнюватиме визначення об'єктів для кіберзахисту на практиці.

До числа суб'єктів забезпечення кібербезпеки законодавець також включив:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадян України та об'єднання громадян, інших осіб, 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.

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»[106].

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

Стаття 6 Закону України «Про основні засади забезпечення кібербезпеки України» визначає «об'єкти критичної інфраструктури» як підприємства, установи і організації, що відповідають певним критеріям. Беручи до уваги сферу дії закону можливо визначити, що мова йде про об'єкти критичної інфраструктури щодо яких існують загрози у кіберпросторі. На нашу думку, саме собою визначення таких об'єктів та їх вразливості від традиційних військових дій та актів розвідувально-підривної діяльності за своєю сутністю виходить за межі сфери правового регулювання, встановлені Законом України «Про основні засади забезпечення кібербезпеки України». Тобто це визначення має бути відображено в актах спеціального законодавства у сфері забезпечення національної безпеки.

Як зазначалося вище, конкретні критерії віднесення тих чи інших об'єктів до числа об'єктів критичної інфраструктури передбачені законом, але рішення про віднесення конкретного об'єкту прийматиме Кабінет Міністрів України або Національний банк України на підставі та у порядку, визначеному законодавством. Закон містить поняття застосування *«індикаторів кіберзагроз»* як основи для вироблення критеріїв віднесення об'єктів та прийняття з цього приводу відповідних рішень. Такими *«індикаторами кіберзагроз»* ст. 1 Закону визначено вважати *«показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози»*.

Закон вводить також поняття «аудиту» та «незалежного аудиту» інформаційної безпеки, хоча сферою регулювання Закону є кібербезпека,

[106] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).

а не інформаційна безпека. Щодо об'єктів критичної інфраструктури Кабінетом Міністрів України має бути сформована система аудиту інформаційної безпеки на таких об'єктах. Щодо інших об'єктів проведення аудиту покладено на суб'єкти забезпечення кібербезпеки.

Слід зазначити, що термін *«незалежний аудит»* законодавець не визначив, хто саме і в якому порядку повинен його проводити. Буквальне тлумачення правового припису дозволяє прийти до висновків, що мова йде про діяльність зовнішнього суб'єкта, а чи буде це господарською, фаховою чи іншою діяльністю наразі з тексту Закону не випливає. Зазначене питання скоріше за все буде вирішуватись у практичній площині, беручи до уваги приписи стосовно порядку розробки нормативно-правових актів з питань такого аудиту та існування суб'єктів господарювання, що здійснюють заходи з аудиту систем безпеки у різних сферах.

Як вже зазначалось, відповідно до вимог ст. 6 Закону *«розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов'язковим залученням представників основних суб'єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій»*.

Закон вводить нове поняття – Національна система кібербезпеки. Стаття 8 Закону визначає її як *«сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури»*. Отже зазначену систему складають одночасно суб'єкти та заходи. До числа суб'єктів (основних суб'єктів за термінологією статті 8 Закону) системи законодавець відносить наступні:

– Державна служба спеціального зв'язку та захисту інформації України;

– Національна поліція України,

– Служба безпеки України,

– Міністерство оборони України та Генеральний штаб Збройних Сил України,

– розвідувальні органи,

– Національний банк України.

Конкретні повноваження суб'єктів Національної системи визначатимуться з урахуванням приписів спеціального законодавства, яке визначає їх компетенцію. Водночас для кожного із суб'єктів Національної системи Законом України «Про основні засади забезпечення кібербезпеки України» визначені конкретні завдання з урахуванням компетенції цих органів

Зокрема, згідно п. 1 ч. 2 ст. 8 Закону Державна служба спеціального зв'язку та захисту інформації:

– забезпечує формування та реалізацію державної 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 зазначених вище 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, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

– забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

При цьому Національна поліція України *«забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі». Служба безпеки України «здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і 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»*.

Функція забезпечення кібероборони, як *«сукупності політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії»* покладена на Міністерство оборони України та Генеральний штаб Збройних Сил України. Окрім цього для зазначених органів визначено завдання по здійсненню військової співпраці з НАТО та іншими суб'єктами оборонної сфери стосовно забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз. Також на них покладено завдання впровадження заходів

із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану.

