УДК 658:330.87

ДОВГАНЬ О.Д., *доктор юридичних наук, старший науковий співробітник,*
НДІ інформатики і права НАПрН України
ТАРАСЮК А.В., *кандидат юридичних наук,* Служба безпеки України

КОРПОРАТИВНА КУЛЬТУРА КІБЕРБЕЗПЕКИ СУБ’ЄКТІВ НАУКОВОЇ ТА НАУКОВО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ

Анотація. *У статті запропоновано авторське бачення поняття корпоративної культури кібербезпеки суб’єктів наукової та науково-технічної діяльності, її складових, принципів та методів формування. Основна увага приділяється питанням забезпечення кібербезпеки у контексті захисту авторських і суміжних прав, честі, гідності, ділової репутації фізичних і юридичних осіб.*

Ключові слова: *корпоративна кібербезпека, корпоративна культура кібербезпеки, суб’єкти наукової та науково-технічної діяльності.*

Summary: *The paper presents an author’s perspective of internal cyber security of scientific and research institutions, its components, principles and methods of formation. The main attention is paid to the issues of ensuring the cyber security of scientific institutions in the context of copyright and related rights protection, honor, dignity, business reputation of individuals and legal entities.*

Keywords: *corporate cyber security, internal cyber security culture, scientific and research institutions.*

Аннотация: *В статье предложено авторское видение понятия корпоративной культуры кибербезопасности субьектов научной и научно-технической деятельности, ее составляющих, принципов и методов формирования. Основное внимание уделяется вопросу обеспечения кибербезопасности в контексте защиты авторских и смежных прав, чести, достоинства, деловой репутации физических и юридических лиц.*

Ключевые слова: *копоративная кибербезопасность, корпоративная культура кибербезопасности, субьекты научной и научно-технической деятельности.*

Постановка проблеми. Однією із важливих складових сучасної практики забезпечення корпоративної безпеки в державних та приватних структурах є кібербезпека, що включає заходи: захисту інформації з обмеженим доступом (далі – ІзОД) від несанкціонованого доступу; захисту ІзОД та відкритої інформації від загроз її несанкціонованої модифікації, блокування та знищення; протидії розповсюдженню неповної, невчасної та неправдивої інформації у кіберпросторі. Як правило, сучасні заходи із забезпечення корпоративної кібербезпеки обумовлюються технологічними особливостями та можливостями сучасного кіберпростору, охоплюють технічні питання захисту інформаційних ресурсів (продуктів/активів) та захисту іміджевих позицій як організації, так і її співробітників (честі, гідності, ділової репутації та майнових прав фізичних і юридичних осіб).

Традиційно людина вважається найбільш вразливим об’єктом у системі забезпечення безпеки, і ступінь вразливості залежить від багатьох факторів, насамперед, рівня усвідомлення (сприйняття) можливих загроз та їх наслідків, обізнаності щодо методів захисту, психологічних особливостей людини, її світоглядних позицій, морально-етичних цінностей, психологічного клімату у колективі, сімейних обставин та інших складових. При цьому функціональні обов’язки конкретного співробітника

визначають ступінь зацікавленості у його використанні для порушення корпоративної безпеки шляхом використання кібератак на його корпоративну та особисту кібернетичну інфраструктуру.

В умовах неумотивованості (відсутності підстав) співробітників у порушенні корпоративної безпеки, формування корпоративної культури кібербезпеки є дієвим і актуальним заходом підвищення рівня виконавчої дисципліни при виконанні регламентів із захисту інформаційних ресурсів організації, а також додатковим чинником для забезпечення корпоративної безпеки у розрізі завдань кіберзахисту особи – співробітників, що функціонально не задіяні у системі кіберзахисту організації.

Звісно, корпоративна культура кібербезпеки є частиною загальної корпоративної культури організації, що зорієнтована на загальні принципи забезпечення корпоративної безпеки та кібербезпеки зокрема.

