

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Навчально-науковий інститут права та психології
Кафедра інформаційних технологій



СУЧАСНІ ВИКЛИКИ У СФЕРІ КІБЕРБЕЗПЕКИ
ТА ШЛЯХИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Матеріали круглого столу
(м. Київ, 23 жовтня 2025 року)



Київ
2026

УДК 343.9:004.7 (477)
С916

Матеріали круглого столу за загальною редакцією:

Кудінов В.А. – кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ

Рецензенти:

Зверєв Володимир Павлович – заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки Апарату РНБО України, кандидат технічних наук, старший науковий співробітник

Хахановський Валерій Георгійович – професор кафедри інформаційних технологій навчально-наукового інституту права та психології Національної академії внутрішніх справ, доктор юридичних наук, професор

Матеріали схвалено та рекомендовано до друку на засіданні науково-методичної ради Національної академії внутрішніх справ (протокол № 12 від «19» грудня 2025 року)

Усі матеріали надані в авторській редакції та виражають персональну позицію учасників науково-практичного семінару

С916 Сучасні виклики у сфері кібербезпеки та шляхи протидії кіберзлочинності: матеріали круглого столу (м. Київ, НАВС, 23 жовтня 2025 р.); за заг. редакцією В. А. Кудінова. Київ: Нац. акад. внутр. справ, 2026. 56 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на круглий стіл на тему «Сучасні виклики у сфері кібербезпеки та шляхи протидії кіберзлочинності», який відбувся на базі навчально-наукового інституту права та психології Національної академії внутрішніх справ 23 жовтня 2025 року.

Для здобувачів вищої освіти, науково-педагогічних працівників закладів вищої освіти, практичних працівників органів та підрозділів системи МВС України.

УДК 343.9:004.7 (477)

© Національна академія внутрішніх справ, 2026

ЗМІСТ

Програма проведення круглого столу.....	4
Червинська К.О., Хахановський В.Г. Сучасні виклики в сфері кібербезпеки....	7
Клименко С.П., Хахановський В.Г. Кібербезпека та захист критичної інфраструктури в сучасних умовах.....	9
Стрельцова К.Ю., Хахановський В.Г. Кібербезпека бізнесу: від малого до великого.....	12
Левченко Д.О., Хахановський В.Г. Штучний інтелект в руках хакерів: нова ера кіберзагроз та виклики для України.....	15
Гусол О.Д., Хахановський В.Г. Сучасні виклики в сфері кібербезпеки.....	16
Горенчук Є.А., Хахановський В.Г. Основи цифрової гігієни для працівників правоохоронних органів.....	18
Федорова Л.Ф., Пакриш О.Є. Використання емоцій людини для вчинення кіберзлочинів.....	20
Слепко А.І., Пакриш О.Є. Вікові та гендерні відмінності в довірливості до онлайн-пропозицій як фактор ризику до кібершахрайства.....	23
Гуменюк В.О., Пакриш О.Є. Значення людського фактору у кібербезпеці.....	26
Yarotska A.S., Pakrysh O.Y. Psychological types of cybercriminals.....	29
Жицька В.О., Тарасенко В.П. Стан та шляхи підвищення рівня кібербезпеки в Україні.....	32
Савчин Є.А., Тарасенко В.П. Роль ІІІ у протидії кіберзлочинності.....	35
Богула С.Д., Тарасенко В.П. Психологічні наслідки кібершахрайства.....	39
Чистоклетова А.Д., Тарасенко В.П. Методи психологічного впливу у кіберзлочинності.....	41
Маленко А.О., Кудінов В.А. Протидія діпфейкам як сучасній формі кіберзагроз.....	44
Шуляк Б.А., Кудінов В.А. Вплив міжнародного досвіду та українських реалій на впровадження Концепції кіберстрахування баз даних в освітніх установах системи МВС України.....	47
Гончарова А.В., Кудінов В.А. Виклики для України у сфері кібербезпеки та основні підходи щодо запобігання кіберзлочинності.....	51
Шинкаренко А.Ю., Кудінов В.А. Основи кібергігієни в правоохоронній діяльності.....	53



**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
Навчально-науковий інститут права та психології
Кафедра інформаційних технологій**



ПРОГРАМА

проведення круглого столу на тему:

**«СУЧАСНІ ВИКЛИКИ У СФЕРІ КІБЕРБЕЗПЕКИ
ТА ШЛЯХИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ»**

(23 жовтня 2025 року)



Київ – 2025

Дата проведення: **23 жовтня 2025 року**

Початок роботи: **14.30**

Місце проведення: Національна академія внутрішніх справ (м. Київ, пл. Солом'янська 1, Цифровий Hub) та ZOOM.

Регламент: доповіді – до 5 хв.; обговорення – до 3 хв.

Відкриває захід директор ННІ права та психології НАВС, кандидат юридичних наук, доцент **Кульчицька Оксана Вікторівна**.

Вступне слово завідувача кафедри інформаційних технологій ННІ права та психології НАВС, кандидата фізико-математичних наук, доцента **Кудінова Вадима Анатолійовича**.

Модератори заходу:

- 1) професор кафедри інформаційних технологій ННІ права та психології НАВС, доктор юридичних наук, професор **Хахановський Валерій Георгійович**.
- 2) старший викладач кафедри інформаційних технологій ННІ права та психології НАВС **Вітязь Антон Анатолійович**.

ДОПОВІДІ:

1. Студентка 105СПД н.гр. **Червинська Ксенія Олегівна** «Сучасні виклики в сфері кібербезпеки» (д.ю.н. Хахановський В.Г.).
2. Студентка 105СПД н.гр. **Клименко Софія Павлівна** «Кібербезпека та захист критичної інфраструктури в сучасних умовах» (д.ю.н. Хахановський В.Г.).
3. Студентка 105СПД н.гр. **Стрельцова Кіра Юріївна** «Кібербезпека бізнесу: від малого до великого» (д.ю.н. Хахановський В.Г.).
4. Студент 105СПД н.гр. **Кульбако Артем Ігорович** «Штучний інтелект у кібербезпеці: нові горизонти захисту чи загроза майбутнього» (д.ю.н. Хахановський В.Г.).
5. Студентка 103СПД н.гр. **Левченко Дарина Олександрівна** «Штучний інтелект в руках хакерів: нова ера кіберзагроз та виклики для України» (д.ю.н. Хахановський В.Г.).
6. Студентка 104СПД н.гр. **Ткаченко Карина Станіславівна** «Кібербезпека в часи війни: досвід України» (д.ю.н. Хахановський В.Г.).
7. Студент 104СПД н.гр. **Гусол Олексій Дмитрович** «Сучасні виклики в сфері кібербезпеки» (д.ю.н. Хахановський В.Г.).
8. Студентка 103СПД н.гр. **Горенчук Євгенія Андріївна** «Основи цифрової гігієни для працівників правоохоронних органів» (д.ю.н. Хахановський В.Г.).
9. Студентка 202СПС н.гр. **Федорова Людмила Федорівна** «Використання емоцій людини для вчинення кіберзлочинів» (к.т.н. Пакриш О.Є.).

10. Студентка 202СПС н.гр. **Слепко Ангеліна Іванівна** «Вікові та гендерні відмінності в довірливості до онлайн-пропозицій як фактор ризику до кібершахрайства» (к.т.н. Пакриш О.Є.).
11. Студентка 202СПС н.гр. **Гуменюк Вікторія Олегівна** «Значення людського фактору у кібербезпеці» (к.т.н. Пакриш О.Є.).
12. Student of academic group 301_SPS **Yarotska Anastasiia Stanislavivna** «Psychological types of cybercriminals» (с.т.с. Pakrysh O.Y.).
13. Студентка 117СПД н.гр. **Жицька Валерія Олегівна** «Стан та шляхи підвищення рівня кібербезпеки в Україні» (к.ф.-м.н. Тарасенко В.П.).
14. Студентка 117СПД н.гр. **Савчин Євгенія Андріївна** «Роль ШІ у протидії кіберзлочинності» (к.ф.-м.н. Тарасенко В.П.).
15. Студентка 302СПС н.гр. **Богула Софія Дмитрівна** «Психологічні наслідки кібершахрайства» (к.ф.-м.н. Тарасенко В.П.).
16. Студентка 302СПС н.гр. **Чистоклетова Анна Денисівна** «Методи психологічного впливу у кіберзлочинності» (к.ф.-м.н. Тарасенко В.П.).
17. Студент 2 н.гр. 4-КВ курсу ІЗДН **Маленко Андрій Олександрович** «Протидія діпфейкам як сучасній формі кіберзагроз» (к.ф.-м.н. Кудінов В.А.).
18. Студент н.гр. 102СПД **Шуляк Богдан Андрійович** «Вплив міжнародного досвіду та українських реалій на впровадження Концепції кіберстрахування баз даних в освітніх установах системи МВС України» (к.ф.-м.н. Кудінов В.А.).
19. Студентка н.гр. 101СПД **Гончарова Анастасія Володимирівна** «Виклики для України у сфері кібербезпеки та основні підходи щодо запобігання кіберзлочинності» (к.ф.-м.н. Кудінов В.А.).
20. Студентка н.гр. 101СПД **Шинкаренко Ангеліна Юріївна** «Основи кібергігієни в правоохоронній діяльності» (к.ф.-м.н. Кудінов В.А.).

Червинська Ксенія Олегівна

Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:

Хахановський Валерій Георгійович

доктор юридичних наук, професор,
професор кафедри інформаційних
технологій ННІ права та психології
НАВС

СУЧАСНІ ВИКЛИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

Кіберпростір сьогодні – це середовище, де взаємодіють мільярди пристроїв, а обсяги інформації подвоюються щороку. Разом з цим зростає і кількість кіберзагроз. Якщо на початку 2000-х більшість атак мали аматорський характер, то сьогодні вони організовуються цілими хакерськими угрупованнями, фінансуються державами чи кримінальними синдикатами. Це робить кібербезпеку глобальним викликом ХХІ століття.

