УДК 004.056.53:351.862.4
DOI: 10.31733/15-03-2024/2/387-388

Вероніка ТИМОЩЕНКО
здобувач вищої освіти

Юлія СИНИЦІНА
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

СТАН КІБЕРБЕЗПЕКИ В УКРАЇНІ ВИКЛИКИ ТА ЗАГРОЗИ

На сучасному етапі розвитку кіберпростору виникла переконаність у тому, що видалення інформації з глобальної мережі є завданням відносно набагато складнішим, ніж її розміщення. Ця проблема виникає через специфіку структури та функціонування Інтернету, де інформація може бути швидко поширена та збережена в найрізноманітніших куточках віртуального простору. Таким чином, видалення даних вимагає від користувача спеціальних знань, витрат терпіння та матеріальних ресурсів [1, с. 58].

Актуальність теми очевидна через кілька ключових факторів, а саме:

Зростання кіберзлочинності: Україна, як і багато інших країн, стикається зі зростанням кіберзлочинності, що включає в себе кібератаки, шахрайство, витоки даних та інші кіберзагрози. Це ставить під загрозу як індивідуальні громадяни, так і підприємства та урядові структури.

Геополітичні конфлікти та кібервійна: Україна перебуває в складній геополітичній ситуації, де кібератаки можуть бути використані як знаряддя віртуальної війни. Захист критично важливої інфраструктури та державних систем є надзвичайно важливим для національної безпеки.

Цифрова трансформація: Україна активно просувається в цифровій трансформації, що створює нові можливості, але також збільшує ризики в кіберпросторі. Великі обсяги даних та підключеність до Інтернету роблять компанії та організації більш уразливими перед кібератаками.

Необхідність захисту особистої інформації: Захист особистої інформації громадян є ключовим аспектом кібербезпеки. Із зростанням використання цифрових технологій зростає і значення захисту приватності та конфіденційності даних.

Важливість кіберінфраструктури для економіки: Наявність надійної кіберінфраструктури є ключовою для економічного розвитку країни. Кібератаки на бізнес-структури можуть призвести до серйозних фінансових втрат та порушень в роботі підприємств.

Отже, тема кібербезпеки в Україні має велику актуальність через поєднання технологічного розвитку, геополітичних чинників, захисту особистих даних та важливості для економіки країни. Розвиток стратегій та заходів з кібербезпеки стає необхідністю для забезпечення національної безпеки та стійкості у цифровому віці

Важливо пам’ятати, що інформація, яку користувач залишає про себе в мережі, може стати об’єктом негативного використання проти нього. Особливо важливою стає проблема кібербезпеки в умовах воєнного конфлікту, де ворог може оперувати поза моральними та етичними нормами. Основною метою кібератак у таких умовах є дестабілізація ситуації в країні, знищення або приховане утримання «невигідної» для них інформації, а також атака на інфраструктуру обробки та зберігання даних [2, с. 33].

Тривожним є існування внутрішніх загроз безпеці кіберпростору, що можуть включати установу колаборантських зв’язків з потенційними ворогами. У зв’язку з цим умови воєнного стану вимагають оновлення правових норм щодо кібербезпеки. Саме тому було прийнято рішення про редакцію статті 361 Кримінального кодексу України та утворення нового закону під назвою 2149-IX [3]. Метою цього нового законодавчого акту є:

– оптимізація та посилення можливостей національної системи кібербезпеки для протидії загрозам, що виникають з кіберпростор;

– впровадження нових кримінально-правових механізмів для протидії кіберзлочинності;

– забезпечення безпечного використання цифрових послуг державного значення.

Завдяки новому закону відбулося оновлення формулювання статті 361 Кримінального кодексу України. Зокрема, відбулася зміна оцінки категорії шкоди, а також посилені санкції за кримінальні порушення. Значна увага була приділена інструментам протидії білим хакерам та учасникам програми Bug Bounty, які відіграють важливу роль у виявленні та ліквідації вразливостей в інформаційних системах та мережах [4].

