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

ГЛОБАЛЬНА КУЛЬТУРА КІБЕРБЕЗПЕКИ В СИСТЕМІ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Анотація. *В статті досліджується питання дефініції поняття “глобальна культура кібербезпеки”, розглядаються принципи та підходи формування глобальної культури кібербезпеки на національному рівні. Основна увага приділяється складовим феномена культури кібербезпеки, її ролі та місцю в системі запобігання кіберзлочинності.*

Ключові слова: *кібербезпека, кіберзлочинність, протидія кіберзлочинності, система запобігання кіберзлочинності, глобальна культура кібербезпеки.*

Summary. *The article explores a definition of concept “global culture of cyber security”, the principles and approaches of forming a global culture of cyber security on the national level. The main focus is on the cyber security culture, its role and place in the system of cyber crime prevention.*

Keywords: *cyber security, cyber crime, countereffort of cyber crime, cyber crime prevention system, global cyber security culture.*

Аннотация. *В статье исследуется вопрос дефиниции понятия “глобальная культура кибербезопасности”, рассматриваются принципы и подходы формирования глобальной культуры кибербезопасности на национальном уровне. Основное внимание уделяется составляющим феномена культуры кибербезопасности, ее роли и месту в системе предупреждения киберпреступности.*

Ключевые слова: *кибербезопасность, киберпреступность, противодействие киберпреступности, система предупреждения киберпреступности, глобальная культура кибербезопасности.*

Постановка проблеми. Проблема протидії кіберзлочинності є одним із пріоритетів у системних заходах забезпечення кібербезпеки на національному та міжнародному рівні, має правовий, технічний і організаційний аспект у запобіганні, виявленні (розслідуванні), припиненні та розкритті кіберзлочинів. При цьому, складність, відповідно, і ефективність заходів виявлення, припинення та розкриття кіберзлочинів обумовлена технологічними особливостями процесів створення, зберігання, обміну, обробки та знищення інформації у сучасних технологіях кіберпростору, складністю доведення причетності конкретної особи до здійснення певних дій, юридичними особливостями надання офіційної правової допомоги від держав, з територіальної частини кіберпростору яких здійснювались кіберзлочини. В свою чергу, ефективність заходів запобігання кіберзлочинам визначається рівнем достатності заходів стримування потенційних правопорушників (зниженням ризику вчинення кіберзлочинів), можливостями усунення або зменшення потенційно шкідливих наслідків вчинення кіберзлочинів, а також організаційно-технічними характеристиками рівня захищеності всіх об’єктів кібербезпеки.

Загалом, протидія кіберзлочинності реалізується через систему заходів, спрямованих на усунення причин і умов, які сприяють вчиненню кіберзлочинів, які вже мають місце, або готуються чи вже почалися, виявлення винних осіб та притягнення їх до відповідальності. Разом з тим, ефективність заходів протидії кіберзлочинності визначається не лише ефективністю діяльності правоохоронних органів, а і ефективністю

діяльності національної і міжнародної системи кібербезпеки в цілому, включаючи і ефективність співпраці їх суб’єктів на національному і міжнародному рівнях.

Актуальність дослідження зумовлена сучасними викликами і загрозами проявів кіберзлочинності в Україні, необхідністю реалізації системних заходів протидії у рамках Національної системи кібербезпеки, національною відповідальністю за підтримання міжнародного правопорядку тощо.

Результати аналізу наукових публікацій. Проведений контентний аналіз публікацій В. Брижка, В. Бутузова, В. Гавловського, О. Довганя, М. Карчевського, В. Кудінова, М. Кравцової, В. Маркова, А. Марущака, О. Орлова, В. Пилипчука, Е. Рижкова, К. Тітуніної, В. Хахановського, В. Шеломенцева, О. Юрченка та інших авторів свідчать про достатню розробленість проблеми протидії кіберзлочинності, однак залишається малодослідженим соціальний аспект заходів запобігання кіберзлочинів, що стосується формування глобальної культури кібербезпеки.

Мета статті полягає у науковому обґрунтуванні сутності поняття “глобальна культура кібербезпеки”, основних складових, принципів та підходів до її формування. Завданнями статті є розкриття сутності феномена глобальної культури кібербезпеки через такі складові, як “кіберзлочинність”, “протидія та запобігання кіберзлочинності”, “культура та глобальна культура”, “професійна культура”, “культура кібербезпеки” та ін.