Кібербезпека – це система організаційних, технічних і правових заходів, спрямованих на захист інформаційних систем від несанкціонованого доступу, знищення, блокування чи викривлення даних.

Значення кібербезпеки зростає через: 1) цифровізацію державного управління (електронні сервіси, «Дія», електронні документи); 2) онлайн-банкінг і фінансові операції, де витік інформації може призвести до мільйонних збитків; 3) зростання кількості електронних пристроїв (смартфони, «розумні» годинники, IoT-пристрої); 4) кібервійни, що стають елементом міжнародних конфліктів.

Кіберпростір перетворився на арену геополітичної боротьби. Хакерські атаки можуть паралізувати роботу електростанцій, транспортних мереж чи банківських систем. Прикладом є масові атаки на Україну в 2015–2017 роках, що призводили до відключення електроенергії та блокування державних ресурсів.

Кібершпигунство дозволяє державам та корпораціям отримувати конфіденційні дані конкурентів, впливати на політику інших країн та здійснювати маніпуляції в інформаційному просторі.

Кіберзлочини проти приватних осіб. Найбільш поширені форми:

- фішинг – виманювання особистих даних через підроблені сайти та повідомлення;
- віруси та шкідливе програмне забезпечення, які блокують роботу комп'ютерів чи викрадають інформацію;
- шантаж (ransomware) – блокування пристрою з вимогою викупу;
- крадіжка даних банківських карток (завдає мільярдні збитки щороку).

Виклики інтернету речей. Мільярди «розумних» пристроїв (камери, датчики, побутова техніка) часто не мають достатнього захисту. Хакери можуть використати їх як «точку входу» для масштабних атак. Наприклад, заражені «розумні» телевізори чи маршрутизатори об'єднують у «ботнети», які паралізують роботу великих сайтів.

Соціальна інженерія. Сучасні атаки дедалі частіше спрямовані не на комп'ютери, а на людей. Хакери створюють психологічні маніпуляції: дзвінки від «працівників банку», підроблені електронні листи, повідомлення від «знайомих» у соцмережах. Людина сама передає зловмиснику потрібну інформацію.

Штучний інтелект як виклик і можливість. З одного боку, AI дозволяє швидше виявляти аномалії та підозрілі дії. З іншого – зловмисники застосовують його для створення реалістичних фейкових відео, автоматизації атак чи масового фішингу.

Дефіцит кваліфікованих кадрів. За даними міжнародних організацій, у світі не вистачає понад 3 мільйонів фахівців із кіберзахисту. Це означає, що навіть великі компанії залишаються без належного рівня безпеки.

Шляхи протидії кіберзагрозам:

1. *Розвиток національних стратегій кібербезпеки.* Україна вже ухвалила відповідні документи, але їх необхідно постійно оновлювати відповідно до нових викликів.

2. *Використання сучасних технологій.* Багаторівнева аутентифікація, шифрування, системи виявлення вторгнень, аналіз великих даних.

3. *Міжнародне співробітництво.* Кіберзагрози не мають кордонів, тому боротьба з ними вимагає спільних дій. Приклад – Будапештська конвенція про кіберзлочинність.

4. *Освіта та підготовка кадрів.* Важливо створювати програми навчання з кіберзахисту в школах і закладах вищої освіти.

5. *Цифрова грамотність населення.* Користувачі мають знати основи безпеки: не відкривати підозрілі листи, не повідомляти паролі, перевіряти сайти.

Отже, кібербезпека стала однією з найважливіших сфер у житті сучасного суспільства. Від неї залежить стабільність економіки, національна безпека, особиста безпека кожної людини.

Сучасні виклики – кібервійни, кіберзлочинність, розвиток інтернету речей, використання штучного інтелекту – потребують комплексної відповіді. Подолати їх можливо лише за умови поєднання новітніх технологій, ефективного законодавства, міжнародної співпраці та підвищення цифрової культури суспільства.

На мою думку, кібербезпека – це не лише завдання держави чи ІТ-компаній, а спільна справа кожного громадянина, адже найчастіше саме людський фактор є ключовим у питаннях захисту інформації.

Клименко Софія Павлівна

Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:

Хахановський Валерій Георгійович

доктор юридичних наук, професор,
професор кафедри інформаційних
технологій ННІ права та психології
НАВС

КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В СУЧАСНИХ УМОВАХ

Сучасний світ дедалі більше залежить від цифрових технологій: нині всі працюють, навчаються, спілкуються та навіть зберігають власні гроші в електронному просторі. Разом із новими можливостями зростає й кількість ризиків, пов'язаних із кіберпростором. Кібератаки вже не є лише технічною проблемою – вони перетворилися на глобальний виклик, що впливає на економіку, політику та національну безпеку. Саме тому дослідження проблем кібербезпеки набуває особливого значення у ХХІ столітті.

Загальні тенденції впровадження цифрових технологій:

- цифровізація суспільства призводить до збільшення кількості пристроїв, що підключені до мережі, а отже – й точок потенційної атаки;
- зростання обсягів персональних даних робить користувачів більш вразливими до крадіжок інформації;
- гібридні війни активно використовують кіберінструменти як засіб впливу на супротивника.

Основними сучасними викликами кібербезпеки є:

1. Кіберзлочинність (хакерські атаки на банківські системи, крадіжка коштів і даних; використання шкідливого програмного забезпечення (вірусів, троянів, програм-вимагачів)).
2. Кібертероризм і кібервійни (атаки на критичну інфраструктуру: енергетичні системи, транспорт, медицину; використання кіберзасобів у збройних конфліктах, як це спостерігається нині під час агресії проти України).
3. Соціальна інженерія (фішинг; маніпуляції довірою користувачів, щоб отримати доступ до конфіденційної інформації).
4. Загрози для приватності (масове збирання й використання персональних даних великими корпораціями; проблеми захисту інформації у соціальних мережах).

5. Штучний інтелект та нові технології – з одного боку вони допомагають захищати дані, з іншого – створюють нові ризики (наприклад, deepfake, автоматизовані атаки).

В умовах війни Україна постійно зазнає масштабних кібератак з боку росії, метою яких є паралізація роботи державних органів, дезінформація, створення паніки серед населення. Це доводить, що кіберпростір став окремим фронтом сучасної війни.

Основні тренди кібербезпеки у 2025 році:

1. Штучний інтелект у захисті (використання AI для виявлення та блокування загроз у реальному часі; прогнозування потенційних атак за допомогою аналітики даних).

2. Мережна сегментація (розділення мережі на сегменти для мінімізації ризику поширення загроз; підвищення контролю над доступом до критичних систем).

3. Багатофакторна аутентифікація (активне впровадження додаткових рівнів безпеки; захист доступу до корпоративних систем і особистих даних).

4. Кібербезпека в хмарних середовищах (посилення захисту даних у хмарних платформах; використання спеціалізованих інструментів для моніторингу та захисту).

5. Навчання співробітників (підвищення рівня обізнаності працівників про сучасні загрози; регулярні тренінги для зменшення ризику людського фактору).

Сьогодні більшість речей навколо нас працює завдяки складним системам (електростанції, лікарні, транспорт, банки, водопостачання, зв'язок та Інтернет тощо). Усі ці об'єкти утворюють так звану критичну інфраструктуру. Якщо хоча б одна з цих систем перестане працювати, це може спричинити значні проблеми: зупиниться транспорт, зникне електроенергія, не буде доступу до грошей, може постраждати здоров'я людей. Через це питання захисту критичної інфраструктури стає одним із найважливіших у сучасному світі. З розвитком технологій з'являються і нові небезпеки: хакери можуть зламати комп'ютерні мережі, правопорушники – пошкодити обладнання, стихійні лиха – знищити важливі об'єкти. Завдання держави, бізнесу та суспільства – не допустити таких ситуацій або швидко реагувати, якщо вони трапляються.

Критична інфраструктура – це найважливіші системи та об'єкти, без яких не може нормально існувати суспільство й держава. Вона забезпечує життя людей, роботу економіки та безпеку країни. До неї належать:

- Енергетика – електростанції, газо- та нафтопроводи, теплопостачання.
- Транспорт – залізниці, метро, морські порти, авіаційні системи.
- Зв'язок і Інтернет – мобільні мережі, супутникові системи, пошта.
- Охорона здоров'я – лікарні, лабораторії, системи швидкої допомоги.
- Фінанси – банки, банкомати, системи оплати.
- Безпека держави – військові об'єкти, поліція тощо.

Якщо одна з цих сфер буде пошкоджена або знищена, це може спричинити серйозні наслідки для життя всієї країни.

Загроз для об'єктів критичної інфраструктури багато. Найпоширеніші з них:

- Кібератаки. Злочинці можуть зламати комп'ютерні мережі та паралізувати роботу електростанцій, банків чи транспорту.
- Фізичні напади. Терористи або зловмисники можуть пошкодити об'єкти інфраструктури.
- Технічні аварії. Іноді системи виходять з ладу через несправність або людську помилку.
- Природні катастрофи. Повені, землетруси, пожежі можуть знищити важливі об'єкти.
- Військові дії. Під час війни такі об'єкти стають однією з головних цілей ворога.

Відомі приклади атак на критичну інфраструктуру:

- ✓ Україна, 2015 рік. Кібератака на енергетичну систему призвела до відключення електроенергії в кількох регіонах країни.
- ✓ США, 2021 рік. Злочинці зламали систему нафтопроводу «Colonial Pipeline», через що постачання палива на східному узбережжі було зупинене на кілька днів.
- ✓ Україна, 2022 рік. Під час війни росія неодноразово атакувала енергетичні підприємства та Інтернет-мережі, намагаючись порушити роботу критичних систем.

Ці приклади доводять, що загроза реальна і може торкнутися кожної людини.

