УДК 34:004.9

ПРАВОВЕ РЕФОРМУВАННЯ КІБЕРЗАХИСТУ

Іван ФЛИС[1], Василь ТКАЧЕК[2]

[1] ПрАТ «ВНЗ "МАУП"», (Львівський інститут), Україна
[2] Львівський державний університет фізичної культури імені Івана Боберського, Україна

Вступ. З активним розвитком у різних сферах діяльності людини інформаційних технологій, глобалізації інформаційних процесів і появи глобальних комп'ютерних мереж, кінець XX — початок XXI ст. позначився появою нової специфічної інформаційної протиправної діяльності, що передбачає використання комп'ютерів, комп'ютерних мереж або мережевих пристроїв у посяганні на урегульовані законодавством суспільні відносини в інформаційному просторі, — кіберзлочинністю.

«Кіберзлочинність» як загальне поняття кримінальної діяльності, що з'явилася на інтернет-просторах, охоплює весь спектр злочинів у сфері інформаційних технологій, чи це використання комп'ютерних мереж для вчинення злочину, чи будь-який злочин, скоєний за допомогою комп'ютерів, комунікаційних мереж та інформаційних систем або злочини, предметом яких є інформація, що зберігається в них. Як протидія кіберзлочинності, кібербезпека — це такий стан захищеності життєво важливих інтересів особистості, суспільства й держави в умовах використання комп'ютерних

систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність і невірогідність інформації, що використовують; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання й порушення цілісності, конфіденційності й доступності інформації.

Мета — проаналізувати стан і показати потребу кіберзахисту в боротьбі з кіберзлочинністю.

В безпековому полі України в повному обсязі наявні всі ключові «класичні» кіберзлочини, а їхня кількість щорічно зростає у 2,5 раза. За словами високих представників кіберполіції України, у червні 2016, у рік створення Національного координаційного центру кібербезпеки, збитки від кіберзлочинів збитки сягнули близько 39–40 млн. гривень. Протягом 2022 року фахівці Держспецзв'язку зареєстрували в Україні понад 2 тисячі кіберінцидентів та ще більшу кількість кібератак. Збитки від шахрайства з використанням методів соціальної інженерії тільки 2022 року становили понад 1 млрд. грн.

У червні 2017 р. відбулася наймасштабніша кібернетична атака, що зупинила роботу декількох тисяч українських компаній і державних органів. Лише упродовж одного дня комп'ютерний шкідник «Ransom: Win33/Petya» атакував державний і приватний сектор економіки країни. Атаки зазнали банки, держзалізниця, аеропорти, телекомпанії, гіганти-супермаркети, державні фіскальні служби, органи місцевого самоврядування тощо. Вірус-вимагач заморозив дані і вимагав внесення викупу в криптовалюті за відновлення доступу. Безпекові структури виявилися безсилими в протистоянні злочинним діям зловмисників. Загалом можна констатувати, що кількість реєстрованих! злочинів демонструє виразну тенденцію до зростання абсолютно за всіма основними статтями кримінального законодавства України, що стосуються злочинів, скоєних із використанням високих інформаційних технологій. Держава, далеко не завжди реально обізнана з масштабами кіберзлочинності, більшість інцидентів залишаються незафіксованими або не публікуються в офіційних звітах державних органів.[5] Наразі кіберпростір є ідеальним місцем для безкарного вчинення злочину. Як зазначає американський журнал «The Economist», «кіберепростір — це п'ятий регіон воєнних дій, після землі, моря, повітря й космосу».

Упродовж останніх років Україна реалізквала заходи щодо вдосконалення законодавства у сфері кібербезпеки. Водночас, слід зазначити, що прогнози українських експертів щодо позитивного рівня й стану готовності кібербезпеки невтішні. Якщо узагальнено, то «уявлення України про кібербезпеку поки досить абстрактні, проте ведеться активна робота в цьому напрямі. Кожне з відомств вживає заходів щодо безпеки й веде статистику відповідних показників, проте їхня діяльність охоплює тільки окремі власні сфери відповідальності. Цілісна політика поки відсутня, як і універсальні індикатори кібербезпеки, що могли б охарактеризувати її рівень», — саме так проблему висвітлюють у Національному інституті стратегічних досліджень. Проблема полягає в тому, що українська правоохоронна система сконцентрована на майнових злочинах і злочинах проти життя й здоров'я. А законодавство у сфері інформаційних технологій, доступу до інформації та захисту персональних даних в Україні почало розвиватися лише у 2010-х роках. І досі система ігнорує це питання.