Виклад основного матеріалу. У науковій спільноті України ще має місце дискусія відносно визначення термінів у сфері кібербезпеки [1]. Однак, при проведенні дослідження будемо користуватися термінами “кібербезпека”, “кіберпростір”, “кіберзлочин”, “кіберзлочинність”, “кібершпигунство”, “кібертероризм”, “кіберзахист”, “кіберінцидент” та “кібератака” у відповідності з визначеннями, що запропоновані в Законі України “Про основні засади забезпечення кібербезпеки України”.

Формування та реалізація державної політики щодо запобігання та протидії кіберзлочинності – це процеси, що відбуваються в рамках Національної системи кібербезпеки, які можна розглянути через організаційно-правовий, організаційно-технічний та правоохоронний аспекти.

У рамках міжнародної співпраці Україною ратифіковано Конвенцію Ради Європи про кіберзлочинність, Угоду про асоціацію між Україною та Європейським Союзом, у якій передбачено, що сторони Угоди співробітничають, у тому числі, і з питань протидії кіберзлочинності. Крім того, одним із пріоритетів співпраці України з НАТО та США є співпраця в галузі протидії кіберзлочинності, в рамках якої Україна отримує можливість координації дій та обміну інформацією при розслідуванні кіберзлочинів.

На сьогодні Стратегія кібербезпеки України (рішення Ради національної безпеки і оборони України від 27 січня 2016 року), Указ Президента України “Про загрози кібербезпеці держави та невідкладні заходи з їх реалізації” (рішення Ради національної безпеки і оборони України від 29 грудня 2016 року) та Закон України від 05 жовтня 2017 року “Про основні засади забезпечення кібербезпеки України”, визначають організаційно-правову основу протидії кіберзлочинності, яка полягає, насамперед, у визначенні суб’єктів, сфер їх компетенції, напрямів взаємодії у рамках Національної системи кібербезпеки та міжнародної співпраці.

Так, у сфері компетентності Держспецзв’язку України, до організаційно-правових заходів запобігання і протидії кіберзлочинності відноситься регуляторна діяльність у сферах технічного і криптографічного захисту інформації, яка полягає у створенні умов для формування ринку засобів і послуг із захисту інформації у кіберпросторі *(забезпеченні конфіденційності, цілісності, підтвердження авторства та доступності інформації)*, а також забезпеченні необхідних рівнів кіберзахисту засобами і послугами,

що пропонуються як для юридичних, так і фізичних осіб. Тобто, мова йде про створення умов для забезпечення доступності надійних засобів і систем кіберзахисту для фізичних і юридичних осіб України.

Нормативно-правове забезпечення у сферах технічного і криптографічного захисту інформації:

– структурує та упорядковує відносини між державою, тими хто забезпечує та отримує захист інформації, насамперед, шляхом регулювання технічних регламентів із захисту інформації, що мають примусовий і рекомендаційний характер;

– стосується процедур ліцензування, розроблення, виготовлення, модернізації, експертизи, впровадження, експлуатації та виведення із експлуатації засобів і систем захисту інформації.

Серед чинних нормативно-правових актів виділимо: Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 19.04.2014 року; постанову Кабінету Міністрів України “Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 07.09.2011 року № 373; нормативний документ системи технічного захисту інформації “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі” від 08.11.2005 року НД ТЗІ 3.7-003-05; нормативний документ системи технічного захисту інформації “Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу” від 20.12.2000 року НД ТЗІ 3.6-001-2000; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації” від 30.05.2007 року № 141; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про державну експертизу в сфері технічного захисту інформації” від 16.05.2007 року № 93; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації” від 23.06.2008 року № 100.

З метою забезпечення системності заходів протидії кіберзлочинності в Україні є актуальним завдання приведення до єдиних формулювань законодавство у сферах забезпечення кібербезпеки, технічного і криптографічного захисту інформації, визначення норм для віднесення об’єктів до критичної інформаційної інфраструктури тощо.