Захист таких об'єктів складається з багатьох заходів:

- Постійний нагляд і моніторинг. Фахівці відстежують роботу систем, щоб одразу помітити небезпеку.
- Резервні системи. Створюються запасні джерела енергії, копії даних та інші механізми на випадок аварій.
- Навчання персоналу. Людей навчають діяти в кризових ситуаціях та правильно реагувати на загрози.
- Законодавчий захист. Приймаються закони, які визначають правила безпеки та покарання за злочини проти критичних об'єктів.
- Міжнародна співпраця. Держави обмінюються досвідом і допомагають одна одній захищати важливі системи.

В Україні для цього діє Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони. Він координує роботу державних органів, приватних компаній і міжнародних партнерів.

Отже, критична інфраструктура – це серце сучасної держави. Без електрики, води, транспорту, зв'язку та лікарень життя людей зупинилося б. Тому її захист – це не просто технічне питання, а гарантія безпеки кожного громадянина.

Список використаних джерел:

1. Міністерство цифрової трансформації України. Офіційний сайт. – <https://thedigital.gov.ua>
2. Кіберполіція України. Аналітичні матеріали та новини. – <https://cyberpolice.gov.ua>
3. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Reports. – <https://ccdcoe.org>
4. Symantec. Internet Security Threat Report. – <https://symantec.com>
5. FireEye Mandiant. Cyber Security Reports. – <https://www.mandiant.com>
6. CERT-UA (Computer Emergency Response Team of Ukraine). Офіційні публікації. – <https://cert.gov.ua>
7. Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.).
8. Офіційний сайт Ради національної безпеки і оборони України – www.rnbo.gov.ua.
9. ENISA. Reports on Critical Infrastructure Protection.
10. Symantec. Internet Security Threat Report.
11. Zetter K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. – 2014.

Стрельцова Кіра Юріївна

Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:

Хахановський Валерій Георгійович

доктор юридичних наук, професор,
професор кафедри інформаційних
технологій ННІ права та психології
НАВС

КІБЕРБЕЗПЕКА БІЗНЕСУ: ВІД МАЛОГО ДО ВЕЛИКОГО

Сьогодні кібербезпека стала однією з ключових умов стабільності бізнесу незалежно від його масштабу. Малі, середні та великі підприємства дедалі частіше стають мішенню кіберзлочинців, адже дані, ресурси та фінансові активи є об'єктом особливої цінності.

Мета даної роботи – розглянути виклики та підходи до забезпечення кібербезпеки бізнесу на різних рівнях його розвитку.

Під *кібербезпекою* розуміють комплекс заходів, спрямованих на захист інформаційних систем, мереж, даних і цифрових активів від несанкціонованого доступу, кібератак, витоку інформації та інших загроз. Для бізнесу кібербезпека має стратегічне значення, адже інциденти у сфері безпеки можуть призвести до фінансових збитків, втрати репутації, а також до юридичної відповідальності.

Серед найбільш поширених кіберзагроз для підприємств є:

- фішингові атаки та соціальна інженерія;
- віруси, шпигунське програмне забезпечення та програми-вимагачі;
- несанкціонований доступ до корпоративних даних;
- витік конфіденційної інформації через внутрішні помилки співробітників;
- DDoS-атаки, що паралізують діяльність компаній.

Кожна з цих загроз може завдати бізнесу значних збитків, особливо якщо не існує плану реагування.

Малі підприємства зазвичай мають обмежені ресурси, тому кібербезпека часто недооцінюється. Проте саме вони стають легкою мішенню для хакерів.

Основні кроки для захисту малого бізнесу:

- впровадження базових правил кібергігієни (складні паролі, двофакторна автентифікація);
- регулярне оновлення програмного забезпечення;
- навчання персоналу основам інформаційної безпеки;
- використання хмарних сервісів із вбудованим захистом даних.

Середні компанії володіють більшими інформаційними потоками та клієнтськими базами. Для них особливо важливим є:

- розробка політик безпеки та внутрішніх регламентів;
- впровадження систем моніторингу та виявлення інцидентів;
- сегментація корпоративної мережі;
- створення резервних копій і планів відновлення даних.

Завдяки системному підходу середній бізнес може не лише захистити свої активи, а й підвищити довіру клієнтів.

Великі корпорації часто стають мішенню цілеспрямованих атак, спрямованих на фінансову вигоду чи промислове шпигунство.

Тут необхідні комплексні рішення, а саме:

- створення окремих відділів кібербезпеки;
- використання інноваційних технологій (штучний інтелект для виявлення аномалій);
- постійні аудити та тестування на проникнення;
- співпраця з державними структурами та міжнародними організаціями.

У країнах ЄС та США кібербезпека бізнесу регламентується законодавством, що передбачає сувору відповідальність за витік персональних даних.

Прикладом цього є Загальний регламент із захисту даних (GDPR), який зобов'язує компанії дотримуватися високих стандартів безпеки.

Для України важливим є гармонізація власних законодавчих норм із міжнародними стандартами.

Майбутнє кібербезпеки тісно пов'язане з розвитком новітніх технологій:

- використання штучного інтелекту та машинного навчання;
- впровадження блокчейн-технологій для безпечних транзакцій;
- підвищення ролі кіберосвіти серед працівників;
- створення культури безпеки як невід'ємної частини бізнес-процесів.

Отже, кібербезпека є невід'ємним елементом сучасного бізнесу незалежно від його масштабів. Малі компанії повинні приділяти увагу базовим заходам захисту, середні – впроваджувати системні підходи, а великі корпорації – інвестувати у комплексні рішення та міжнародну співпрацю.

Тільки так, на наш погляд, можна зменшити ризики та забезпечити стійкість бізнесу у цифрову епоху.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
2. Загальний регламент захисту даних (General Data Protection Regulation, GDPR). Regulation (EU) 2016/679.
3. National Institute of Standards and Technology (NIST). Cybersecurity Framework. U.S. Department of Commerce, 2020.
4. International Telecommunication Union. Global Cybersecurity Index 2021.
5. Symantec. Internet Security Threat Report. Vol. 24, 2022.
6. ENISA (European Union Agency for Cybersecurity). Cybersecurity Threat Landscape 2023.
7. Кудінов, С. С. Кібербезпека в умовах цифровізації бізнесу: виклики та рішення // Науковий вісник ХНУВС, 2022. С. 34-37.
8. Гаврилюк, О. П. Інформаційна безпека підприємств: проблеми та шляхи їх вирішення // Економіка і суспільство, 2021.
9. PwC. Global Digital Trust Insights 2024: Cybersecurity trends.
10. Cisco. Cybersecurity Annual Report 2023.

Левченко Дарина Олександрівна
Студентка н.гр. 103_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор,
професор кафедри інформаційних технологій ННІ права та психології НАВС

ШТУЧНИЙ ІНТЕЛЕКТ В РУКАХ ХАКЕРІВ: НОВА ЕРА КІБЕРЗАГРОЗ ТА ВИКЛИКИ ДЛЯ УКРАЇНИ

Поширення інструментів ШІ кардинально змінює ландшафт кіберзагроз: автоматизація збору даних, генерація персоналізованих фішингових атак, створення deepfake-контенту та автоматизоване сканування вразливостей підвищують ефективність і масштабність атак при значному зниженні порога входу для зловмисників. Це створює нову ітерацію загроз для національної безпеки, особливо в умовах гібридної агресії проти України, де кібероперації вже використовуються як складова гібридного тиску.

Як саме хакери використовують ШІ (тактики й приклади):

- Автоматизація фішингу та соціальної інженерії.
- Deepfake та клонування голосу.
- Автомотогенерація шкідливого коду.
- Аналіз великих масивів даних для вибору мішеней.

Наслідки для України.

Українська критична інфраструктура залишається в зоні підвищеного ризику. Поєднання традиційних тактик і нових можливостей ШІ здатне підвищити як частоту, так і складність атак на промислові системи управління. CERT-UA та Держспецзв'язку фіксують збільшення інцидентів соціальної інженерії, де елементи ШІ пришвидшують виробництво контенту.

Проблеми адаптації:

- технічні бар'єри: відсутність сучасних систем виявлення аномалій;
- кадрові проблеми: дефіцит фахівців зі знанням ШІ;
- правове регулювання: недостатня нормативна база щодо ШІ.

Рекомендації:

- розробка національної стратегії «ШІ-безпека»;
- інтеграція ШІ у засоби захисту;
- захист від deepfake і верифікація каналів;
- розширення освітніх програм;

- публічно-приватна платформа обміну даними;
- законодавче оновлення стандартів.

Висновки. ШІ змінює правила гри у кіберпросторі: атаки стають більш масштабними, персоналізованими й дешевими. Україна має створити комплексну політику, яка поєднує технічні рішення, кадрову підготовку, нормативну базу та етичні стандарти. Круглий стіл може стати платформою для вироблення дорожньої карти впровадження таких змін.

Список використаних джерел:

1. CERT-UA – Офіційний сайт Національної команди реагування на кіберінциденти. <https://cert.gov.ua/>
2. РНБО України. Річний аналітичний огляд кіберзагроз, 2024–2025.
3. Vavryk Y., Opirskyu I. Штучний інтелект: кібербезпека нового покоління. *Ukrainian Scientific Journal of Information Security*, 2024.
4. Сироватченко М. Правові аспекти забезпечення кібербезпеки в Україні, 2024.
5. Аналітичні матеріали Київстар Hub – «Тренди кібербезпеки на 2025 рік».

Гусол Олексій Дмитрович

Студент н.гр. 104_СПД ННІ права та психології НАВС

Науковий керівник:

Хахановський Валерій Георгійович

доктор юридичних наук, професор,
професор кафедри інформаційних
технологій ННІ права та психології
НАВС

СУЧАСНІ ВИКЛИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

У сучасному світі інформаційні технології стали невід’ємною частиною економіки, політики, освіти та безпеки. Водночас активна цифровізація створює передумови для виникнення нових загроз у сфері кібербезпеки. Під кібербезпекою розуміють стан захищеності кіберпростору, при якому забезпечується цілісність, конфіденційність і доступність інформації. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», держава зобов’язана створювати систему захисту критичної інфраструктури та інформаційних ресурсів від кібератак. Одним із головних викликів сьогодення є зростання кількості цілеспрямованих атак на державні установи та правоохоронні органи.