В Україні кібербезпеку вважають складником національної безпеки, вона грунтується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року, а також Стратегії кібербезпеки, яку затвердив Указ Президента України 15 березня 2016 року. Оновлені з урахуваннями часу й вимог Стратегії ухвалювали також у 2015 та 2021 рр.

У липні 2018 року ухвалено закон «Про основні засади забезпечення кібербезпеки України», що радше, як заявляють фахівці, є дорожньою картою для розроблення майбутніх нормативних актів, а не законом про кібербезпеку, який регулює повний спектр питань кібербезпеки й відповідає міжнародним стандартам і найкращим практикам. Відповідно, цей напрям роботи і досі потребує значної уваги й відповідних зусиль. Закон визначив основні завдання й компетенцію суб'єктів забезпечення кібербезпеки, до яких належить Національний координаційний центр кібербезпеки, МО, Генштаб ЗСУ, Державна служба спеціального зв'язку й захисту інформації, СБУ, Національна поліція, Національний банк, розвідувальні органи України тощо. Також передбачено створення умов для залучення до співпраці підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних

комунікацій, захисту інформації, та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян. До основних досягнень зазначеного Закону також належить впровадження до правового поля однозначних правових визначень, що стосуються кібербезпеки, кібератак, кіберзахисту тощо. Відтак Закон України «Про основні засади забезпечення кібербезпеки України» є важливим кроком держави у сфері регулювання кіберпростору. Також «критичні інформаційні структури» як об'єкти зобов'язані проходити обов'язковий аудит з кібербезпеки й відповідати інфраструктурним вимогам Кабінету Міністрів України.

Нині правову основу кібернетичної безпеки України гарантують Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки», Доктрина інформаційної безпеки, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

Фахівці галузі зазначають, що в Україні є потреба змінити національне законодавство відповідно до сучасних міжнародних стандартів, на сьогодні галузі бракує і високих технологій, і належних методологій із кібербезпеки. Фактично відсутня імплементація реальних заходів кіберзахисту в IT-інфраструктурах, наявний слабий процес навчання й підвищення обізнаності у питань кібербезпеки.

Висновок. Україна повинна беззаперечно виконувати вимоги для операторів об'єктів критичної інфраструктури щодо інформування із зазначенням обставин, за яких вони повинні інформувати про інциденти, а також категоризацію кіберінцидентів, установити процедуру інформування інших держав про кіберінциденти, які можуть на них вплинути, з урахуванням вимог конфіденційності й комерційної таємниці, здійснити аудит чинного Законодавства. Протидія дезінформаційним кампаніям з міркувань національної безпеки, формування правових механізмів протидії дезінформації в соціальних медіа в контексті національної безпеки здійснюються недостатньо продуктивно. Президент України Указом № 187/2021 затвердив Положення «Про створення Центру протидії дезінформації»,

яким встановив його сфери впливу: воєнний напрям, боротьбу зі злочинністю та корупцією, зовнішню й внутрішню політику, економіку, інфраструктуру, екологію, охорону здоров'я, соціальну сферу та науково-технологічний напрям. Але основну увагу зосереджено на протидії поширенню неправдивої інформації в Інтернеті та фейків у медіа. Центр не має каральних функцій за дезінформацію і не зможе застосовувати санкції, але може вносити подання до РНБО щодо певних порушень. Зважаючи на суспільно негативні наслідки, які спричиняє дезінформування, доцільно законодавчо цей вид інформаційного правопорушення внести в кримінальне й адміністративне законодавства у вигляді окремого складу правопорушення за умисне поширення неправдивої, неточної або такої, що вводить в оману інформації.