Результати аналізу наукових публікацій. Проведений контент аналіз публікацій [5 – 12] свідчить, що формування корпоративної культури кібербезпеки розглядається сьогодні у якості одного із ключових завдань національної системи кібербезпеки та національної безпеки загалом. При цьому процес формування корпоративної культури кібербезпеки спрямований на забезпечення кібербезпеки особи як в рамках адміністративних (бізнес) процесів організації, так і в її повсякденному житті. Однак слід зазначити, що концептуальні та організаційно-правові питання формування корпоративної культури кібербезпеки суб’єктів наукової та науково-технічної діяльності (науково-дослідних, науково-виробничих та проектних установах, центрах, кафедрах – далі наукових установ) мають свої особливості та є актуальними в сучасних умовах розвитку кіберпростору України, а потребують наукового осмислення.

Метою статті є обґрунтування сутності корпоративної культури кібербезпеки, її складових, принципів та методів формування з позицій діяльності наукових установ. Завданнями статті є розкриття сутності феномена корпоративної культури кібербезпеки наукових установ через поняття “корпоративної безпеки”, “інформаційної та кібернетичної безпеки”, “відкритих даних”, “авторських і суміжних прав”, “професійної культури”, “корпоративної культури”, “культури безпеки”, “інформаційної культури” та інших.

Виклад основного матеріалу. Поняття корпоративної безпеки, інформаційної та кібернетичної безпеки зокрема, є інтегративним міждисциплінарним феноменом, який може бути досліджено через управлінські, професійні (фахові), правові, психологічні та інші аспекти.

Корпоративна кібербезпека наукових установ. Зрозуміло, що корпоративна безпека передбачає системно-цілісне бачення проблеми управління економіко-технологічною частиною та “людською складовою” організації як рівноправних підсистем управління. Тому корпоративну безпеку можна розглядати як систему заходів, спрямованих на захист організації від будь-яких навмисних/ненавмисних, зовнішніх/внутрішніх деструктивних дій, що можуть призвести до порушення неперервності економіко-технологічних процесів продуктивної діяльності, сталого розвитку організації тощо. Загалом до категорії зовнішніх деструктивних чинників можна віднести: конкурентну боротьбу; корумпованість державних установ; криміналізацію в окремих сферах діяльності. В свою чергу, у якості внутрішніх чинників можна розглянути передусім: нездоровий психологічний клімат у колективі; недостатність компетентності та відповідальності кадрів; низький рівень мотивації та корпоративної надійності співробітників. Виходячи із мети та завдань статті зосередимо

увагу лише на чинниках компетентності з питань корпоративної безпеки (кібербезпеки зокрема), відповідальності та особистої умотивованості співробітників у її забезпеченні.

1. Управлінський аспект корпоративної безпеки передбачає, як правило, використання процесного підходу, що розглядає організацію як набір процесів, відповідно, управління організацією – це управління певними процесами. На кожному етапі процес має свою ціль, ступінь виконання якої є показником, що визначає його ефективність. Тому заходи із забезпечення корпоративної безпеки реалізують контроль за ефективністю процесів шляхом управління ризиками її самої, як з точки зору імовірності реалізації потенційних загроз, так і з точки зору можливих наслідків їх реалізації.

Виходячи із мети та завдань статті, зосередимо увагу на процесах одержання, використання (обробки, зберігання) та поширення (передачі) інформаційних ресурсів, безпосередньо пов’язаних із науковою (науково-технічною) діяльністю.

Метою управління діяльністю наукової установи із забезпечення корпоративної безпеки є забезпечення її сталого розвитку, яка досягається передусім шляхом забезпечення інформаційної та кібернетичної безпеки.

2. Професійний аспект корпоративної безпеки наукових установ, незалежно від напрямів фундаментальних та прикладних наукових досліджень, визначає потреби, цілі та задачі діяльності із забезпечення фінансово-економічної безпеки організації, включаючи захист: ІзОД та виробів у яких вона реалізована (якщо така існує); відкритої інформації (у контексті забезпечення авторських і суміжних прав); критичної кібернетичної інфраструктури (ІзОД, відкритої інформації, програмних та технічних засобів, що її обробляють); іміджевої політики організації. У зв’язку з цим звернемо увагу на поняття інформаційної та кібернетичної безпеки наукової установи, підходи щодо її забезпечення.

