

Горошко Юлія Андріївна,

здобувач ступеня вищої освіти магістра
навчально-наукового інституту права та
психології Національної академії
внутрішніх справ

Науковий керівник:

Шрамко С. С., завідувач кафедри
кримінального права та кримінології
навчально-наукового інституту права та
психології Національної академії
внутрішніх справ, кандидат юридичних
наук, старший дослідник

ВІКТИМОГЕННІ ФАКТОРИ У СФЕРІ КІБЕРБЕЗПЕКИ: ДОСЛІДЖЕННЯ КОРЕЛЯЦІЇ РІВНЯ ЦИФРОВОЇ ОБАЧНОСТІ

Прогресивна цифровізація економічних процесів, та становлення цифрової економіки є детермінантами якісної трансформації кримінальних діянь, що проявляється у формі шахрайства та набуває нових форм і модифікує способи свого вчинення [1, с. 22].

Під впливом цифрових технологій шахрайство набуло нових, високотехнологічних форм, а саме: фішингових атак, створення підроблених вебресурсів, використання шкідливого програмного забезпечення для викрадення фінансової інформації, підміни SIM-карт, генерації штучних голосів і зображень за допомогою технологій deepfake, а також автоматизованих схем обману через платформи електронної комерції, онлайн-банкінг [2].

Ключовими віктимогенними чинниками у сфері кібербезпеки є низький рівень цифрової грамотності, неусвідомлене поширення персональних даних, схильність до довірливої поведінки онлайн, відсутність навичок розпізнання фішингових атак, використання слабких або повторюваних паролів, а також недосконалості управлінських механізмів експлуатації та контролю за дотриманням протоколів кіберзахисту. Ці та інші детермінанти створюють сприятливе криміногенне середовище для успішних кібератак, що становить загрозу сталому функціонуванню об'єктів критичної інфраструктури та конфіденційності персональних даних фізичних осіб [3].

Зокрема, такий випадок трапився 12 грудня 2023 року, коли хакери атакували ядро мережі «Київстару». Тоді зловмисникам вдалося це зробити через злам акаунту одного з партнерів компанії внаслідок чого без зв'язку опинилися близько 24 млн абонентів. Атака на віртуальну інфраструктуру виявилась успішною, хакерам вдалося знищити 40 % інфраструктури, використовуючи стилер Mimikatz, який збирає інформацію на комп'ютері жертви та передає хакерам [4]. Подібні приклади ставалися і через через DDoS-атаки, завдані банківським установам, центральним органам державної влади, критичній інфраструктурі, офіційним ресурсам Міністерства оборони та Збройних Сил України [5].

Успішне протистояння кіберзагрозам вимагає комплексного регулювання, а саме впровадження програм з підвищення цифрової грамотності, що включатимуть курси кібергігієни для мінімізації віктимогенності користувачів, та запровадження систематичних тренінгів і симуляційних атак для забезпечення стійкості їхніх інформаційних систем [6].

Ще одним із аспектів кіберзагроз є інформаційна агресія, а саме вплив на громадську думку, що має тривалі наслідки. Пропаганда створює викривлене уявлення про реальність, маніпулює настроями у суспільстві. Через соціальні мережі та інші цифрові канали поширюються матеріали, спрямовані на розкол у суспільстві та розпалювання ворожнечі.

Слід зазначити, що на відміну від традиційних форм віктимізації, у цифровому середовищі ключову роль відіграє поведінковий компонент, тобто те, як особа здійснює власну «онлайн-навігацію», сприймає інформацію, та, наприклад, управляє своїми цифровими активами. У центрі цієї моделі стоїть цифрова обачність – особистісний ресурс, який визначає здатність до безпечної поведінки в Інтернеті. Така поведінка охоплює знання, навички, когнітивні фільтри та стратегії уникнення ризиків віктимізації. Отже, кореляція між цифровою обачністю та ймовірністю віктимізації проявляється у зворотній залежності: чим вищий рівень обачності, тим нижчий ризик потрапляння у шахрайські, маніпуляційні чи інші небезпечні ситуації в інтернет-просторі.

Таким чином, кібербезпека потребує, насамперед, комплексного державного підходу, глобальною метою якого є мінімізація ризиків як для окремих громадян, так і держави в

цілому. Зважаючи на те, що людський чинник у детермінації кіберзлочинів є домінуючим, то актуальним є формування культури інформаційної безпеки в суспільстві, яка включатиме навички безпечної поведінки у цифровому середовищі, критичне мислення та способи виокремлення потенційних загроз.

Список використаних джерел

1. Коновалова О. І. Запобігання шахрайству у сфері електронної торгівлі : дис. ... д-ра філософії. URL: https://dspace.nlu.edu.ua/bitstream/123456789/19894/1/Konovalova_dis.pdf (дата звернення: 07.11.2025).

2. Шахраї у 2025 році: 6 найпопулярніших схем, на які ведуться люди. URL: <https://www.rbc.ua/rus/news/shahrayi-2025-rotsi-6-naypopulyarnishih-shem-1755871833.html>

3. Свєрдлик З. Кібербезпека та кіберзахист: питання порядку денного в українському суспільстві. *Український журнал з бібліотекознавства та інформаційних наук*. 2022. № 10. С. 175–188.

4. Коваль О. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. URL: <https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/>.

5. Приват24, Ощадбанк, сайти Міноборони, ЗСУ, Українського радіо зазнали DDoS-атаки. URL: <https://suspilne.media/207368-privat24-ne-pracuvav-cerez-pereboi-zi-zvazkom-ci-bula-ddos-ataka-zasovuut-fahivci-pressluzba/>.

6. Державна служба спеціального зв'язку та захисту інформації України. Як протидіяти кіберзагрозам та захистити системи від ворожих кібератак – важливі рекомендації та допомога CERT-UA. URL: <https://www.kmu.gov.ua/news/yak-protydiaty-kiberzahrozam-ta-zakhystyty-systemy-vid-vorozhykh-kiberatak-vazhlyvi-rekomendatsii-ta-dopomoha-cert-ua>.