Використання штучного інтелекту у злочинних цілях – це нова тенденція, яка ускладнює виявлення та запобігання кіберзлочинам. Атаки стають дедалі складнішими: кіберзлочинці використовують фішингові кампанії, шкідливе програмне забезпечення, методи соціальної інженерії. Особливої уваги потребує захист персональних даних громадян та державних реєстрів, оскільки їх витік може мати масштабні наслідки.

Важливу роль у протидії кіберзагрозам відіграє міжнародне співробітництво. Україна є учасником Будапештської конвенції про кіберзлочинність, що встановлює стандарти міжнародного обміну інформацією та спільного реагування на кібератаки. Крім того, розвиток кіберосвіти та підготовка кваліфікованих фахівців у сфері безпеки мають стати стратегічним напрямом державної політики.

Отже, сучасні виклики у сфері кібербезпеки вимагають системного підходу — поєднання технологічних, правових та освітніх заходів, спрямованих на захист державних і приватних ресурсів у кіберпросторі.

Розвиток сучасних технологій докорінно змінює функціонування правової системи, роботу правоохоронних органів і навіть психологічні підходи до вивчення поведінки людини. Використання штучного інтелекту, великих даних, відеоаналітики та цифрових платформ дозволяє підвищити ефективність правозастосовної діяльності, проте породжує нові правові та етичні дилеми.

У сфері права технології забезпечують автоматизацію процесів, зокрема електронне судочинство, електронні докази та використання блокчейн-систем для зберігання юридично значущих даних. Проте надмірна цифровізація створює ризики для конфіденційності особистої інформації. Використання алгоритмів прийняття рішень може призводити до помилкових або упереджених висновків, що ставить під сумнів принцип справедливості.

Правоохоронна діяльність сьогодні активно інтегрує технології відеоспостереження, біометрії та штучного інтелекту. Це сприяє ефективнішому розслідуванню злочинів, однак водночас вимагає чіткого правового регулювання збору, зберігання та використання персональних даних. Українське законодавство поступово адаптується до цих змін, спираючись на положення Закону «Про захист персональних даних» та міжнародні стандарти, такі як Загальний регламент ЄС із захисту даних (GDPR).

У психологічній практиці технології використовуються для аналізу емоційного стану, прогнозування поведінки та оцінки психічного здоров'я. Проте постає питання етичності таких методів, адже втручання в психіку людини через алгоритми або нейромережі може порушувати її право на приватність та самовираження.

Отже, впровадження сучасних технологій у право, правоохоронну діяльність і психологію потребує комплексного балансу між ефективністю, етикою та захистом прав людини. Це ключова умова розвитку безпечного цифрового суспільства в Україні.

Горенчук Євгенія Андріївна

Студентка н.гр. 103_СПД ННІ права та психології НАВС

Науковий керівник:

Хахановський Валерій Георгійович

доктор юридичних наук, професор,
професор кафедри інформаційних
технологій ННІ права та психології
НАВС

ОСНОВИ ЦИФРОВОЇ ГІГІЄНИ ДЛЯ ПРАЦІВНИКІВ ПРАВООХОРОННИХ ОРГАНІВ

Сучасний світ неможливо уявити без інформаційних технологій. Працівники правоохоронних органів щодня використовують комп'ютери, мобільні пристрої, інформаційні бази даних і мережеві ресурси. У цих умовах питання цифрової гігієни – грамотного, безпечного та відповідального користування цифровими засобами, набуває особливої ваги.

Недотримання базових правил інформаційної безпеки може призвести до витоку службової інформації, зламу електронної пошти чи службових акаунтів, підробки документів або навіть кібератак на державні системи. Саме тому тематика цифрової гігієни є надзвичайно актуальною для підготовки майбутніх фахівців у сфері правоохоронної діяльності.

У сучасному світі розвиток інформаційних технологій суттєво впливає на діяльність правоохоронних органів. Більшість службових завдань пов'язана з використанням комп'ютерних систем, баз даних, електронного документообігу та мережевої взаємодії. У таких умовах важливого значення набуває поняття цифрової гігієни – сукупності правил, що забезпечують безпечне, відповідальне та ефективне користування інформаційними технологіями.

Цифрова гігієна – це система знань, навичок і звичок, спрямованих на захист користувача від кіберзагроз, витоку інформації та технічних збоїв.

Для працівників правоохоронних органів вона має особливе значення, оскільки недотримання базових правил може призвести до втрати службової інформації або порушення державної таємниці.

Основними принципами цифрової гігієни є:

1. Використання складних паролів та багатофакторної автентифікації.
2. Регулярне оновлення програмного забезпечення.
3. Заборона відкриття підозрілих електронних листів і посилань.
4. Використання офіційних джерел під час завантаження програм.
5. Захист персональних та службових даних від стороннього доступу.

6. Контроль конфіденційності у соціальних мережах.

Загрози у сфері цифрової безпеки правоохоронців.

Працівники правоохоронних органів часто стають мішенню кіберзлочинців, які намагаються отримати доступ до внутрішніх баз даних або персональних акаунтів. Найпоширеніші загрози: фішинг, шкідливе програмне забезпечення, злами месенджерів, соціальна інженерія. Важливо вміти розпізнавати ознаки кібератак і своєчасно повідомляти відповідні правоохоронні органи про підозрілі інциденти.

Правові аспекти цифрової гігієни.

В Україні питання кібербезпеки регулюються Законом України «Про основні засади забезпечення кібербезпеки» [1] та Законом України «Про захист персональних даних» [2]. Працівники правоохоронних органів зобов'язані дотримуватись вимог цих законів, не допускаючи розголошення службової або конфіденційної інформації у цифровому середовищі.

Отже, цифрова гігієна є невід'ємною частиною професійної культури правоохоронця. Вона сприяє збереженню особистої та службової інформації, підвищує рівень довіри громадян до поліції й державних інституцій загалом. Формування навичок цифрової грамотності – це запорука ефективної роботи в умовах сучасних кіберзагроз.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 403.
2. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

Федорова Людмила Федорівна
Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:

Пакриш Олександр Євгенійович
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій ННІ права та психології НАВС

ВИКОРИСТАННЯ ЕМОЦІЙ ЛЮДИНИ ДЛЯ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

У сучасному цифровому світі кіберзлочини стають дедалі витонченішими. Якщо раніше злочинці здебільшого використовували технічні методи злому систем, то сьогодні вони дедалі частіше звертаються до психологічних методів впливу на людину. Найефективнішим серед них є використання емоцій. Людські почуття – страх, довіра, співчуття, жадібність, цікавість – стають знаряддям злочину, яке дозволяє обійти навіть найсучасніші системи безпеки. Цей феномен отримав назву *соціальна інженерія* – це використання психологічних прийомів для маніпулювання людьми з метою отримання конфіденційної інформації або доступу до систем. Кіберзлочинці розуміють: у стані сильних емоцій люди частіше діють імпульсивно і рідше аналізують ситуацію. Вони не зважають на логіку чи перевірку фактів, а керуються почуттями. Тому злочинці створюють ситуації, що викликають емоційну напругу або, навпаки, приємне очікування вигоди. Основні емоції, які експлуатують злочинці:

1. *Страх і паніка.* Найпоширеніша емоція, яку використовують для тиску.

Приклад: користувач отримує лист із нібито офіційного джерела – наприклад, «Ваш банківський рахунок буде заблоковано через підозрілу активність! Потрібно терміново підтвердити Вашу особу за посиланням!». Злякавшись, людина натискає на посилання і вводить свої дані – логін, пароль, номер картки. Так злочинці отримують доступ до її коштів. У цьому випадку страх паралізує критичне мислення: людина діє миттєво, щоб «уникнути небезпеки».

2. *Співчуття і бажання допомогти.* Маніпуляції часто побудовані на людяності.

Приклад: зловмисник створює фейкову сторінку у соцмережі й поширює пости на кшталт: «Дитині терміново потрібна операція, допоможіть хто чим може». Люди, керуючись співчуттям, переказують гроші на картку, навіть не перевіряючи достовірність інформації. Подібні «емоційні пастки» особливо поширені у часи воєн, катастроф, коли емоційна напруга в суспільстві висока.

3. Жадібність і бажання швидкого прибутку. Емоція вигоди часто приглушує обережність.

Приклад: користувач отримує повідомлення: «Ви стали переможцем лотереї Google! Для отримання призу введіть свої дані». Або ж – «Інвестуйте 1000 грн сьогодні й заробіть 10000 за тиждень». Очікування легкої вигоди змушує людину ігнорувати підозри.

4. Бажання дізнатися щось «таємне» або «сенсаційне» – ще один гачок.

Приклад: людині надсилають повідомлення: «Подивись, що про тебе написали!» або «Шокуюче відео твого знайомого». Відкриваючи посилання, користувач активує вірус або надає доступ до свого акаунта.

5. Почуття авторитету і довіри. Злочинці часто видають себе за представників офіційних структур, банків, керівників або навіть знайомих.

Приклад: співробітник отримує лист нібито від директора компанії: «Терміново надішліть мені звіт і паролі до системи». Прагнучи виконати наказ керівництва, працівник не перевіряє справжність відправника.

Дослідження показують, що люди більш схильні піддаватися емоційним маніпуляціям у стані:

- втоми, коли увага розсіяна;
- стресу, коли знижується раціональне мислення;
- багатозадачності, коли одночасно потрібно вирішувати кілька питань;
- коли людина має низький рівень цифрової грамотності.

Крім того, деякі особистісні риси – наприклад, довірливість, відкритість, співчутливість – також підвищують ризик потрапити на гачок кіберзлочинців.

Приклади реальних випадків дії психологічних чинників вразливості:

1. “Love Scam” (романтичні шахрайства): злочинці знайомляться в соцмережах, вибудовують довіру, а потім просять гроші на «лікування», «переїзд» чи «візу». Жертви часто втрачають великі суми, бо керуються емоцією кохання та довіри.