У науковій спільноті України ще триває дискусія щодо співвідношення між поняттями “інформаційна безпека”, “кібернетична безпека”, “безпека інформації” та “інформаційно-психологічна (у тому числі і психофізична) безпека”, а також “захист інформації” та “інформаційно-психологічний захист”. Обумовлено це історичними етапами та технологічними особливостями розвитку інформаційного і кібернетичного простору, різними поглядами науковців та практиків з позицій: носія інформації, що захищається (людина, папір, електричний сигнал, фізичні поля); об’єкта захисту (інформаційні ресурси, свідомість та підсвідомість людини); рівня захисту (захист людини, організації, держави та міжнародного правопорядку); методологічних основ діяльності із забезпечення інформаційної та кібернетичної безпеки (правові, правоохоронні, організаційні, технічні та інформаційні заходи профілактики, захисту, виявлення та реагування на можливі інциденти (успішні реалізації загроз).

Загалом же існує певна узгодженість думок відносно того, що поняття кібернетичної безпеки є складовою частиною поняття інформаційної безпеки, оскільки сутність загроз, методів, засобів і заходів захисту є однаковою та обмежується (і окремо доповнюється) особливостями кіберпростору. Отже, заходи інформаційної безпеки із забезпечення надійності персоналу, спеціального паперового діловодства, об’єктового режиму та акустичного захисту навряд чи можна віднести до сфери кібербезпеки. Однак, кіберпростір є унікальним явищем, що не має національних кордонів. Відповідно, кібербезпека, на відміну від інформаційної безпеки, є не лише невід’ємною складовою кожної зі сфер національної безпеки та водночас самостійною сферою забезпечення національної безпеки, а також додатково є самостійною сферою забезпечення міжнародної безпеки.

Виходячи із мети та завдань статті, розглянемо поняття кібербезпеки у розрізі діяльності із забезпечення захисту інформаційних ресурсів та захисту іміджевої політики організації від загроз кібершпигунства та кібертероризму.

Відповідно до положень міжнародного стандарту ISO/IEC 27032 “Guidelines for cybersecurity” (сімейства стандартів з управління інформаційною безпекою ISO/IEC 270k) під кібербезпекою розуміють властивість захищеності інформаційних ресурсів від загроз порушення їх конфіденційності, цілісності та доступності у кіберпросторі. Тезаурус кібербезпеки інтегрований з поняттями інформаційної безпеки як стану захисту (захищеності) інформації, комп’ютерної та мережевої безпеки тощо. У якості кіберпростору розглядається комплексне віртуальне середовище, сформоване за результатами дії людей, програм і сервісів у мережі Інтернет з використанням мережевих і комунікаційних технологій.

Агентство ENISA (Європейське агентство з питань мережевої та інформаційної безпеки), спершу надавало настанови та рекомендації з інформаційної безпеки, а згодом розширило сферу своєї діяльності на вирішення питань кібербезпеки. Кібербезпека зазвичай стосується заходів і дій, спрямованих на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов’язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них.

Міжнародна асоціація ISACA (Асоціація аудиту та контролю інформаційних систем) пропонує наступні визначення. Кібербезпека – це захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж. Кібербезпека охоплює все, що захищає організація та фізичні особи від умисних атак, порушень, інцидентів і їх наслідків. Відповідно до рекомендацій ISACA організації повинні вміти розрізняти стандартну інформаційну безпеку та кібербезпеку. Різниця полягає в масштабах, мотивах, можливостях і методах атак.

У свою чергу відповідно до чинного Закону України “Про основні засади забезпечення кібербезпеки України” мають місце наступні 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. Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Крім того, законодавець надав і інші визначення, зокрема, кіберзахист – 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. Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням. Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

У наукових працях поняття кібернетичного (інформаційного) тероризму тлумачиться по різному, однак має спільну ознаку – особливий різновид психологічного

терору, що здійснюється у кіберпросторі або з його використанням. Тактична мета інформаційного тероризму полягає в тому, щоб привернути увагу до проблеми, зчинити навколо неї галас, стратегічна – залякування і деморалізація людей задля досягнення певного результату. Тобто мова йде про застосування деструктивних інформаційно-психологічних впливів у кіберпросторі, що можуть бути спрямовані як на окремих осіб, так і організацію, до якої вони належать.