Організаційно-технічна складова заходів протидії кіберзлочинності полягає у впровадженні організаційно-технічної моделі кіберзахисту, включаючи забезпечення державно-приватної взаємодії при реалізації заходів запобігання, виявлення, реагування на кіберінциденти і кібератаки, усунення їх наслідків.

На сьогодні організаційно-технічна модель кіберзахисту доопрацьовується за участю компетентних вітчизняних структур та міжнародних експертів. При цьому, вона напевне повинна орієнтуватись на сучасні міжнародні практики, що базуються на ризик-орієнтованих стандартах управління кібербезпекою (сімейства стандартів з управління інформаційною безпекою ISO/IEC 270k), насамперед, ISO/IEC 27032 Guidelines for cybersecurity *(“Рекомендації з кібербезпеки”)*, а також ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence *(“Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів”)*, ISO/IEC 27041 Guidance on assuring suitability and adequacy of incident investigative method *(“Настанова щодо забезпечення прийнятності та адекватності методів розслідування”)*, ISO/IEC 27043 Incident investigation principles and processes *(“Принципи та процеси розслідування інцидентів”)*. Загалом же організаційно-технічна модель

кіберзахисту повинна включати моделі оцінки ризику та прийняття рішень, а їх стандартизація та впровадження безпосередньо вплине на ефективність правоохоронних заходів із протидії кіберзлочинів в Україні.

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA [2] (Державний центр кіберзахисту) є акредитованим членом FIRST та активно взаємодіє з аналогічними командами в усьому світі, орієнтована на кіберзахист державних інформаційних ресурсів, співпрацює та допомагає правоохоронним, банківським, комерційним, іншим державним і приватним структурам. Однак, цього недостатньо, провідні країни світу мають більше 20 CERT, у тому числі і в правоохоронних органах, інших суб’єктах Національної системи кібербезпеки і у вищих навчальних закладах зокрема.

Правоохоронний аспект в системі протидії кіберзлочинності стосується передусім кримінальної відповідальності для осіб, що вчинили кіберзлочини. Так, у відповідності з КК України розслідуються наступні категорії злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж [3]: ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку); ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут); ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації); ст. 362 (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї), ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється); ст. 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку).

Крім цього [3], варто звернути увагу на: ст. 176 *(Порушення авторського права і суміжних прав)*; ст. 185 *(Крадіжка)*; ч. 3, 4 ст. 190 *(Шахрайство)*; ст. 200 *(Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення)*; ст. 229 *(Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару)*; ст. 231 *(Незаконне збирання інформації, що становить банківську таємницю)*; ч. 3 – 5 ст. 301 *(Ввезення, виготовлення, збут і розповсюдження порнографічних предметів)*.

Виходячи із сучасних уявлень про кібербезпеку, неможливо оминути увагою також кримінальні правопорушення з використанням можливостей соціальних мереж (кіберпростору), відповідальність за вчинення яких передбачено такими статтями КК України [4]: ст. 120 *(Доведення до самогубства)*; ст. 160 *(Підкуп виборця, учасника референдуму)*; ст. 161 *(Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за ін. ознаками)*; ст. 163 *(Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер)*; ст. 189 *(Вимагання)*; ст. 192 *(Заподіяння майнової шкоди шляхом обману або зловживання довірою)*; ст. 258-4 *(Сприяння вчиненню терористичного акту);* ст. 258-2 *(Публічні заклики*

до вчинення терористичного акту); ст. 338 *(Наруга над державними символами)*; ст. 345-1 *(Погроза або насильство щодо журналіста)*; ст. 350 *(Погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов’язок)* та ін.

У свою чергу, ратифікована Україною Конвенція Ради Європи про кіберзлочинність визначає: 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.