2. “Фішинг” від імені банку: під час пандемії COVID-19 тисячі людей отримали листи про нібито фінансову допомогу від банків. Натиснувши на фальшиве посилання, вони передавали свої дані шахраям.

3. Соціальні мережі: зловмисники використовують фейкові сторінки відомих благодійних фондів, які викликають довіру, і збирають пожертви для власної вигоди.

Наслідки таких злочинів можуть бути дуже серйозними:

- Фінансові втрати – від кількох сотень до мільйонів гривень.
- Витік персональних даних – доступ до паролів, фото, листування.
- Емоційна травма жертви – почуття провини, сором, недовіра до оточення.
- Репутаційні збитки – особливо для організацій і компаній.

Шляхи захисту від кіберзлочинів:

1. *Розвивати емоційну обізнаність.* Якщо повідомлення викликає сильну емоцію – страх, злість, азарт чи співчуття – це сигнал бути обережним.
2. *Зробити паузу.* Не приймати жодних рішень одразу, особливо якщо вас підганяють словами «терміново».
3. *Перевіряти джерело інформації.* Телефонувати або писати офіційним контактам замість натискання на сумнівні посилання.
4. *Підвищувати цифрову грамотність.* Знання про фішинг, шкідливі сайти, конфіденційність допомагають уникнути маніпуляцій.
5. *Психологічна стійкість.* Людина, яка розуміє власні емоційні реакції, рідше стає жертвою маніпуляцій.

Висновки. Використання емоцій у кіберзлочинності – це приклад того, як психологія може стати зброєю в руках маніпулятора. Емоції – це природна і важлива частина людського життя, але саме вони можуть зробити нас вразливими.

Знання власних реакцій, розвиток критичного мислення і цифрової культури – це головні засоби захисту у світі, де замість фізичних грабіжників з'явилися емоційні хакери.

Список використаних джерел:

1. Schmitt, Marc, and Ivan Flechais. 2024. *Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing*. Artificial Intelligence Review 57: Article 324. <https://doi.org/10.1007/s10462-024-10973-2>.
2. Europol. 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. The Hague: Europol. PDF. <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>.
3. National Cyber Security Centre (NCSC). 2024. *NCSC Annual Review 2024*. London: NCSC. PDF. https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf.
4. Sandoval, María Paz, Maria de Almeida Vau, John Solaas, and Luano Rodrigues. 2024. "Threat of Deepfakes to the Criminal Justice System: A Systematic Review." *Crime Science* 13 (1): 41. <https://doi.org/10.1186/s40163-024-00239-1>.
5. Wiemken, Mika, Kilian Hildebrandt, André Jeworutzki, and Larissa Putzar. 2025. "Emotional Manipulation in Phishing Emails: Experimental Study of Affective Responses and Human Classification Errors in a Simulated Email Environment." Proceedings / Publication record (ACM / conference paper; Hamburg University of Applied Sciences). DOI/ACM record: <https://doi.org/10.1145/3733155.3736796>
6. Wu, Jie. 2024. "Social and Ethical Impact of Emotional AI Advancement: The Rise of Pseudo-Intimacy Relationships and Challenges in Human Interactions." *Frontiers in Psychology* 15:1410462. <https://doi.org/10.3389/fpsyg.2024.1410462>.
7. Balcombe, Luke. 2025. "The Mental Health Impacts of Internet Scams." *International Journal of Environmental Research and Public Health* 22, no. 6: 938. <https://doi.org/10.3390/ijerph22060938>.

8. Espinoza, Michelle. 2024. *Weaponization of Conscience in Cybercrime and Online Fraud: A Novel Systems Theory*. arXiv preprint arXiv:2403.14667. <https://arxiv.org/abs/2403.14667>.

9. “A Comprehensive Survey on Social Engineering-Based Attacks on Social Networks.” 2024. *International Journal / IJAAS (online)* — A comprehensive review article (systematic survey; PDF available). <https://www.science-gate.com/IJAAS/Articles/2024/2024-11-04/1021833ijaas202404016.pdf>.

10. Tóth, R., et al. 2024. “Impact of Emotions on User Behavior Toward Phishing Emails.” *Nordic Institute for Knowledge and Technology (NIKT) / NTNU open journal* (conference/journal item). PDF available from NTNU repository. <https://www.ntnu.no/ojs/index.php/nikt/article/view/6243>.

Слєпко Ангеліна Іванівна

Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:

Пакриш Олександр Євгенійович

кандидат технічних наук, доцент,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

ВІКОВІ ТА ГЕНДЕРНІ ВІДМІННОСТІ В ДОВІРЛИВОСТІ ДО ОНЛАЙН-ПРОПОЗИЦІЙ ЯК ФАКТОР РИЗИКУ ДО КІБЕРШАХРАЙСТВА

У сучасному цифровому середовищі кількість користувачів Інтернету стрімко зростає, що, з одного боку, відкриває нові можливості для спілкування, роботи й навчання, а з іншого – створює нові загрози. Однією з найпоширеніших небезпек є *кібершахрайство* – комплекс дій, спрямованих на отримання особистих даних, грошей чи доступу до конфіденційної інформації. Одним із ключових чинників, що визначає ймовірність стати жертвою кібершахрайства, виступає довірливість до онлайн-пропозицій. Довірливість у цьому контексті розуміється як схильність приймати інформацію або пропозицію без достатньої перевірки її достовірності.

Актуальність теми полягає в тому, що рівень довірливості значною мірою залежить від індивідуально-психологічних особливостей людини, зокрема від її віку та гендерної належності. Дослідження показують, що вікові зміни когнітивних функцій, емоційна вразливість і соціальна ізоляція можуть підвищувати рівень довірливості серед літніх осіб [1, с. 4]. Водночас молодь, попри високий рівень технічної грамотності, часто переоцінює свої навички розпізнавання шахрайства, що також створює ризик стати жертвою.

Тему довіри в Інтернет-середовищі, вікових та гендерних особливостей сприйняття ризику активно вивчають: Н. М. Василець – досліджує соціально-психологічні чинники довіри громадян в умовах цифровізації [2]; О. М. Мосол – аналізує психологічні аспекти міжособистісної довіри та її роль у взаємодії людей [3]. Зарубіжні автори, зокрема D. Modic і M. Anderson, досліджують когнітивні та емоційні механізми, які роблять людей більш сприйнятливими до шахрайських повідомлень [4].

В межах гендерного аспекту науковці звертають увагу, що чоловіки й жінки по-різному оцінюють ступінь ризику та довіри до джерел інформації. Наприклад, жінки частіше довіряють відгукам, емоційним повідомленням та соціальним рекомендаціям, тоді як чоловіки – інформації, яка виглядає логічно структурованою чи офіційною. У роботі Rebecca Cole [5, с. 3] наголошується, що самотність і прагнення до соціального контакту підсилюють довірливість жінок у випадках онлайн-знайомств, що призводить до зростання кількості романтичних шахрайств.

Як показує дослідження Chen Н. та співавторів, літні користувачі мережі частіше піддаються на шахрайські схеми, пов'язані зі здоров'ям, оскільки мають обмежену цифрову компетентність і схильні довіряти повідомленням, які апелюють до страху за власний добробут. У той же час молоді люди є вразливими до фінансових ігор, інвестиційних пропозицій або швидких заробітків, що базуються на довірі до “молодіжних” брендів і популярних блогерів.

Вікові відмінності також впливають на емоційну складову сприйняття інформації. Літні особи демонструють нижчу здатність до критичної оцінки контенту, часто сприймають повідомлення буквально та покладаються на попередній життєвий досвід, який не завжди адаптований до цифрового середовища. Як зазначено у звіті MDPI [6], з віком знижується здатність розрізняти безпечні й шкідливі повідомлення, що збільшує ризик стати жертвою фішингу.

Гендерні відмінності проявляються і в особистісних якостях, що визначають ступінь довірливості. Жінки схильні виявляти більше емпатії та відкритості до міжособистісних контактів, що може збільшувати ризик під час онлайн-спілкування. Чоловіки, навпаки, часто демонструють надмірну впевненість у власній цифровій компетентності, через що ігнорують попереджувальні сигнали шахрайства

Типи онлайн-пропозицій, що найчастіше стають інструментами шахрайства, охоплюють кілька категорій: медичні та оздоровчі поради, пропозиції швидкого заробітку, онлайн-знайомства, “акційні” покупки, розіграші, а також запрошення до сумнівних фінансових проєктів. Для кожної вікової та гендерної групи шахраї створюють окремі тактики маніпуляції. Наприклад, для літніх – через емоційні повідомлення (“Ви виграли приз” або “Терміново потрібно оновити дані банку”), для молоді – через цікаві виклики, “прибуткові інвестиції” або псевдопартнерства.

Психологічними чинниками підвищеної довірливості є низький рівень критичного мислення, потреба у визнанні, відчуття самотності, а також відсутність навичок перевірки джерел. Вік і гендер лише підсилюють ці механізми, створюючи специфічний профіль потенційної жертви. Як зазначає Cole [5, с. 4], “самотність і віра в щирість іншої людини в онлайні часто є тим самим гачком, який призводить до фінансових і емоційних втрат”.

З огляду на викладене, для зниження ризику потрапляння в пастку кібершахрайства доцільно дотримуватися *низки загальних порад*. Насамперед, слід розвивати критичне мислення та навички перевірки достовірності онлайн-інформації. Важливо не реагувати імпульсивно на емоційні або “термінові” повідомлення, уникати розголошення особистих і фінансових даних, а також перевіряти джерело будь-яких пропозицій. Рекомендується використовувати складні паролі, двофакторну автентифікацію та регулярно оновлювати програмне забезпечення. Особливу увагу варто приділяти підвищенню цифрової грамотності літніх користувачів і формуванню у молоді звички критично оцінювати онлайн-контент. Для жінок важливо зберігати обережність у випадках емоційних або соціально орієнтованих пропозицій, а чоловікам – уникати надмірної самовпевненості у власних технічних навичках.