Розглядаючи поняття кібербезпеки організації (у тому числі і наукової установи) не залишимо поза увагою ратифіковану в Україні Конвенцію Ради Європи про кіберзлочинність, у якій визначені: правопорушення проти конфіденційності; правопорушення, пов’язані з комп’ютерами (проти цілісності та доступності інформації); правопорушення пов’язані зі змістом; правопорушення пов’язані з порушенням авторських та суміжних прав. У чинній конвенції про кіберзлочинність у якості правопорушень, пов’язаних зі змістом, розглядаються лише дії із вироблення, пропонування, розповсюдження, здобуття та володіння дитячої порнографії, однак у цьому контексті доцільно звернути також увагу на чинне законодавство України щодо прав захисту фізичних і юридичних осіб від поширення відомостей про події та явища, котрих не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені).

Здається справедливим, що питання захисту авторських та суміжних прав, честі, гідності та ділової репутації у кіберпросторі можливо теж віднести до заходів кіберзахисту, оскільки мова йде також про заходи забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів у кіберпосторі, а також заходи забезпечення спостережності інформації у кіберпросторі для вирішення питань виявлення, інформаційного та технологічного реагування на спеціальні інформаційні акції і операції. Враховуючи глобальність, транснаціональність кіберпростору здається очевидним те, що дієве реагування на спеціальні інформаційні акції і операції можливе лише організаційно-технічними заходами.

Таким чином, доцільно розглядати процес забезпечення корпоративної кібербезпеки наукових установ як комплекс заходів з протидії загрозам кібершпигунства і кібертероризму, що стосуються забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів – захисту інформації у кіберпросторі, а також як комплекс заходів із захисту честі, гідності, ділової репутації та майнових прав – інформаційно-психологічного захисту у кіберпросторі.

3. Правовий аспект корпоративної безпеки (у тому числі і наукових установ) – це передусім питання визначення об’єктів та суб’єктів захисту, вимог до методів, засобів та заходів захисту, відповідальності за їх порушення. Відповідно до мети і завдань статті зосередимо увагу лише на кібернетичному захисті відкритої інформації з позиції авторських та суміжних прав, інформаційно-психологічному захисті юридичної та фізичної особи у кіберпросторі. Питання ж захисту ІзОД, включаючи комерційну таємницю наукової устави, є окремим питанням забезпечення корпоративної кібербезпеки, що пов’язане із заходами формування корпоративної культури кібербезпеки лише в завданнях підвищення виконавчої дисципліни при виконанні регламентів захисту інформації – перехід від необхідності сумлінного виконання функціональних обов’язків із захисту інформації до свідомості корпоративної кібербезпеки.

Зазначимо, що визначення поняття “відкриті дані” наведено у Законі України “Про доступ до публічної інформації”. Так, публічною інформацією у формі відкритих даних є публічна інформація у форматі, що дозволяє її автоматизоване оброблення

електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Будь-яка особа може копіювати, публікувати, поширювати, використовувати, у тому числі в комерційних цілях, у поєднанні з іншою інформацією або шляхом включення до складу власного продукту, публічну інформацію у формі відкритих даних з обов’язковим посиланням на джерело отримання такої інформації.

Відкриті дані та інші дані у відкритому доступі є неоднорідними з правової точки зору та в контексті можливості їх обробки, копіювання, передачі та використання [1]. Правові підстави для таких дій щодо відкритих даних визначаються законодавчими актами відповідних країн, що оприлюднюють публічну інформацію у формі відкритих даних.