Сьогоднішня практика кіберполіції пропонує громадянам звертатись [5]: щоб повідомити інформацію про суїцидальні групи в Інтернет; якщо є інформація про ресурси чи осіб, що поширюють порнографію, порушують авторські чи суміжні права в Інтернет; якщо є дані про торгівлю наркотиками чи зброєю, або інші види забороненої в мережі інтернет діяльності; щоб повідомити про матеріали, які закликають до сепаратизму чи тероризму; для надання інформації щодо спроб незаконного зняття коштів з рахунків; викрадення даних платіжних карток чи інших фінансових шахрайств, зокрема, про фінансові піраміди в Інтернеті, про скімінг, кардерство тощо; щоб повідомити про віруси, ботнети чи інші види інтернет шахрайства. Фактично, охоплює всі напрями протидії кіберзлочинності, що віднесені до підслідності органів внутрішніх справ. Але, у Національній системі кібербезпеки є також актуальними питання щодо ефективної протидії правопорушенням у кіберпросторі, які стосуються боротьби зі спамом, захисту персональних даних, комерційної таємниці та ін.

Отже, здається очевидним завдання приведення до єдиних формулювань диспозиції та кваліфікуючих ознак КК України, що передбачають відповідальність за злочини, які можна віднести до категорії кіберзлочинів.

За результатами аналізу статистичної інформації щодо протидії кіберзлочинності можна стверджувати, що практика припинення і розкриття кіберзлочинів стикається зі значними труднощами, зумовленими складністю виявлення цих високотехнологічних злочинів, високим рівнем їх латентності. Тому розглядаються криміналістичні характеристики кіберзлочинів [6]: типові слідчі ситуації; спосіб вчинення та приховання злочину; типові матеріальні сліди злочину та механізм слідоутворення; характеристика особистості обвинуваченого й потерпілого; обстановка злочину. Водночас, широкий спектр ІТ-технологій, що використовуються правопорушниками, передбачають анонімність та захищеність у кіберпросторі, відповідно, відзначаються різноманітністю та складністю механізмів слідоутворення з можливістю приховання або змін комп’ютерної/мережевої інформації щодо слідів злочину. Зазначені чинники не сприяють чіткому уявленню щодо всіх компонентів криміналістичної характеристики кіберзлочинів, а в кінцевому підсумку, ускладнюють процес розкриття кіберзлочинів відповідно [6].

Тому є актуальною потреба у постійному удосконаленні тактики проведення слідчих дій із розслідування кіберзлочинів, методик та ефективних методів комп’ютерно-технічної експертизи, що відповідають сучасним реаліям та тенденціям розвитку ІТ-технологій.

Далі, під системою протидії кіберзлочинності у широкому розумінні (не обмежуючись правоохоронною діяльністю) можна розуміти взаємопов’язану сукупність організаційно-правових, організаційно-технічних та правоохоронних (кримінологічних і криміналістичних) заходів запобігання, виявлення, припинення та розкриття кіберзлочинів.

У свою чергу, під системою запобігання кіберзлочинності можна розуміти сукупність взаємопов’язаних спеціально-кримінологічних, індивідуальних та загальних

заходів попередження, спрямованих на виявлення й усунення причин та умов, які сприяють вчиненню кіберзлочинів.

Спеціальне попередження кіберзлочинів здійснюється в рамках правоохоронної діяльності шляхом впливу на соціальні групи, окремих осіб і організації щодо яких є підстави вважати, що вони мають підвищену криміногенність. Суб’єктом індивідуального попередження як одного із видів спеціального попередження, є конкретна людина, особисті характеристики якої об’єктивно говорять про можливість здійснення нею у майбутньому злочинного діяння. Спеціальне попередження повинно передбачати заходи формування та ведення оперативних і профілактичних обліків визначених груп суб’єктів підвищеного кіберкриміногенного ризику, активізацію превентивної діяльності щодо виявлення осіб, схильних до вчинення кіберзлочинів, запобігання й припинення їх кримінальної активності тощо [7].

Загальне попередження кіберзлочинів:

– являє собою системні соціальні заходи державних органів Національної системи кібербезпеки, громадських організацій та бізнесу, які спрямовані на зниження ризику вчинення кіберзлочинів, усунення або зменшення потенційно шкідливих наслідків від їх вчинення;

– реалізується шляхом управління кібербезпекою на корпоративному рівні, забезпеченням широких верст населення надійними засобами і послугами із кіберзахисту, формуванням обізнаності суспільства в питаннях кіберзахисту, що стосуються, насамперед, організаційно-технічних та правоохоронних аспектів;

– орієнтоване на категорію потенційних потерпілих від кіберзлочинів, які не є фахівцями з ІТ-технологій та кіберзахисту, має за мету зменшення їх уразливості за рахунок формування глобальної культури кібербезпеки.