Висновки. Довірливість до онлайн-пропозицій є одним із ключових психологічних чинників, що підвищують ризик стати жертвою кібершахрайства. Вікові та гендерні особливості користувачів суттєво впливають на рівень цієї довірливості: літні люди частіше демонструють емоційну вразливість і знижену критичність сприйняття інформації, тоді як молодь нерідко переоцінює власну цифрову компетентність. Гендерні відмінності проявляються у різних формах довіри до джерел – емоційній у жінок та раціональній у чоловіків. Отже, ефективна профілактика кібершахрайства потребує диференційованого підходу: розвитку цифрової грамотності серед літніх осіб, формування критичного мислення у молоді та підвищення емоційної стійкості в усіх групах користувачів. Підвищення обізнаності й уважності в онлайн-середовищі є запорукою безпечного цифрового простору.

Список використаних джерел:

1. Chen H., He M., Xu X., Atkin D. Examining older adults' vulnerability to online health scams: insights from routine activity theory // *Frontiers in Public Health*. – 2025.
2. Василюк Н. М. Соціально-психологічні чинники довіри громадян в умовах цифровізації: дис. канд. психол. наук. – Київ: ІПЗД НАПН України, 2021. – 201 с.
3. Мосол О. М. Психологічні аспекти міжособистісної довіри. – *Науковий вісник Ужгородського університету. Серія: Психологія*, 2019. – Вип. 1(44). – С. 49–54.

4. Modic, D., Anderson, R. Reading this may harm your computer: The psychology of scams. – *Journal of Cybersecurity*, 2015. – Vol. 1(1). – P. 87–97.
5. Cole R. Scammed by Love: The Role of Loneliness, Trust, and Age in Financial Losses from U.S. Online Romance Scams // *Innovation in Aging*. – 2024.
6. Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review // *MDPI*. – 2022. – Vol. 15(4), p. 2236.

Гуменюк Вікторія Олегівна

Студентка групи 202_СПС ННІ права та психології НАВС

Науковий керівник:

Пакриш Олександр Євгенійович

кандидат технічних наук, доцент,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

ЗНАЧЕННЯ ЛЮДСЬКОГО ФАКТОРУ У КІБЕРБЕЗПЕЦІ

У сучасному світі, де більшість інформаційних процесів відбувається у цифровому просторі, питання кібербезпеки набуває вирішального значення. Ми живемо в епоху, коли інформація стала не лише ресурсом, а й об'єктом постійних атак. Щодня відбуваються мільйони кібератак на приватні особи, підприємства й навіть державні установи. Попри стрімкий розвиток технологій захисту – антивірусів, систем виявлення вторгнень, шифрування даних, – головним і найвразливішим елементом системи безпеки залишається людина. Саме людський фактор, тобто дії, помилки чи поведінкові особливості користувачів, визначає, наскільки ефективною буде будь-яка система кіберзахисту.

Людський фактор у кібербезпеці – це сукупність психологічних, поведінкових і організаційних аспектів, які впливають на безпеку інформаційних систем. Іншими словами, це все, що пов'язано з тим, як люди взаємодіють із технологіями.

Людина може бути як найсильнішою, так і найслабшою ланкою в системі. З одного боку, жодна система не може ефективно працювати без відповідальних і навчених працівників. З іншого – саме через необережність, неуважність або навмисні дії люди часто виникають серйозні порушення безпеки.

Помилки користувачів є однією з найпоширеніших причин кіберінцидентів. Наприклад, відкриття шкідливих файлів, натискання на підозрілі посилання, введення паролів на фішингових сайтах або ненавмисне розголошення конфіденційних даних.

Такі помилки часто спричинені не злим умислом, а браком знань чи звичайною неухважністю. Дослідження різних компаній показують, що близько 88% усіх витоків даних пов'язані саме з людським фактором – помилками, порушенням політик безпеки або соціальною інженерією.

Аналогічно, за даними Crowe, у 74% кібератак людська дія відіграла ключову роль. Особливу загрозу становить явище соціальної інженерії – це коли зловмисники використовують психологічні прийоми, щоб змусити людину самостійно відкрити їм доступ до системи.

Найчастіше це відбувається через електронні листи або повідомлення, які виглядають правдоподібно. Людина натискає на шкідливе посилання або вводить пароль, вважаючи, що спілкується з колегою чи офіційною службою. Подібні атаки доводять, що технологічні системи можуть бути надійними, але людська довірливість залишається найслабшим місцем у будь-якому захисті.

Не менш небезпечними є так звані «інсайдерські загрози», коли співробітники навмисно порушують правила безпеки. Це може бути зрада, корупційний вплив або звичайне невдоволення умовами праці. В одному з наукових звітів за 2023 рік зазначається, що приблизно чверть кіберінцидентів відбувається через навмисні дії співробітників. Тобто небезпека походить не лише ззовні, а й із середини організації.

Велику роль відіграє також психологічний стан людини. Стрес, перевтома, перевантаження інформацією або багатозадачність суттєво збільшують ризик помилок. Працівники, які працюють у режимі постійного тиску або поспіху, частіше ігнорують процедури безпеки чи шукають «короткі шляхи» виконання завдань. Таким чином, створення комфортного робочого середовища є не лише питанням турботи про персонал, а й одним із аспектів кіберзахисту.

Попри те, що людський фактор є причиною більшості інцидентів, саме людина може стати ключем до їх запобігання. Для цього потрібно інвестувати у навчання, підвищення обізнаності та формування культури безпеки. Як свідчить досвід компаній, що впроваджують програми підготовки персоналу, регулярні тренінги, симуляції фішингових атак і навчальні кампанії значно знижують кількість успішних кібератак.

Сьогодні важливо не лише навчити працівників технічним правилам – створювати складні паролі, не відкривати невідомі файли, – а й пояснити, як працюють психологічні пастки, на які розраховують хакери. Сучасний підхід до кіберзахисту базується на поєднанні технологічних і людських ресурсів. Технології здатні відслідковувати аномальну поведінку користувачів, автоматично оновлювати системи, обмежувати доступи.

Але жодна технологія не може повністю замінити людське мислення, інтуїцію й відповідальність. Саме тому ефективна кібербезпека передбачає створення систем, які враховують людські обмеження.

Наприклад, інтерфейси мають бути зрозумілими, попередження – чіткими, а процеси – такими, щоб користувачеві було простіше діяти безпечно, ніж ризиковано.

Важливим напрямом є формування культури кібербезпеки в організаціях. Це означає, що питання безпеки повинно бути не лише технічним завданням ІТ-відділу, а спільною відповідальністю кожного працівника. Коли керівництво демонструє, що безпека – це цінність, а не формальність, персонал починає ставитися до цього серйозніше. Успішні компанії впроваджують системи мотивації, винагороджують уважність, проводять конкурси на кращі безпечні практики.

Історія кіберінцидентів показує, що навіть одна людська помилка може спричинити мільйонні збитки. Наприклад, у 2017 році під час атаки WannaCry багато організацій зазнали втрат не через недосконалість технологій, а через те, що працівники не встановили оновлення безпеки. Інший приклад – недавня атака на авіакомпанію Qantas, де зловмисники змогли отримати доступ до системи через один телефонний дзвінок і довірливу відповідь працівника. Це яскраво ілюструє, що навіть найдосконаліші системи можуть бути зруйновані одним людським рішенням.

Отже, людський фактор – це не лише слабкість, а й ресурс, який можна перетворити на перевагу. Якщо організація правильно працює зі своїми людьми, навчає їх, мотивує, створює сприятливе середовище та розумно поєднує технології з людською відповідальністю, рівень кібербезпеки зростає в рази. Кіберзахист – це не тільки питання програм і систем, це насамперед питання культури, поведінки й свідомості кожного користувача.

Підсумовуючи, можна сказати, що жодна технологія не здатна повністю усунути людський фактор, але його можна контролювати, передбачати й використовувати на користь безпеки. Люди залишаються головною силою й водночас головним викликом кібербезпеки. Саме від рівня їхньої підготовки, уваги та відповідальності залежить, наскільки захищеним буде наш цифровий світ.

Список використаних джерел:

1. Crowe. The Human Factor in Cybersecurity. – Режим доступу: <https://www.crowe.com/>
2. BCS365. The Importance of Employee Training in Cybersecurity. – Режим доступу: <https://www.bcs365.com/>
3. Kaspersky. Human Factor Report 2023. – Режим доступу: <https://www.kaspersky.com/>
4. LevelBlue. Behavioral Insights and Mitigation Strategies. – Режим доступу: <https://www.levelblue.com/>
5. Наука Онлайн. Вплив людського фактора на якість систем безпеки. – Режим доступу: <https://nauka-online.com/>

6. SpringerLink. Human factors in cybersecurity: An interdisciplinary review. – Режим доступу: <https://link.springer.com/Threatscape>. The Human Factor in Cyber Security. – Режим доступу: <https://www.threatscape.com/>

7. The Guardian. Qantas cyberattack: staff error leads to data exposure. – Режим доступу: <https://www.theguardian.com/>

Yarotska Anastasiia Stanislavivna

Student of academic group 301_SPS,
Institute of Law and Psychology, NAIA

Scientific supervisor:

Pakrysh Oleksandr Yevheniiovych

Candidate of Technical Sciences,
Associate Professor, Associate Professor
of the Department of Information
Technologies, Institute of Law and
Psychology, NAIA

PSYCHOLOGICAL TYPES OF CYBERCRIMINALS

In the modern world, where almost every person has easy access to the Internet, and it is not limited to a home desktop computer, new ways of illegal, criminal behavior are opening up, and therefore, with the advent of the Internet, cybercriminals have appeared in our lives. According to the definition of the Law of Ukraine “On the Basic Principles of Ensuring Cybersecurity of Ukraine”, a cybercrime is a socially dangerous guilty act in cyberspace and/or with its use. A cybercriminal, accordingly, is a person who committed such a crime.