Інформація, яка розміщена в мережі Інтернет, може містити об’єкти авторського права і для використання таких об’єктів необхідно мати правову підставу – дозвіл (ліцензію) від власника виключних майнових авторських прав або підставу, визначену відповідним законом. У будь-якому випадку, таке використання може бути здійснене в межах відповідних ліцензій або в межах норм, що визначають умови добросовісного використання щодо конкретних об’єктів та на інших правових підставах, що визначені в законодавстві відповідної держави.

Можливість інформації бути об’єктом власності, з точки зору права власності на майно, продовжує залишатися в Україні дискусійним. В Україні галузева належність інформації як об’єкта права загалом, і як об’єкта права власності зокрема, визначена нечітко [2]. Так, у статті 969 Цивільного кодексу України (далі – ЦКУ) визначаються документи, як окрема форма інформації, в якості цінностей, які можуть бути передані до банку на зберігання. Крім того, у статті 1010 ЦКУ до майна довірителя відносяться його документи. Відповідно до Глави 62 ЦКУ до результатів виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, які має право використовувати замовник, відносяться наукові дослідження та конструкторська документація, в якості конкретних організаційних форм інформації.

Звісно, виникає питання щодо правового регулювання відносин, пов’язаних з обігом електронних документів, правового визначення поняття веб-документ та інших.

У Законі України “Про інформацію” визначено, що документ – це передбачена законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві. Закон України “Про електронні документи та електронний документообіг” визначає, що електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Обов’язковий реквізит електронного документа – обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили (це передусім електронний цифровий підпис та дата підписання документу). Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

В Україні законодавством не встановлений перелік способів фіксації змісту веб-сторінок в мережі Інтернет та не розв’язані інші питання здійснення права на захист авторських прав на твори, розміщені в мережі Інтернет. Хоча вже існує практика надання послуг з проведення фіксації змісту веб-сторінок у мережі Інтернет з видачею Експертних висновків, що дозволяє формувати докази для ефективного захисту прав інтелектуальної власності та прав осіб від порушень у мережі Інтернет [3], насамперед, щодо незаконного використання об’єктів права інтелектуальної власності, зокрема, об’єктів авторського права і суміжних прав.

Відносно інформаційно-психологічного захисту зазначимо, що сьогодні кіберпростір є зручною платформою для поширення негативної та недостовірної інформації про осіб, що може порушувати їх особисті немайнові права та завдавати шкоди честі, гідності та діловій репутації. Чинне законодавство, що регулює правовідносини у сфері захисту честі, гідності та ділової репутації – Цивільний кодекс України, Закони України “Про інформацію”, “Про друковані засоби масової інформації (пресу) в Україні”, “Про телебачення і радіомовлення” є багато у чому застарілими. У випадках поширення інформації в мережі Інтернет адвокати керуються роз’ясненнями, наданими у постанові Пленуму Верховного Суду України від 27 лютого 2009 року № 1 “Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи”. Взагалі, ця постанова є чи не найголовнішим документом, до якого звертаються адвокати, що практикують у так званих “репутаційних” справах [4]. Верховний Суд України встановив ряд правил визначення належного відповідача у таких випадках:

– належними відповідачами є автор інформаційного матеріалу та власник веб-сайту;

– позивач повинен встановити особи автора та власника веб-сайту;

– якщо автор матеріалу невідомий або його неможливо встановити, належним відповідачем є власник веб-сайту, оскільки він створив технологічну можливість та умови для поширення інформації;

– дані про власника веб-сайту можуть бути витребувані судом у адміністратора системи реєстрації та обліку доменних імен українського сегмента мережі Інтернет;

– якщо ні автора, ні власника веб-сайту встановити неможливо, факт недостовірності поширеної інформації може бути встановлений судом у порядку окремого провадження.

Однак багато питань є проблематичними: веб-сайт – це і електронна пошта та соціальні мережі (включаючи месенджери); що розуміти під поняттям власник Веб-сайту; як бути, якщо доменне ім’я розміщено не в українському сегменті мережі Інтернет; як встановити хостинг-провайдера та отримати від нього необхідну інформацію, яка містить персональні дані.