Розвідувальним органам визначено завдання із здійснення розвідувальної діяльності в кіберпросторі відповідно до законодавчо визначеної для них компетенції. Зокрема мова йде про діяльність стосовно загроз національній безпеці, інших подій та обставин, які стосуються кібербезпеки.

Особливий статус Національного банку України проявляється і у визначенні його компетенції у сфері кібербезпеки. Зокрема до його основних завдань належить розробка порядку, вимог та заходів із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб'єктів переказу коштів, здійснення контролю за їх виконанням. Окрім цього, Національний банк створює власний центр кіберзахисту та забезпечує функціонування системи кіберзахисту у банківській системі України. Відповідно йому надано повноваження із забезпечення проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

На нашу думку, не досить вдало сформульовані заходи з кібербезпеки як складові Національної системи кібербезпеки. Визначені ст. 8 Закону 25 види заходів не прив'язані до конкретних суб'єктів. А сама система, враховуючи визначену законодавцем компетенцію, не є вертикальною системою, містить у собі фактично декілька паралельних систем за відсутності чітко визначеного органу, що формує державну політику в цій сфері.

Окрім цього, законодавцем передбачено створення ще двох органів (обидва у структурі Державної служби спеціального зв'язку і захисту інформації) – Державного центру кіберзахисту та Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA).

Мета та завдання Державного центру кіберзахисту визначені у ч. 5 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України». Зокрема, зазначений Центр здійснює впровадження організаційно-

технічної моделі кібербезпеки. Окрім цього, він *«забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події».* Також у взаємодії з іншими суб'єктами забезпечення кібербезпеки зазначений Центр *«розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань»*.

Компетенція Урядової команди реагування на комп'ютерні інциденти визначена ст. 9 Закону. Комп'ютерні групи реагування на надзвичайні ситуації (CERT є абревіатурою, утвореною від англомовного словосполучення *"computer emergency response team"*) створювались як команди експертів, що займаються збиранням інформації про кіберінциденти, їх класифікацією та нейтралізацією. Перші команди були вузькими групами технічних спеціалістів, залучених з числа дослідників університетів та наукових лабораторій. Слід зазначити, що в кожній державі є різні підходи до формування зазначених груп (команд) і далеко не завжди вони утворені як структурні підрозділи державних або правоохоронних органів. В Євросоюзі існує координуючий орган – Агентство Євросоюзу з питань мережевої та інформаційної безпеки (ENISA), що розміщений на території Греції. Українська команда CERT існує з 2007 року як структурний підрозділ Державної служби спеціального зв'язку і захисту інформації.

Завданнями команди відповідно до вимог ст. 9 Закону є:

«1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам».

Досить ґрунтовно в Законі визначені засади державно-приватної взаємодії у сфері кібербезпеки, хоча законодавець і утримався від вжиття для характеристики суті таких відносин терміну «партнерство». До числа основних форм взаємодії слід віднести створення (у т.ч. із залученням волонтерських організацій, хоча на нашу думку більш логічним було б вжиття терміну «громадських організацій» або громадськості та приватних осіб) системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз. Інші форми можливо диференціювати на:

– форми взаємодії у сфері належного інформування громадськості (а саме підвищення цифрової грамотності громадян та культури безпекового

поводження в кіберпросторі; розповсюдження комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки; реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту; обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об'єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів);

– форми взаємодії щодо надання сприяння приватних осіб, наукових установ, технічних спеціалістів та громадськості діяльності державних органів у сфері забезпечення кібербезпеки;

– форми взаємодії, пов'язані із належним громадським контролем за ефективністю заходів, що здійснюються для забезпечення кібербезпеки;

– форми взаємодії, пов'язані з налагодженням та функціонуванням системи діалогу між державними органами, відповідальними за забезпечення кібербезпеки із бізнес-середовищем, технічними спеціалістами, науковцями та громадськістю;

Також законодавець визначив для державних органів та органів місцевого самоврядування, їх посадових осіб, підприємств, установ та організацій незалежно від форми власності, окремих осіб, громадян та об'єднань обов'язок сприяти суб'єктам забезпечення кібербезпеки. У тому числі мова йде про покладання на зазначених вище суб'єктів обов'язку повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

Законом визначені також загальні засади юридичної відповідальності за порушення законодавства у сфері кібербезпеки. Так, стаття 12 Закону визначає, що кіберпростір може бути одночасно «місцем та способом вчинення» злочину чи іншого правопорушення. На сьогодні зазначені законодавчі положення потребуватимуть безумовного узгодження із існуючими нормами кримінального, адміністративного та цивільного права.