As each type of illegal behavior in cybercrime has a certain collective profile of the offender, I propose to examine it from several points of view: the general characteristics of the cybercriminal (who are these people and what controls them), psychological types of cybercriminals by motivation for committing crimes and by approaches to illegal activities in cyberspace. I chose to characterize psychological types by their type of activity.

The general profile of a cybercriminal begins with the same general criminal craving/desire to obtain a benefit that is impossible (or difficult) to obtain in a law-abiding way. However, by the nature of the diversity of cyberspace, these benefits are radically different. A cybercriminal is primarily attracted by anonymity, invisibility in an infinite number of Internet connoisseurs. As in the real world, a person who wants to commit a crime is attracted to remaining unexposed, and ultimately unpunished.

Messengers do not leave fingerprints in the conventional sense, and when committing a virtual crime, you do not have to look into the eyes of the people you are robbing, psychologically this aspect can have a calming effect on a potential criminal and lower the threshold for committing the crime. "No one will recognize me here", "They won't be able to find out who I am", and "They can't get me back", this is how I would summarize the main ideas when describing the choice process of cybercrime over another type of crime [1].

With technological development, forced authorization on popular sites, applications, and search engines is increasingly coming to the virtual world, and anonymity has become more difficult to maintain. To do this, the criminal needs at least an initial level of knowledge in information technology. Thanks to specialized browsers (such as Tor, for example) and software that can be customized (operating systems such as Linux, Ubuntu), a cybercriminal can still achieve maximum anonymity. Therefore, in order to engage in cybercrime, it is worth having a large amount of knowledge and technical capabilities. From a psychological point of view, a person who wants to commit a crime, seeks anonymity and achieves it – sends a fairly clear message: it can be assumed that a person is not very socially adapted to a certain level, or at least perceives society with detachment, has a fairly developed level of awareness of technology and has money driven motives.

According to the motivation for committing crimes in cyberspace, offenders can be divided into: scammers, identity thieves, cyberterrorists, stalkers, hacktivists and hobby hackers.

Scammers and identity thieves mainly operate with the desire to get monetary gain, in one way or another: scammers trick people for money, and identity thieves steal personal information and use it to steal money, or resell this information to data brokers. This type of cybercriminal is characterized primarily by selfishness, some degree of immorality, greed for power.

Cyberterrorists operate mainly with DDoS attacks, thanks to such massive attacks, it is possible to leave without information, for example, banks, government agencies, enterprises of any type, due to oversaturation and temporary shutdown of servers. Usually, during or after a massive DDoS attack on software, information remains in danger, and this is followed by data theft. Cyberterrorists usually do not work alone, as they are often sponsored by organizations or specific stakeholders. Psychologically, these are most likely very closed individuals or groups of people who are morally gray, and despite their prejudices, often work under the auspices of customers. If this is a group of cyberterrorists, then most likely their style of activity will converge with hacktivists.

Stalkers, like offline stalkers, are looking for information about a specific person or group of people, their goal is to collect information and directly monitor the activities of the object. Stalking and stalking often have a characteristic for it obsessive nature, sometimes sexually determined.

Hobby hackers are amateur enthusiasts who engage in cybercrime mainly not for reward, but to satisfy their interest or ego. For a hacker's hobby, it is not necessary to steal or break something, for them it is enough to know that this system can be hacked, and hack it. It is logical to expect that first of all this person will be self-centered, primarily love technology, and will orient first and foremost on their own individual goals in criminal acts.

Hacktivists (hackers-activists) use criminal methods to influence the state of events in political terms, achieve the termination of a service, or steal information for distribution to the public. Like ordinary activists, hacktivists tend to have a strong sense of justice, or its violation.

According to the main approaches to illegal activities in cyberspace, criminals can be described as white hats, black hats and gray hats.

“White hat” hackers are known as “ethical hackers”. They have the same experience and knowledge as black hats, but organizations legally allow them to “hack” their systems.

White hats test security weaknesses and vulnerabilities in IT systems before black hats can exploit them. The white hats then patch up all the loopholes they have discovered. In this way, their proactive hacking prevents the actions of black hats or minimizes the damage that black hats can cause. A white hat in itself does not mean criminal activity, but can operate on illegal software, or not request access properly.

“Black hats” are dangerous, highly skilled and motivated by personal and financial gain. They hack with malicious intent and use their knowledge of programming languages, network architecture, and network protocols.

Black hats illegally infiltrate networks to compromise or stop an organization entirely. They hack into accounts to delete, modify, or destroy sensitive data. They also organize small and large-scale phishing attacks and other cybercrimes.

“Gray hats” border between black hats and white hats. While their motives are usually good, they still engage in technically illegal hacks like black hats do.

For example, a gray hat sees that a bank has just updated an app. It can intentionally (but illegally) hack into a system to find potentially vulnerable spots.

Instead of committing a hack, gray hats alert system administrators to flaws so that they can be fixed before the black hat takes advantage.

White, black, and gray hats can be characterized, respectively, by the desire to do good, evil, or something in between [2].

In terms of personality profile, Black Hats are usually highly intelligent and technically gifted. Studies often indicate that they may exhibit traits associated with the “Dark Triad” (Manipulative, Psychopathy), as well as a high propensity for risk and thrill-seeking. Their potential victims range from ordinary citizens with valuable data to large corporations, financial institutions, and government organizations that have weaknesses in their cyber defenses [3].

Cybercrime is evolving due to a combination of several key factors: high financial profitability, the rapid development of technology and the growth of computerization of society, as well as the low level of awareness of many users.

References:

1. Marleen Weulen Kranenbarg, Jean-Louis van Gelder, Ard J. Barends, Reinout E. de Vries. 2023. "Is there a cybercriminal personality? Comparing cyber offenders and offline offenders on HEXACO personality domains and their underlying facets." // *Computers in Human Behavior*. Volume 140. March 2023. <https://doi.org/10.1016/j.chb.2022.107576>.
2. Межа між кіберзлочинністю та етичним хакінгом — 15 типів хакерів, які вам потрібно знати у 2023 році [Electronic resource]. URL: <https://10guards.com/ua/blog/2023/06/20/the-thin-line-between-cybercrime-and-ethical-hacking-the-15-types-of-hackers-you-need-to-know-in-2023/> (date of application 10.10.2025).
3. Truong Jack Luu, Binny M. Samuel, Michael Jones, J.C. Barnes. 2025. "Exploring how the Dark Triad shapes cybercrime responses" // *Personality and Individual Differences*. Volume 244. October 2025. <https://doi.org/10.1016/j.paid.2025.113250>.

Жицька Валерія Олегівна

Студентка н.гр. 117 СПД ННІ права
та психології НАВС

Науковий керівник:

Тарасенко Володимир Петрович

кандидат фізико-математичних наук,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

СТАН ТА ШЛЯХИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

В наш час особливо, під час воєнного стану в Україні, дуже важливим є кібербезпека громадян і країни в цілому. Тому в роботі було розглянуто деякі проблеми кібербезпеки в Україні і шляхи їх усунення. Було проаналізовано проблеми в процесі створення безпечного кіберпростору в Україні, встановлено, що одним із можливих шляхів до створення безпечного кіберпростору є розвиток відповідної освіти в Україні.

Громадяни мають бути забезпечені знаннями щодо захисту особистих даних, продуктів власної творчості, ділової інформації та мати відповідні вміння щодо безпечного використання інформаційного середовища. Доведено важливість поширення комп'ютерної грамотності серед студентів.

Сучасні інформаційні технології розвиваються швидко. Одночасно і зростає рівень незахищеності людини в інфопросторі, який став невід'ємною частиною життя.

Кіберзагрози та кібератаки стали звичайним явищем в сучасному світі. Кібербезпека – частина національної безпеки. Її стан – умова стабільного розвитку країни. Тому постійне вдосконалення системи кіберзахисту – одна із актуальних сучасних завдань держави. Шляхів такого вдосконалення існує достатньо. Важливою є міжнародна співпраця в обміні досвідом між різними країнами світу стосовно створення безпечного кіберпростору. В умовах посилення кібератак та інформаційної війни для України така співпраця є необхідною, а робота зі створення ефективної системи кіберзахисту має проходити пришвидшеними темпами, особливо під час воєнного стану в країні.

Вважається, що кіберпростір дуже скоро стане новим полем для війн в сучасному світі, а рівень обороноздатності країни буде визначатись за показниками якості та ефективності кіберзахисту. Тому дуже важливо знайти оптимальні шляхи удосконалення системи кібербезпеки в Україні та забезпечити їх впровадження.

Вперше поняття «кіберпростір» було використано у 1980-х роках. *Кіберпростір* – це нове середовище, яке з'явилося внаслідок функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем; нова сфера, яка не існує в фізичній формі, але передбачає активну взаємодію осіб, програмного забезпечення та послуг у мережі Інтернет.

Кібербезпека – це захищеність важливих інтересів людини, суспільства і держави в кіберпросторі, яка забезпечує сталий розвиток інформаційного суспільства, цифрового середовища, швидке виявлення та реагування на загрози безпеці. Це збереження конфіденційності та цілісності інформації у кіберпросторі. Таким чином, кібербезпека стосується захисту прав і свобод громадян в ході пересування кіберпростором та національних інтересів держави.

Кіберзахист – це система організаційних, правових, інженерно-технічних та інших заходів, спрямованих на запобігання кіберзагрозам, ліквідацію їх наслідків, відновлення надійності інформаційних систем. Деякі дослідники вважають, що ми вступили в фазу кібервійн (кіберінтревенції), оскільки факти небезпечних дій в кіберпросторі зростають кількісно та якісно.

Кіберінтревенція – це комплекс суспільно небезпечних дій, які наносять шкоду важливим сферам існування держави та суспільства. Різні сектори державного, економічного, суспільного життя стають більш уразливими до подібного роду дій, потребують захисту.