Окремим питанням є складнощі із застосуванням статті 361 Кримінального кодексу України (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку) у випадках успішної реалізації загроз кібершпигунства та кібертероризму відносно фізичних і юридичних осіб.

Враховуючи мету та завдання статті, можна дійти висновку, що у правовому сенсі основа корпоративної кібербезпеки наукових установ полягає, перш за все, у засвідченні авторства, цілісності та часу створення електронних ресурсів у рамках правових можливостей Національної системи електронного цифрового підпису.

4. *Психологічний аспект корпоративної безпеки* (у тому числі і наукових установ) можна розглянути через призму таких соціально-психологічних категорій, як корпоративні цінності та корпоративна культура.

Корпоративні цінності є основою корпоративної культури, що спрямована на формування корпоративної ідентичності співробітника (корпоративної свідомості) шляхом збалансування особистих і корпоративних інтересів, формування корпоративної відповідальності співробітника за реалізацію стратегії сталого розвитку організації, забезпечення корпоративної безпеки зокрема. Відповідно, одним із результатів формування корпоративної культури є наявність у співробітників стратегічного

корпоративного мислення – фундаменту для розв’язання проблем, пов’язаних з попередженням та реагуванням на загрози продуктивній діяльності організації, забезпечення конкурентоздатності організації тощо.

Виходячи із зазначеного зрозуміло, що поняття корпоративної культури кібербезпеки наукових установ є не тільки уточненням понять психологічного аспекту корпоративної кібербезпеки, а в силу технологічної основи заходів із її забезпечення, враховує також професійний, управлінський та правовий аспект.

Корпоративна культура кібербезпеки наукових установ. Як відомо, існує достатня кількість визначень поняття “культура”, які розглядаються у філософії, культурології, педагогіці, психології, соціології, економіці та інших галузях знань, жодне з яких поки що не стало загальноприйнятим. У якості спільної основи цих визначень можна виділити те, що культура людини утверджується як комплекс якостей, які людина виробила в собі власними зусиллями, і вона є проявом людської самосвідомості. Одним із таких явищ є професійна культура, основи якої закладаються у людини під час навчання, у період підготовки до професійної діяльності та професійного становлення.

Професійна культура розглядається як інтегральний показник діяльності фахівця. Вона забезпечується єдністю та взаємодією всіх її чинників, зокрема такими, як: тезаурус і кругозір (характеристика пізнавальної здатності та інтелектуального потенціалу), вміння і здібності (предметно-практичний досвід особистості), діапазон інтересів (рівень духовних ідеалів), світогляд (як соціальна спрямованість особистісної культури), норми і методи діяльності (регулятор вчинків і дій), культура почуттів (уособлення гуманістичної спрямованості спілкування, що визначає естетичну насиченість поведінки і діяльності) [5]. Виходячи із мети та завдань статті для нас більш цікаве трактування професійної культури як характеристики рівня компетентності фахівця та ставлення його до праці та себе як суб’єкта праці.

Корпоративна культура здається більш вузьким розумінням поняття професійної культури у фаховому сенсі та більш орієнтованим на організаційний аспект у системі управління персоналом організації. Корпоративна культура організації [6] – це сукупність прийнятих на даному підприємстві норм і правил поведінки по відношенню до клієнтів і партнерів, а також культура міжособових стосунків на підприємстві і саме від неї залежить ефективність діяльності організації, стан міжособистісних стосунків в ній та сформований імідж. Власна культура співробітників є зовнішнім відображенням корпоративної культури, яка виражає себе через імідж організації, оскільки співробітники є носіями корпоративної культури.

Доцільно також звернути увагу на поняття наукової культури, яку можна розглядати у вигляді норм й ідеалів наукового пізнання, тобто як професійну культуру. З іншої точки зору, наукова культура – це особливість життя наукового співтовариства, і її можна віднести до рамок корпоративної культури.

