УДК 343.53:004.738.5
DOI: 10.31733/15-03-2024/2/355-357

Ростислав ЗАРДОВ
студент ННІ права
та інноваційної освіти

Таїсія ШЕВЧЕНКО
старший викладач кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ

ВПЛИВ КІБЕРЗЛОЧИННОСТІ НА КРИМІНАЛЬНИЙ ПРОЦЕС В УКРАЇНІ: СТРАТЕГІЇ ТА ПРІОРИТЕТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

У сучасному світі інформаційні технології стають неодмінною складовою всіх сфер життя суспільства. Зростаюча кількість інтернет-користувачів та розвиток цифрових технологій створюють нові можливості для комунікації, навчання, розваг та розвитку бізнесу. Проте, разом із цим, зростає й загроза кіберзлочинності. Кібератаки, крадіжки даних, онлайн-шахрайство та інші види кіберзлочинності є серйозними викликами для кримінального правосуддя.

Так, на законодавчому рівні, кібербезпека регулюється законом України «Про основні засади забезпечення кібербезпеки України».

Зі ст. 4 цього закону можна зрозуміти що об'єктами кібербезпеки та кіберзахисту можуть бути:

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.

Об'єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1].

В Україні, як і в інших країнах, кіберзлочинність стала предметом розгляду та регулювання в кримінальному процесі. Під впливом швидкого розвитку технологій та зміни уявлень про злочинну діяльність, правоохоронні органи та законодавці стикаються з необхідністю постійного удосконалення законодавства та стратегій боротьби з кіберзлочинністю.

На жаль, одна з проблем у цьому контексті полягає в тому, що державні органи з кібербезпеки не можуть забезпечити захист усіх суб'єктів кіберпростору вчасно. Це призводить до того, що організації та комерційні підприємства також повинні докласти зусиль для забезпечення своєї власної кібербезпеки. Крім того, важливою є не лише кібербезпека на рівні держави чи організації, але і на рівні окремої особи, яка може стати найбільш слабкою ланкою у системі кібербезпеки [2. С.8].

Однією з основних стратегій забезпечення кібербезпеки в Україні є підвищення кваліфікації правоохоронців та працівників судової системи. З урахуванням швидкого темпу розвитку технологій, необхідно постійно навчати правоохоронців новим методам

виявлення та розслідування кіберзлочинності. Також важливо забезпечити їх доступ до сучасних технічних засобів для аналізу цифрових доказів. Потрібні координація і переорієнтація наукових досліджень і розробок у сфері комп'ютерної безпеки, в області вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливий напад і локалізацію джерела нападу [3, С. 155].

Іншою важливою стратегією є співпраця з міжнародними партнерами у сфері кібербезпеки. Злочинні мережі та хакерські групи діють без врахування кордонів, тому важливо мати міжнародну співпрацю для обміну інформацією та спільних дій у боротьбі з кіберзлочинністю. Для досягнення мети забезпечення більш високого рівня мережевої та інформаційної безпеки в межах Європейського Союзу, необхідно вжити заходів у трьох основних напрямках:

– підвищити спроможність системи кібербезпеки на національному рівні;

– підвищити рівень європейського співробітництва;

– запровадити управління ризиками та зобов'язати сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг [4, С. 105].

А також, важливо розвивати ефективні законодавчі механізми для протидії кіберзлочинності. Воно містить у собі не лише прийняття нових законів, але й постійний моніторинг їх ефективності та готовність до змін у зв'язку з технологічним прогресом. Важливим елементом є також сприяння розвитку кібербезпеки в приватному секторі шляхом створення стимулів для компаній у впровадженні заходів захисту інформації та даних.

Проте, найважливішою стратегією в боротьбі з кіберзлочинністю є попередження. Забезпечення кібербезпеки має бути комплексним підходом, що має у своєму складі як технічні заходи, так і освітні програми для громадян щодо безпеки в інтернеті. Навчання людей розпізнавати потенційні загрози та захищати свої дані може значно зменшити кількість успішних кібератак.

Окрім зазначених стратегій та пріоритетів, існують інші важливі аспекти, які необхідно враховувати при забезпеченні кібербезпеки та впливі кіберзлочинності на кримінальний процес в Україні.

Один із таких аспектів – це взаємодія між різними секторами суспільства. Кіберзлочинність може впливати на різні сфери, включаючи державні установи, приватні компанії, фінансові установи та інші організації. Тому важливо створити ефективні механізми співпраці між ними для обміну інформацією про загрози та спільних дій у разі кібератак.

Додатково потрібно приділяти увагу захисту критично важливої інфраструктури, такої як енергетичні системи, транспортні мережі та комунікаційні системи. Атаки на такі об'єкти можуть мати серйозні наслідки для безпеки та економічного розвитку країни.