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

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

Історично, термін “культура кібербезпеки” був використаний саме у глобальному розумінні в Резолюції Генеральної Асамблеї “Створення глобальної культури кібербезпеки” (Creation of a global culture of cybersecurity) у 2002, 2003 та 2009 роках, хоча у цих документах не запропоновано його визначення. Зазначені документи були запропоновані як рекомендації для розроблення національних стратегій кібербезпеки, що визначають сутність національних систем кібербезпеки та заходи з поширення передових практик кіберзахисту.

Досліджуючи дефініцію “глобальна культура кібербезпеки” доцільно, перш за все, звернути увагу на концепти масової та глобальної культури. Так, спираючись на поняття кібербезпеки і кіберпростору, під “масовістю” будемо розуміти обсяг носіїв культури,

фактично, широкі верстви населення – масового користувача. В свою чергу, під “глобальністю” розуміємо не інтеграцію національних культур, а феномен наднаціональної професійної культури. Тобто, глобальну культуру кібербезпеки можна розглядати як наднаціональну масову культуру кібербезпеки, що охоплює категорії “культури кібербезпеки”, “інформаційної культури”, “професійної культури”, “культури” тощо.

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

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

У філософії культура (матеріальна і духовна категорія) розглядається у всесторонньому історичному розумінні як: процес розвитку людських сил і здібностей; показник міри людського в людині; характеристика розвитку людини як людської істоти; процес освоєння природи, який одержує своє зовнішнє вираження у всьому багатстві і різноманітті створюваної людьми дійсності, у всій сукупності результатів людської праці і думки. При цьому, на думку більшості сучасних філософів, в структурі феномена культури можна виділити два класи елементів. Перший характеризує культуру як систему еталонів суспільної поведінки людей, другий – як систему, що здійснює соціальний контроль над цінностями та ідеями. Вочевидь, у контексті запобігання кіберзлочинності доцільно розглядати матеріальну культуру в розумінні системи еталонів суспільної поведінки людей.

В даний час у культурології виділяють передусім наступні аспекти культури як неприродного штучного явища:

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

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

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

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

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

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

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

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

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

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

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

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

У загальному випадку Вікіпедія пропонує розуміти під культурою сукупність матеріальних та духовних цінностей, створених людством протягом його історії; історично набутий набір правил всередині соціуму для його збереження та гармонізації. Серед видів культури – культуру суспільства, організації та особистості.

Отже, виходячи із завдань запобігання кіберзлочинності варто звернути увагу на психологічний, правовий та соціологічний аспекти культури суспільства, особистості соціальної взаємодії з формування досвіду, розвитку форм та способів інформаційній діяльності у кіберпросторі.

Далі розглянемо таку категорію як “професійна культура” і її складові – “правову, управлінську та інформаційну культуру”, “культуру кібербезпеки” відповідно. В науковому середовищі запропоновано багато визначень професійної культури як специфічної культури професійного товариства та його представників, зокрема, з позицій аксіологічного, діяльнісного та особистісного підходів під професійною культурою можна розуміти [8]:

– систему професійних цінностей, професійних норм і переконань, професійних традицій, що обумовлюють ставлення фахівців до предметів і об’єктів їх діяльності;

– єдність професійної зрілості, професійної етики, естетики, громадянської й етичної вихованості;

– характеристика рівня і якості професійної діяльності, яка залежить від соціально-економічного стану суспільства й сумлінності в оволодінні певними знаннями, навичками конкретної професії та їх практичному використанні;

– інтегральний показник діяльності, що забезпечується єдністю та взаємодією всіх її чинників, включаючи тезаурус і кругозір, вміння і здібності, діапазон інтересів, світогляд, норми і методи діяльності, культуру почуттів тощо.

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

Інформаційна культура передбачає також [9] високий рівень загальної культури міжособистісного спілкування; готовність толерантно сприймати іншу точку зору; вміння аргументовано вести дискусії, готовність визнати себе переможеним у цій дискусії; готовність не тільки отримувати нові знання, а й ділитися своїми; знання норм і правил, що регламентують використання інтелектуальної власності і готовність користуватися ними тощо.