Як уже зазначалось раніше, метою корпоративної культури є формування у співробітників стратегічного корпоративного мислення – фундаменту для розв’язання проблем, пов’язаних з попередженням та реагуванням на загрози продуктивній діяльності організації. При цьому загальне поняття культури безпеки визначається як рівень розвитку людини і суспільства, що характеризується значущістю забезпечення безпеки життєдіяльності в системі особистісних і соціальних цінностей, безпечної поведінки в повсякденному житті і в умовах небезпечних та надзвичайних ситуацій, рівнем захищеності від загроз і небезпек в усіх сферах життєдіяльності [7].

Враховуючи специфіку заходів із забезпечення корпоративної безпеки наукових установ, доцільно також звернути увагу на поняття інформаційної культури, а також співвідношення між поняттями інформаційної культури та культури кібербезпеки.

Аналіз підходів до сутності інформаційної культури [8], які сформувалися в різних галузях знань свідчить, що розуміння цього поняття є неоднозначним. Спільною рисою, зокрема, є визнання детермінаційних зв’язків між рівнем інформаційної культури і розвитком певної сфери професійної активності особистості. Відмінності полягають у широкому та вузькому охопленні ознак інформаційної культури, від навичок володіння окремими інформаційними технологіями (комп’ютерної грамотності) до опанування знань та навичок майже у всіх сферах людської діяльності. З погляду на визначення корпоративної культури становить інтерес наступне визначення інформаційної культури у вузькому розумінні [9]: інформаційна культура в управлінській діяльності включає культуру правил організації подання, сприймання та використання інформації, культуру правил суспільних відносин із використанням мережі Інтернет та культуру суспільних правовідносин із застосуванням нових комп’ютеризованих інформаційних технологій.

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

Ототожнення культури кібербезпеки як складової інформаційної культури у вузькому розумінні уявляється обґрунтованим, оскільки безпековий аспект є вагомою частиною інформаційних відносин, що передбачають використання сучасних ІТ-технологій мережі Інтернет [10; 11].

Поняття культури кібербезпеки (у розумінні захисту інформації) почалось поширюватись у світі після прийняття у 2003 році Резолюції Генеральної Асамблеї ООН “Створення глобальної культури кібербезпеки”. У звіті Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) 2017 року “Культура кібербезпеки організації” запропоновано наступне визначення культури кібербезпеки [12]: знання, переконання, уявлення, норми і цінності людей по відношенню до кібербезпеки та використанню інформаційних технологій. Формування культури кібербезпеки в організації спрямоване на зміну мислення співробітників, сприйняття ризику та спільної відповідальності за забезпечення кібербезпеки організації, сприйняття заходів із забезпечення особистої кібербезпеки як побутової звички.

Складові культури кібербербезпеки визначені у Резолюції Генеральної Асамблеї ООН, у якості найбільш вагомих виділимо:

– обізнаність – учасники повинні бути інформовані про ризики та необхідність забезпечення кібербезпеки, а також про свої можливості у підвищенні стану захищеності;

– відповідальність – учасники відповідають за безпеку інформаційних систем та мереж згідно зі своєю роллю в системі кібербезпеки;

– реагування – учасники повинні вживати своєчасні і спільні заходи щодо попередження інцидентів, які стосуються кібербезпеки, їх виявленню і реагування на них;

– переоцінку – учасники повинні піддавати оцінюванню стан забезпечення кібербезпеки та вносити належні зміни в політику, практику, заходи і процедури забезпечення кібербезпеки, враховуючи при цьому появу нових і зміну колишніх загроз і чинників уразливості;

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

Таким чином, на авторську думку, корпоративна культура кібербезпеки наукових установ – це компетентність та корпоративні цінності наукового співтовариства, пов’язані із забезпеченням особистої та корпоративної безпеки у кіберпросторі у відповідності із визначеною політикою кібербезпеки наукової установи.