Процедура контролю у сфері кібербезпеки визначена законом достатньо повно. Водночас, виникає декілька моментів, що можуть ускладнити застосування норм права на практиці. Так, ст. 15 Закону визначено, що контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України, а контроль за діяльністю суб'єктів забезпечення кібербезпеки державними органами та суб'єктами сектору безпеки і оборони – Президентом України та Кабінетом Міністрів України у порядку визначеному Конституцію України та законами України. Але у подальшому законодавець встановлює процедуру звітування певним колом суб'єктів забезпечення кібербезпеки. До них належать Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. Ці органи мають провести *«незалежний аудит діяльності»* з дотриманням *«міжнародних стандартів аудиту»*. Зазначений звіт про результати проведеного аудиту має бути поданий одночасно Верховній Раді України, Кабінету Міністрів України та Верховній Раді України. У Верховній Раді України такі звіти розглядатимуть два Комітети Верховної Ради України. Тобто саме ці комітети фактично і представлятимуть Верховну Раду України, оскільки подальші їхні дії з цього приводу законодавчо не визначені. Окрім цього, стаття 14 Закону України «Про комітети Верховної Ради України», яка розкриває зміст контрольної функції комітетів, не містить згадок про заслуховування звітів за результатами «незалежного аудиту» та не окреслює подальші дії комітету з цього приводу.

Слід також зазначити, що формулювання, вжиті в абзацах четвертому та п'ятому ч. 3 ст. 15 Закону України *«Про основні засади забезпечення кібербезпеки України»* мають двояке значення оскільки одночасно згадують *«звіт про результати незалежного аудиту»* і *«звіт про стан виконання заходів з питань забезпечення кібербезпеки»*, що містить також інформацію про результати проведення незалежного аудиту. При цьому лише щодо другого з них визначена процедура розгляду – у Комітеті, до предмета

відання якого належать питання інформатизації та зв'язку, який *«може порушити питання про розгляд цих питань Верховною Радою України»*, хоча у чому полягають такі «питання» не роз'яснено.

У прикінцевих та перехідних положеннях Закону України «Про основні засади забезпечення кібербезпеки України» визначається строк набуття ним чинності, а також вносяться зміни і доповнення до чинних Законів України у частині регламентації повноважень Національного банку України, Міністерства оборони України, Генерального штабу Збройних Сил України, розвідувальних органів, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України.

Як вже зазначалось вище, 15 березня 2016 року було ухвалено новий вид документу стратегічного планування – Стратегію кібербезпеки України. Стосовно його правового статусу та місця в системі законодавства слід зазначити наступне. Його прийняття на той час не було викликано прямими вимогами чинного законодавства, оскільки Закон України «Про основи національної безпеки України» визначав необхідність ухвалення тільки Стратегії національної безпеки і Воєнної доктрини. Законом України «Про основні засади забезпечення кібербезпеки України», що набуває чинність 9 травня 2018 року, було внесено відповідні доповнення до Закону України «Про основи національної безпеки України», і це легітимізує статус Стратегії кібербезпеки.

Оскільки існування Стратегії кібербезпеки було новим для нашої держави, її розробка та ухвалення не зумовлювалося прямими вимогами чинного законодавства, можливо стверджувати, що при цьому керівництво держави не в останню чергу виходило з наявних у світовій політиці трендів забезпечення безпеки. Протягом останніх п'яти років такі стратегії, як документи стратегічного планування, ухвалено практично в усіх державах світу.

Незважаючи на різні правові та політичні системи, в їх переважній більшості демонструвались спільні підходи. Зокрема, спочатку характеризувалось безпекове середовище загалом, кібепростір та його вплив на середовище, наявні та потенційні загрози у цій сфері, а вже потім –

відповідні заходи реагування державних органів (або інших суб'єктів, що наділені відповідними повноваженнями) в залежності від характеру загроз. Слід зазначити, що заходи з протидії загрозам, як правило, не були деталізовані, а лише визначали відповідні напрями державної політики. У деяких випадках лише фіксувались загальні тренди.

Підхід, подібний до вище зазначеного застосовано у Стратегії кібербезпеки України.

Зазначений документ досить складний та комплексний і скоріше є документом визначення державної політики, аніж документом планування чи нормативно-правовим актом. Але все ж слід звернути увагу на певні аспекти правового характеру.

