СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ ТА ЇХ ВПЛИВ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

DOI https://doi.org/10.36059/978-966-397-550-4-56

Мариніч П. В.
здобувач
Одеський державний університет внутрішніх справ
м. Одеса, Україна
Науковий керівник: **Грезіна О. М.**
доктор філософії, доцент кафедри кримінального аналізу
та інформаційного аналізу
Одеський державний університет внутрішніх справ
м. Одеса, Україна

У сучасному світі стрімкий розвиток інформаційних технологій приносить не лише переваги для економіки, державного управління та повсякденного життя, а й створює нові загрози. Однією з найнебезпечніших є кіберзлочинність, яка охоплює широкий спектр злочинних дій – від шахрайства та викрадення персональних даних до атак на державні органи та критичну інфраструктуру. З кожним роком масштаби, складність і наслідки таких злочинів зростають. Хакери атакують державні установи, банки, медичні заклади та об'єкти енергетики, що може спричинити масові відключення електроенергії та паралізувати роботу цілих регіонів.

В Україні спостерігається в середньому 15 кібератак на день з боку держави-агресора. Атаки спрямовані на інфраструктуру (енергетика, телекомунікації), які супроводжують чи передують військовим діям, а також включають віруси/шкідливе ПЗ, що вражає електростанції чи енергосистему. Крім того, проводяться масштабні операції дезінформації, поширення фейків, маніпуляцій громадською думкою та пропаганди – із застосуванням соціальних мереж, ботів і мемів. Атаки на енергетичні, транспортні, медичні та водопостачальні системи можуть спричинити катастрофічні наслідки – як економічні, так і соціальні.

Найпоширенішими видами шахрайства у віртуальному просторі є продаж неіснуючих товарів та фішингові онлайн-магазини. Злочинці часто ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або в соцмережах, вимагаючи повну передоплату, після чого зникають. Правоохоронці та власники платформ, наприклад OLX, намагаються протидіяти цьому: модератори видаляють заборонений

контент і блокують публікації товарів, що вимагають особливих умов зберігання.

Кіберзлочинність перетворилася на серйозну загрозу для національної безпеки. Зловмисники шифрують важливі файли та вимагають викуп за розшифрування, часто у криптовалюті. Такі атаки спрямовані на великі компанії чи державні структури для отримання високих виплат. Кібершахраї використовують психологічні прийоми для маніпуляції: фішингові листи чи підроблені сайти для викрадення логінів, паролів і банківських даних. Існують підпільні ринки, де продаються послуги з атак, шкідливе ПЗ та анонімний хостинг. Навіть без технічних знань можна замовити хакерську атаку.

Використання штучного інтелекту (AI) та машинного навчання хакерами для автоматизації атак, створення фейкових зображень, голосів (deepfake) або прогнозування слабких місць у системах захисту [1]. Біткойн та інші криптовалюти використовуються для анонімних переказів, відмивання грошей та фінансування злочинів. Хакерські угруповання, часто підтримувані ворожими державами, проводять шпигунські операції проти урядових структур, оборонних підприємств та дипломатичних місій. Поширення фейкових новин, злив конфіденційної інформації, втручання у вибори чи судові процеси дестабілізують суспільство та підривають довіру до влади.

Кібератаки завдають колосальної шкоди економіці: глобальні збитки перевищують трильйони доларів щорічно. Вони стали елементом гібридної війни поряд з інформаційними кампаніями, економічним тиском і пропагандою. Такі атаки важко ідентифікувати та реагувати на них. Механізми вчинення кібератак постійно вдосконалюються [3].

Починаючи з лютого 2021 року, Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони фіксує масовані DDoS-атаки на український сегмент Інтернету, переважно на веб-сайти сектору безпеки і оборони, зокрема на сайти СБУ, РНБО та інших державних установ. Джерелом атак є IP-адреси російських мереж. Зловмисники використовують новий механізм: інфікують вразливі веб-сервери державних органів вірусом, роблячи їх частиною бот-мережі для DDoS-атак. Системи безпеки провайдерів блокують ці сервери, роблячи сайти недоступними навіть після атаки.

Для протидії необхідні спеціалізовані підрозділи в МВС, СБУ, Міністерстві оборони для оперативного виявлення та запобігання атакам. Оскільки кіберзлочини часто транскордонні, важливий обмін інформацією між країнами та участь у міжнародних ініціативах. Кожен користувач повинен знати основи кібергігієни: надійні паролі, розпізнавання фішингу, захист даних. Інвестиції у технології захисту, включаючи системи штучного інтелекту, багатофакторну аутентифікацію, шифрування та

кібермоніторинг, підвищують стійкість [1; 2]. Законодавство потрібно адаптувати: чітко визначити кіберзлочини, встановити відповідальність, спростити міжнародний розшук.

Відповідно до Рішення РНБО «Про Стратегію національної безпеки України» від 14.09.2020 р., введеного Указом Президента № 392/2020, основне завдання – гарантування кіберстійкості національної інформаційної інфраструктури в умовах цифрової трансформації. Національна безпека неможлива без надійної кібербезпеки.

Боротьба з кіберзлочинністю повинна стати пріоритетом на всіх рівнях – від індивідуального до глобального. Об'єднання зусиль держави, суспільства, бізнесу та міжнародних партнерів дозволить протидіяти викликам цифрової епохи. Тенденції кіберзлочинності, пов'язані зі збройним конфліктом, – це новий фронт, який визначає виживання нації.

Література:

1. Zheng K. Next-Generation Cybersecurity Threat Detection: Integration with Artificial Intelligence. *Highlights in Science, Engineering and Technology*. 2025. Vol. 138. P. 8–16. DOI: https://doi.org/10.54097/nx38v729

2. B. H. Kumar, S. T. Nuka, M. Malempati, H. K. Sriram, S. Mashetty, S. Kannan. Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML. *Metallurgical and Materials Engineering*. 2025. Vol. 31, No. 3. P. 12–20. DOI: https://doi.org/10.63278/1315

3. Sharma S. AI-Powered Cybersecurity: The Future of Threat Detection. *International Journal of Scientific Research in Engineering and Management*. 2025. Vol. 09, No. 04. P. 1–9. DOI: https://doi.org/10.55041/ijsrem45943