Політика кібербезпеки наукової установи повинна бути орієнтована перш за все на попередження загроз витоку електронної інформації щодо результатів наукових досліджень до їх офіційного опублікування та/або оформлення авторських прав, попередження випадків неправомірного звинувачення у порушенні авторських і суміжних прав та негативного впливу на іміджеві позиції наукового співтовариства. Реалізація політики кібербезпеки наукової установи повинна передбачати заходи захисту корпоративної та особистої кібернетичної інфраструктури співробітників установи від загроз несанкціонованого доступу до електронної інформації, її модифікації та знищення, передбачати можливість доведення авторства, цілісності та дати виготовлення електронної інформації, урегулювання питань щодо безпечного використання технологій мережі Інтернет. Політика кібербезпеки наукової установи повинна передбачати заходи корпоративної взаємодії та реагування на інциденти порушення безпеки інформації та інформаційно-психологічної безпеки у рамках діяльності наукової установи.

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

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

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

Висновки.

Формування корпоративної культури кібербезпеки суб’єктів наукової та науково-технічної діяльності належить до завдань системи управління персоналом, що спрямована на посилення заходів забезпечення корпоративної безпеки в частині захисту інформації з обмеженим доступом, авторських і суміжних прав, негативного впливу на іміджеві позиції наукового співтовариства. З позиції соціального партнерства доцільно звернути увагу на заходи інформування, навчання та мотивації співробітників до виконання норм корпоративної культури кібербезпеки. З технічної – це забезпечення співробітників засобами технічного і криптографічного захисту інформації, надання необхідних послуг (у тому числі і з моніторингу контенту кіберпростору) та створення умов для широкого використання електронного цифрового підпису. З правової –

створення умов для надання своєчасної правової допомоги співробітникам в питаннях захисту авторських і суміжних прав, захисту честі, гідності, ділової репутації.

Перспективи подальших досліджень є визначення концептуальних, правових та організаційних основ побудови системи кібербезпеки суб’єктів наукової та науково-технічної діяльності.

Використана література

1. Тарасюк А.В. Відкриті дані та інші дані у публічному доступі : правові аспекти // Інформація і право. – № 2(21)/2017. – С. 59-65.

2. Брижко В.М. Інформаційний продукт як об’єкт права власності // Інформація і право. –№ 4(23)/2017. – С. 5-15.

3. Центр компетенції адресного простору українського сегменту мережі Інтернет. – Режим доступу : //http://web-fix.org

4. Рубля О. Питання належного відповідача у справах про захист честі, гідності та ділової репутації. – Режим доступу : http//jurliga.ligazakon.ua/news/2017/3/29/158027.htm

5. Власюк О. Структура професійної культури сучасного фахівця // Наукові записки. – (Серія : “Психологія”). – 2008. – № 11. – С. 29.

6. Фіщук Н.Ю., Ломачинська І.В. Корпоративна культура організації: сутність, види, принципи та вплив на розвиток організації : зб. наукових праць ВНАУ. – (Серія : “Економічні науки”) . – 2012. – Т. 4. – № 1(56). – С. 81-85.

7. Зоріна М.О. До проблеми визначення актуальності й особливостей формування культури безпеки життєдіяльності // Педагогіка формування творчої особистості у вищій і загальноосвітній школах. – 2010. – № 8. – С. 149-153.

8. Бєляков К.І. Інформаційна культура в Україні : правовий вимір : монографія / К.І. Бєляков, С.Г. Онопрієнко , І.М. Шопіна : за заг. ред. К.І. Бєлякова. – К. : КВІЦ, 2018. – 169 с.

9. Новицька Н. Б. Організаційно-правові аспекти інформаційної культури в управлінській діяльності : дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07. – (Національна академія держ. податкової служби України). – Ірпінь, 2007. – С. 38.

10. Довгань О.Д. Щодо деяких правових аспектів культури кібербезпеки : зб. тез наукових доповідей IX Всеукраїнської науково-практичної конференції [“Актуальні проблеми управління інформаційною безпекою держави”]. – К., 2018. – С. 60-62.

11. Мельник С.В. Формування культури кібербезпеки : особистісний, корпоративний, державний та глобальний вимір. : зб. тез наукових доповідей IX Всеукраїнської науково-практичної конференції [“Актуальні проблеми управління інформаційною безпекою держави”]. – К., 2018. – С. 115-118.

12. Report The European Union Agency for Network and Information Security (ENISA) Cyber Security Culture in organisations. – Режим доступу : https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~