Насамперед, роль зазначених стратегічних документів в сучасній Україні не передбачає прямого впливу на державне управління, визначення організаційних заходів, також вони не є правовими нормами прямої дії. У цьому полягає їх сутність, хоча зазначене і викликає питання щодо їх місця у правовій системі нашої держави.

У той же час, характер організаційних заходів, який пропонується стратегічними документами (у тому числі Стратегією кібербезпеки), вимагає змін у чинному законодавстві. І хоча у подальшому було прийнято спеціальний законодавчий акт – Закон України «Про основні засади забезпечення кібербезпеки України», що регламентує суспільні відносини у цій сфері, окреслені Стратегією напрями державної політики мають бути впроваджені як у законодавство так і в практичну діяльність в інших аспектах.

Якщо проаналізувати імплементацію положень Стратегії кібербезпеки України, то вона відбувається шляхом затвердження розпорядженнями Кабінету Міністрів України Планів заходів на рік. Зокрема, це розпорядження Кабінету Міністрів України від 24.06.2016 № 440-р «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» та розпорядження Кабінету Міністрів України від 10.03.2017 № 155-р «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України».

За останні півтора роки було ухвалено вже два плани. На нашу думку, мова йде про певну надмірність планування. Реальна світова практика дещо інша. Наприклад, Стратегія кібербезпеки Чорногорії, що містить як додаток План дій, визначає період планування у 4 роки, а не в один рік. Аналогічний підхід застосовано у Великій Британії, Чехії, Словаччині, Естонії, Литві, Ірландії, Туреччині, Канаді та інших країнах.

Щорічне планування призводить до систематичного невиконання заходів, зміни відповідальності державних органів, бюрократизації процесу виконання та інших негативних моментів організаційного характеру. Що і має місце якщо проаналізувати зміст Планів заходів з виконання Стратегії кібербезпеки за два останні роки.

Іншим проблемним питанням, є стан реалізації правотворчих заходів, які передбачені зазначеними документами. Якщо у Плані заходів на 2016 рік передбачено формулювання переліку першочергових нормативно-правових актів, які потребують розроблення та внесення змін, як перший захід, то у Плані заходів на 2017 рік передбачено вже 6 законотворчих пропозицій з термінами підготовки у першому півріччі, і ще принаймні 7 заходів явно містять нормотворчу компоненту на рівні підзаконних актів. При цьому такі заходи знову очолюють розроблений Кабінетом Міністрів України план. На нашу думку, такий стан речей є черговою ілюстрацією надмірної захопленості нормотворчою складовою реформ, коли розробка законопроектів та нормативно-правових актів є основним (а іноді єдиним) заходом реагування державних органів на сучасні виклики та загрози.

Підсумовуючи стан розвитку вітчизняного законодавства у сфері забезпечення кібербезпеки можливо прийти до наступних основних висновків.

Розвиток вітчизняного законодавства у сфері забезпечення кібербезпеки відбувався поступово із врахуванням документів міжнародно-правового характеру у розрізі резолюцій Генеральної асамблеї ООН щодо культури кібербезпеки у сучасних умовах. Стан та ступінь загроз у кіберпросторі зумовили реагування держави у документах стратегічного характеру у сфері національної безпеки і оборони України. Агресія проти

України у 2014 році, що відбувалася з активним використанням бойових дій проти нашої держави у кіберпросторі, а також посилення загальносвітових загроз кібербезпеці зумовили формування спеціального законодавства. Найбільш активно зазначений процес відбувався останні два роки. 8 травня 2018 року набуває чинності Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Цей Закон є комплексним спеціальним законодавчим актом у сфері забезпечення кібербезпеки. Попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений. У подальшому буде сформований відповідний масив нормативно-правових актів, що складатиме безпосереднє законодавство у сфері забезпечення кібербезпеки. Одночасно буде відбуватися процес узгодження положень нового законодавства кібербезпеки з нормами права, насамперед у галузі кримінального, адміністративного, цивільного права.

ПІСЛЯМОВА

Розвиток сучасних інформаційних технологій та їх впровадження в усі без винятки сфери життя обумовив виникнення якісно нових загроз національній та міжнародній безпеці. За останні десятиріччя такі загрози як транснаціональна кіберзлочинність, кібертероризм, застосування кібернетичної зброї перетворились із потенційних та гіпотетичних на цілком реальні, а протидія ним на пріоритетне завдання усього сектора національної безпеки і оборони.