Також, важливо розвивати інформаційно-аналітичні центри, які спеціалізуються на виявленні та аналізі кіберзлочинності. Ці центри можуть забезпечити правоохоронні органи та інші зацікавлені сторони актуальною інформацією про потенційні загрози та способи їх протидії.

Невід'ємною частиною стратегії забезпечення кібербезпеки є також заохочення інновацій та розвитку нових технологій у сфері кіберзахисту. Воно має містити в себе розробку нових методів виявлення загроз, створення захищених систем зберігання даних та розробку криптографічних технологій.

Отже, підсумовуючи усе вищесказане, можна сказати, що успішне забезпечення кібербезпеки та протидія кіберзлочинності вимагає комплексного підходу, який охоплює не лише правоохоронні органи та законодавство, але й враховує взаємодію між різними секторами суспільства, розвиток інформаційно-аналітичних центрів та заохочення інновацій у сфері кіберзахисту. Тільки за умови взаємодії та координації всіх зацікавлених сторін можна забезпечити ефективний захист від кіберзагроз і зберегти безпеку та стабільність в цифровому світі.

---

1. Закон України «Про основні засади забезпечення кібербезпеки України». (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Гайтота Є.В., Чуницька В.В., Нікуліщев Г.І. Про перспективи Стратегії кібербезпеки України.

Матеріали Всеукраїнського науково-практичної конференції 23-25 листопада 2016 року, м. Кропивницький. С. 7-8. URL : https://core.ac.uk/download/84825385.pdf.

3. Олена Трофименко, Юлія Прокоп, Наталія Логінова, Олександр Задерейко. Кібербезпека України: Аналіз сучасного стану. Захист інформації, том 21, № 3, липень-вересень 2019, с. 150-158. URL : https://dspace.onua.edu.ua/server/api/core/bitstreams/3acf4b52-6858-4bda-973c-35535be8fcfe/content.

4. Ольга Бакалінська, Олександр Бакалинський. Правове забезпечення кібербезпеки в Україні. 9/2019 Адміністративне право і процес. С. 100-108. URL : http://pgp-journal.kiev.ua/archive/2019/9/18.pdf.

5. Ісланкін С.М. Відсторонення від посади: Міжнародний досвід. Регламентації. Правова позиція № 4 (37) 2022. С. 271-274. URL : https://legalposition.umsf.in.ua/archive/2022/4/51.pdf.

УДК 004.738.5:351.862.4
DOI: 10.31733/15-03-2024/2/357-358

Ярослав ІЖИК
курсант факультету підготовки
фахівців для підрозділів
кримінальної поліції

Олександр ЖУРАВЕЛЬ
старший викладач кафедри
спеціальної фізичної підготовки
Дніпропетровського державного
університету внутрішніх справ,
доктор філософії

ЩОДО ОСНОВНИХ НАПРЯМІВ ТА ОСОБЛИВОСТЕЙ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ В УКРАЇНІ

З 24 лютого 2022 року, з початком повномасштабної агресії з боку росії, український кіберпростір зазнав безпрецедентного натиску. Кібератаки та збої стали зброєю ворога, спрямованою на дестабілізацію роботи державних сайтів, банківських систем, критичної інфраструктури.Під прицілом опинилися сайти Верховної Ради, Кабміну, МЗС, СБУ, Міноборони, Мінреінтеграції, ПриватБанку, Ощадбанку та багатьох інших установ.

Війна в інформаційному просторі несе не меншу загрозу, аніж бойові дії на фронті. Ризик кібератак з боку рф залишається високим як для України, так і для її європейських партнерів. Кібербезпека набуває ключового значення в економічній, політичній, соціальній та військовій сферах.

Сьогодні Україна відстоює не лише свою територіальну цілісність, але й право на незалежність, самостійний розвиток та мирне майбутнє. Перед вітчизняними правоохоронними органами постає все більше завдань з пошуку нових методів та засобів для ефективної протидії кіберзлочинності.

Державна політика України у сфері національної безпеки й оборони має комплексний характер і спрямована на забезпечення стійкості держави перед різними викликами та загрозами й регламентується Законом України «Про національну безпеку України» від 21 червня 2018 р. № 2468-VIII [1].

Стратегія кібербезпеки України (далі – Стратегія) – це документ довгострокового планування, який визначає:

– Загрози кібербезпеці: Стратегія ідентифікує актуальні та потенційні кіберзагрози для життєво важливих інтересів особи, суспільства та держави.

– Пріоритети: Визначає пріоритетні напрямки та концептуальні підходи до забезпечення кібербезпеки.

– Цілі: Створення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства й держави.

Стратегія кібербезпеки України – це ключовий документ, який визначає курс України на забезпечення стійкості кіберпростору та захисту національних інтересів у цій сфері [2].

Кібербезпека України – це динамічна сфера, що потребує постійного вдосконалення та адаптації до нових викликів. Забезпечення стійкості кіберпростору держави ґрунтується на виваженій політиці, чітко окреслених пріоритетах та комплексних