У сучасному суспільстві, де інформаційні технології займають центральне місце у бізнесі та повсякденному житті, виникає реальна загроза безпеці від людського фактора у кіберпросторі. Цей аспект особливо актуалізується у контексті воєнних конфліктів, коли інформація може бути використана в якості зброї, а виток конфіденційних даних через працівників може стати серйозною загрозою для безпеки.

Регулярні консультації та тренінги з питань створення ефективної політики безпеки в кіберпросторі є ключовим елементом у протидії таким загрозам. Важливо, щоб співробітники мали доступ до достовірних джерел інформації щодо поточної ситуації та були обізнані з ризиками фішингу та шахрайських вебсайтів, особливо з тематикою воєнних подій в конкретній країні.

Важливо забезпечити співробітників інформацією про те, як розпізнати потенційно небезпечні ситуації та як захистити себе від кіберзлочинів. Тренінги з кібербезпеки мають бути спрямовані на працівників, які знаходяться в місцях потенційного ризику, таких як правоохоронні органи та державні службовці у секторі оборони. Крім того, важливо забезпечити їм психологічну підтримку та надати поради щодо дій у кризових ситуаціях, включаючи кібератаки.

Управлінням повинно бути приділено увагу терміновій підтримці звичайних функцій безпеки, аналізу збільшеного обсягу сповіщень про загрози та впровадженню термінових заходів щодо забезпечення безпеки. Важливо розробити стратегії реагування на кіберзагрози та підготувати персонал до ефективного виконання цих стратегій у надзвичайних ситуаціях [1, с. 26].

Відтак, умови воєнного стану підкреслюють важливість вжиття заходів із кіберзахисту та попередження витоку конфіденційної інформації через людський фактор. Дотримання простих організаційних та управлінських правил, таких як надання доступу до достовірної інформації та проведення тренінгів з кібербезпеки, може значно зменшити ризик втрати конфіденційності та небажаних наслідків у кіберпросторі.

У висновках можна підкреслити наступні ключові моменти:

Складність видалення інформації з кіберпростору: Видалення інформації з Інтернету є складним завданням через його структуру та функціонування. Це вимагає спеціалізованих знань, терпіння та матеріальних ресурсів.

Актуальність теми кібербезпеки в Україні: Зростання кіберзлочинності, геополітичні конфлікти, цифрова трансформація, необхідність захисту особистої інформації та важливість кіберінфраструктури для економіки роблять тему кібербезпеки актуальною в українському контексті.

Удосконалення законодавства та політики: Новий законодавчий акт із кібербезпеки в Україні відображає потребу у вдосконаленні механізмів захисту в кіберпросторі, включаючи підвищення санкцій за кіберзлочини та підтримку білих хакерів.

Необхідність освіти та підготовки персоналу: Забезпечення тренінгів з кібербезпеки та психологічної підтримки співробітників у воєнних умовах допоможе зменшити загрозу з боку людського фактора та ефективно реагувати на кіберзагрози.

Відповідно, виклики та загрози в сфері кібербезпеки в Україні потребують комплексного підходу, у складі якого є як законодавчі та політичні заходи, так і освіту та підготовку персоналу. Лише такий підхід дозволить ефективно протидіяти кіберзагрозам у сучасному цифровому світі.

1. Карпеченков, М. П., Тулупов В. В. Кібербезпека в умовах війни: що, хто, як. 2022. С. 481
2. Вінник, О. М. Захист прав користувачів електронних комунікаційних послуг в умовах війни. Economics and Law. 2022. С. 68-78.
3. Закон України про внесення змін до Кримінального Кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022 № 2149-IX. URL : https://zakon.rada.gov.ua/laws/show/2149-20#Text.
4. Микола Єрема Боротьба з кіберзлочинністю в умовах дії воєнного стану Закон 2149-IX /Ліга: Закон: офіційний вебсайт. URL : https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-vumovakh-d-vonnogo-stanu-zakon-2149-ix