Питання кіберзахисту, особливо в період застосування країною-агресором по відношенню до України технологій гібридної війни, у першу чергу в інформаційній сфері, що сформувало нові виклики та загрози інформаційній безпеці держави, має надзвичайно велике значення.

Можливо багато говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому і приватного сектора; встановлення контролю над кіберзброєю, а також посиленням охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності тощо. Однак без набуття системного та комплексного характеру всі зазначені підходи не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень.

Боротьба з кіберзлочинністю повинна носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Ефективність заходів у цій сфері повинно досягатися завдяки здійсненню оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики у кіберпросторі.

У сучасному глобалізованому світі Україна потребує створення адекватної системи кібернетичної безпеки. Активність з боку провідних держав світу у кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних

злочинних груп, що спеціалізуються на кіберзлочинах обумовлюють необхідність виробленні пріоритетів трансформації вітчизняного кібербезпекового сектору з урахуванням вищезазначених тенденцій.

Варто зазначити, що у швидкоплинному перебігу подій суспільного життя, з революційними процесами у розвитку інформаційних технологій значна частина чинних нормативних актів як внутрішньодержавних, так і міжнародних поступово втрачає актуальність, відповідність процесам, які ними нормуються, і потребує уточнень або ж перегляду. Розвиток інформаційної діяльності створює необхідність правового урегулювання нових аспектів цієї діяльності. Потребує досконалого правового обґрунтування питання організації ефективного протистояння кібертероризму в умовах активізації глобальних впливів, нових інформаційних технологій. Комплекс відповідних правових актів має постійно вдосконалюватися із урахуванням відповідного міжнародного законодавства, його еволюції і вітчизняної законотворчої практики, що має бути на варті інтересів національної інформаційної діяльності.

У питанні правового регулювання як реалізації функцій держави, зокрема щодо забезпечення кібербезпеки та протидії кіберзагрозам слід виходити насамперед з загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії – зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій. Основна проблема полягає у неочевидності деструктивності і можливих помилок в оцінці суті технологій, тому пошук можливих шляхів вирішення зазначеної низки проблем є перспективним для подальших досліджень у галузі правової науки.

Окрім цього, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. Водночас, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності.

Що стосується питання розвитку вітчизняного законодавства у сфері забезпечення кібербезпеки, то він відбувався поступово із врахуванням документів міжнародно-правового характеру у розрізі резолюцій Генеральної асамблеї ООН щодо культури кібербезпеки у сучасних умовах. Стан та ступінь загроз у кіберпросторі зумовили реагування держави у документах стратегічного характеру у сфері національної безпеки і оборони України. Агресія проти України у 2014 році, що відбувалась з активним використанням бойових дій проти нашої держави у кіберпросторі, а також посилення загальносвітових загроз кібербезпеці зумовили формування спеціального законодавства. Найбільш активно зазначений процес відбувався останні два роки. 8 травня 2018 року набуває чинності Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. Цей Закон є комплексним спеціальним законодавчим актом у сфері забезпечення кібербезпеки. Попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений. У подальшому буде сформований відповідний масив нормативно-правових актів, що складатимуть безпосереднє законодавство у сфері забезпечення кібербезпеки. Одночасно буде відбуватись процес узгодження положень нового законодавства кібербезпеки з нормами права, насамперед у галузі кримінального, адміністративного, цивільного права.

Наукове видання

ДОВГАНЬ Олександр Дмитрович

ДОРОНІН Іван Михайлович

ЕСКАЛАЦІЯ КІБЕРЗАГРОЗ НАЦІОНАЛЬНИМ ІНТЕРЕСАМ УКРАЇНИ ТА ПРАВОВІ АСПЕКТИ КІБЕРЗАХИСТУ

Монографія

Технічне редагування: Ю.І.Крилова

Формат 60*84/16
Папір офсетний. Друк цифровий. Гарнітура Times New Roman.
Умовн.-друк.арк.25,92, Обл.-вид.арк. 22,9.
Замовлення № Д-0223-877
Підисано до друку 09.02.2018р.

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Мельникова, буд. 63
Тел. 067 440 11 37
artek.press@ukr.net
www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія ДК №4779 від 15.10.14р.

АртЕк
видавничий дім