Виходячи із мети та завдань статті, зосередимо увагу на наступних аспектах професійної культури: етичних нормах інформаційної діяльності, компетентності; змісті, видах, та методах професійного переконання суспільства щодо необхідності виконання етичних норм та технічних регламентів безпеки, формуванні професійної зрілості широких верств населення з питань кібербезпеки.

Крім того, звернемо також увагу на визначення культури кібербезпеки у звіті 2017 року Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) “Культура кібербезпеки організації” [10]: знання, переконання, уявлення, норми і цінності людей по відношенню до кібербезпеки та використанню інформаційних технологій.

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

У свою чергу, “глобальною культурою кібербезпеки” будемо вважати наднаціональну масову культуру кібербезпеки суспільства, організацій та особистості.

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

Далі зазначимо, що у Резолюції Генеральної Асамблеї ООН було запропоновано дев’ять взаємопов’язаних принципів глобальної культури кібербезпеки: *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що 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 ефективне співробітництво з попередження, виявлення та реагування на такі інциденти); *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); *проектування та впровадження засобів забезпечення безпеки; переоцінка* (належні та своєчасні заходи з внесення змін у політику, практику забезпечення безпеки з урахуванням нових та зміни існуючих загроз)

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

Заходи формування обізнаності громадян з питань забезпечення кібербезпеки відбуваються шляхом інформування співробітників організацій та установ різних форм власності: в засобах масової інформації; на веб-ресурсах державних і приватних структур; на конференціях, семінарах та тренінгах; при реалізації освітніх програм в середніх і вищих навчальних закладах. Формування та підтримка ринку засобів і послуг із забезпечення

кібербезпеки передбачає: заходи нормативно-правового регулювання сфери технічного і криптографічного захисту інформації; створення громадських організацій для надання правової і технічної допомоги громадянам для забезпечення їх кібербезпеки; розбудову національної системи оповіщення про кібератаки та кіберінциденти; започаткування механізмів страхування ризиків та інших інструментів управління кібербезпекою.

Висновки.

Формування глобальної культури кібербезпеки є дієвим механізмом запобігання кіберзлочинності, який спрямовано на попередження, виявлення й усунення причин та умов, які сприяють вчиненню кіберзлочинів. Мова йде про системні заходи забезпечення життєво важливих інтересів осіб у кіберпросторі, з позицій захисту інформації та інформаційно-психологічного захисту.

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

Перспективою подальших досліджень є нормативно-правові та організаційні аспекти формування глобальної культури кібербезпеки на національному та міжнародному рівні.

Використана література

1. Довгань О.Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія / О.Д. Довгань, І.М. Доронін. – (НДІ інформатики і права НАПрН України – К. : Видавничий дім “АртЕк”. – 2017. – 107с.

2. CERT-UA. – Режим доступу : https://cert.gov.ua

3. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності // Інформація і право. – 2018. – № 1(24). – С. 127-132.

4. Гавловський В.Д. Кримінологічний аналіз злочинів, учинених з використанням соціальних мереж // Інформація і право. – 2017. – № 3(22). – С. 101-107.

5. Кіберполіція Києва. – Режим доступу : https://kyivcity.gov.ua/bezpeka_ta_pravoporiadok/kyivska_politsiia/kiberpolitsiia_kyieva.html

6. Серьогін В.С., Леонов Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов’язаних з неправомірним дистанційним доступом до комп’ютерної інформації // Інформація і право. – 2017. – № 2(21). – С. 108-115.

7. Кравцова М.О. Кіберзлочинність : кримінологічна характеристика та запобігання органами внутрішніх справ : автореф дис. на здобуття наук. ступеня к.ю.н. : 12.00.08 / М.О. Кравцова. – (Харківський університет внутрішніх справ). – Харків, 2016. – С. 19.

8. Миколаєнко Н.М. Сутнісна характеристика поняття “професійна культура” / Естетичне виховання дітей та молоді : теорія, практика, перспективи розвитку : зб. наукових праць ; за ред. О.А. Дубасенюк, Н.Г. Сидорчук. – Житомир : Вид-во ЖДУ ім. І. Франка, 2012. – С. 539-545.

9. 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. – Ст. 60-62.

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

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