Кіберзлочинність набула характеру транснаціонального. Кібергрупи та окремі хакери активізуються, здійснюють атаки на урядові та приватні сайти, порушують роботу інформаційних ресурсів.

Поширився кардінг – фінансові злочини в кіберпросторі. Серед наслідків кіберінцидентів різного характеру завдання удару авторитету держави, розповсюдження неправдивої інформації, дезорієнтація населення, збір цінної інформації, порушення функціонування сайтів, комп'ютерних систем, об'єктів критичної інфраструктури. У 2014 році в Україні було зафіксовано 216 кібератак ззовні, більша частина з яких була здійснена на державні установи. У 2015 році кількість таких атак значно збільшилась. Кожен третій комп'ютер в Україні заражений шкідливими програмами. На одне з 36 мобільних пристроїв встановлені небезпечні додатки. Один з 13 пошукових запитів призводять до шкідливих програм. Тому одним із важливих завдань держави є встановлення таких рівнів захисту інформації, як: запобігання (надання доступу виключно персоналу), виявлення (раннє виявлення злочинних дій), обмеження (зменшення масштабів наслідків злочинів), відновлення (можливість відновлення втраченої інформації).

Створення безпечного кіберпростору передбачає впровадження системи заходів на декількох рівнях одночасно: політичному, юридичному, міжнародному, освітньому, науково-технічному. З кожним роком органи публічного управління дедалі більше залежать від технологій та переводять свою діяльність у цифровий світ. Постає проблема якісної взаємодії з громадянами, що потребує створення нового формату відносин у рамках процесу діджиталізації в Україні.

Кіберзагрози несуть реальні ризики та зумовлюють орієнтацію на цифрову грамотність в публічному управлінні. Здатність ефективно використовувати сучасні цифрові технології – важливе вміння сучасного державного службовця. В умовах децентралізації важливим є й забезпечення компетенції цифрової грамотності в органах місцевого самоврядування.

Україна має орієнтуватись на кращі зарубіжні практики зі створення ефективної системи кіберзахисту, розширювати міжнародну співпрацю в цьому напрямку. У 2005 році була ратифікована Конвенція Ради Європи про кіберзлочинність від 2001 року. Вона була створена для запобігання поширення кіберзлочинності, вказує на необхідність співробітництва між державами з метою створення більш ефективної системи захисту своїх інтересів у ході використання інформаційних технологій.

Це перша спроба у Європі об'єднати зусилля у боротьбі із кіберзлочинністю. Після підписання Україною Угоди з ЄС наша держава взяла на себе зобов'язання впроваджувати чинне законодавство Союзу, в тому числі, у сфері кібербезпеки.

Висновки. В новому середовищі, яким є кіберпростір, особливо актуальною проблемою для всіх сучасних країн є кіберзахист та кібербезпека. XXI століття є часом поширення кібератак та кіберзлочинів різного характеру.

Тому метою України зараз є посилення кіберзахисту, захист прав і свобод громадян, державних інтересів. Нашою країною були ратифіковані відповідні міжнародні угоди, створена юридична база для запуску та функціонування системи кіберзахисту. Для її вдосконалення слід розширювати міжнародну співпрацю, запозичувати корисний досвід, об'єднувати зусилля. Напрямом подальшої роботи є конкретизація Стратегії кібербезпеки України, розробка додаткових нормативно-правових актів, швидка координація дій компетентних органів. Система кіберзахисту має загальнодержавний характер, включаючи декілька напрямків: міжнародний, політичний, юридичний, організаційний, освітній.

Список використаних джерел:

1. Бакалінська О., & Бакалінський О. Правове забезпечення кібербезпеки в Україні. Піприємництво, господарство і право, 2019. 9, 100-108. <https://doi.org/10.32849/2663-5313/2019.9.17>
2. Грицюк Ю.І. Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. Науковий вісник НЛТУ, 2016. 26(8), 327-337. <https://doi.org/10.15421/40260850>
3. Трофименко О., Прокоп Ю., Логінова Н., & Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації, 2019. 150-157. <https://doi.org/10.18372/2410-7840.21.13951>

Савчин Євгенія Андріївна

Студентка н.гр. 117 СПД ННІ права
та психології НАВС

Науковий керівник:

Тарасенко Володимир Петрович

кандидат фізико-математичних наук,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

РОЛЬ «ШІ» У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Штучний інтелект і кібербезпека стають все важливішими в сучасному світі, де кількість кібератак постійно зростає.

Особи, які відповідають за прийняття рішень у різних сферах, зосереджують увагу на аналізі та поліпшенні кібербезпеки. Але це не просте завдання, оскільки треба забезпечити баланс між захистом особистих даних і відповідністю нормативам.

Інновації в галузі кібербезпеки постійно розвиваються, але разом з ними розвиваються й кіберзлочинці, шукаючи нові способи атак. У такому динамічному середовищі кібербезпека стає набагато важливішою, ніж раніше.

Штучний інтелект і кібербезпека йдуть пліч-о-пліч, оскільки ми дивимось в цифрове майбутнє і використовуємо новітні технології, щоб залишатися захищеними. За оцінками Forbes, до 2027 року ринкова вартість ШІ у сфері кібербезпеки досягне 46,3 мільярда доларів, оскільки все більше бізнес-лідерів користуються його можливостями для автоматизації даних, виявлення ризиків і захисту конфіденційної інформації.

Розуміння ландшафту кібербезпеки

Сучасний ландшафт кіберзагроз охоплює всі ризики, на які наражаються різні організації у відповідних контекстах. Кіберзагрози постійно еволюціонують у всі сфери діяльності, особливо з поширенням Інтернету та впровадженням цифрових технологій, що призводить до зростання цих ризиків. Численні інциденти в мережі залишаються постійною загрозою для всіх організацій, які працюють у віртуальному просторі.

За даними CNN, навіть уряд США залишається мішенню, ставши жертвою нещодавньої глобальної атаки, яка використала вразливість програмного забезпечення. Кілька сотень організацій по всій країні постраждали від цієї атаки. На кожен новий інструмент, який розробляється для захисту від кіберзлочинців, хакери створюють свій власний, і кількість випадків кіберзлочинів продовжує зростати.

За даними Північно-Західного університету, середня вартість витоку даних становить близько 4,27 мільйона доларів, тому організації повинні застосовувати надійні заходи кібербезпеки, щоб випереджати небезпеки. Застосування штучного інтелекту в кібербезпеці – це один з багатьох підходів до того, щоб залишатися гнучкими в динамічному просторі. Це інноваційний інструмент, який організації можуть використовувати для захисту конфіденційних даних і запобігання фінансовим і репутаційним наслідкам кібератак.

ШІ в кібербезпеці

Штучний інтелект – це широкий термін, що описує процес імітації людського інтелекту в машинах, щоб вони могли міркувати і використовувати логіку для вирішення проблем. Штучний інтелект у кібербезпеці базується на тому ж принципі: використання швидкості та обчислювальної потужності ШІ для створення протоколів кібербезпеки, які передбачають, ідентифікують та зменшують загрози.

На людські помилки припадає понад 80% кіберінцидентів і ШІ може заповнити цю прогалину, автоматизуючи завдання і розпізнаючи закономірності, невидимі для людського ока. Наприклад, алгоритми машинного навчання можуть класифікувати зловмисні атаки електронною поштою та виявляти схожі функції, які працівники можуть не помітити.

Такі інструменти, як обробка природної мови, можуть виявляти фішингову активність і шкідливе програмне забезпечення шляхом вилучення ключових слів.

Штучний інтелект навчається на власному досвіді. Генеративний ШІ перетинається з кібербезпекою, аналізуючи і навчаючись на величезних обсягах даних, щоб виявляти закономірності і приймати обґрунтовані рішення щодо реагування на потенційні загрози. Хоча він може вирішити лише деякі проблеми кібербезпеки, ШІ відіграє важливу роль у підтримці зусиль з кібербезпеки та дотриманні нормативних вимог.

Виявлення та запобігання загрозам

ШІ має значну перевагу над традиційними програмними системами у виявленні загроз. Оскільки він навчається на власному досвіді і працює швидше, ніж будь-яка людина, можна навчити його виявляти шкідливе програмне забезпечення, розпізнавати шаблони і помічати найнезначніші зміни.

Прогностичний інтелект – це ще одна сфера, у якій ШІ досягає успіху. Завдяки можливостям обробки природної мови штучний інтелект може переглядати статті в новинах, журналах і дослідженнях про кіберзагрози, створюючи чітку картину того, як вони можуть вплинути на вашу організацію.

Ось деякі з інших потенційних ризиків і обмежень:

Помилкові спрацьовування або негативи: ШІ може генерувати хибні спрацьовування – ідентифікуючи нешкідливі дії як зловмисні – і хибні негативи, роблячи протилежну помилку. Помилкові спрацьовування та негативи можуть бути складними для навігації, оскільки вони відволікають цінні ресурси на неіснуючі загрози або ігнорують наявні.

Етичні проблеми: хоча ШІ є революційним у сфері кібербезпеки, він створює етичні та регуляторні проблеми, особливо щодо конфіденційності даних. Наприклад, медичні організації повинні дотримуватися суворих правил HIPAA, щоб забезпечити конфіденційність інформації про пацієнтів.

Дефіцит навичок: ШІ є життєздатним варіантом лише для тих організацій, які мають доступ до кваліфікованих фахівців з кібербезпеки. Оскільки 63% організацій стверджують, що найбільший дефіцит навичок у них спостерігається у сфері ШІ та машинного навчання, подолання цього розриву може бути непростим завданням. Маючи необхідні навички та досвід, організації можуть усвідомити загальну цінність своїх інвестицій у ШІ та машинне навчання.

Якість даних. ШІ настільки ж ефективний, як і дані, на яких ви його тренуєте, і потребує великої кількості високоякісних даних, щоб підвищити точність. Багатьом організаціям важко отримати доступ до достатньої кількості цих високорівневих даних через проблеми конфіденційності та розмежованості.

Перевірка сайтів і безпека онлайн-транзакцій

Один із ключових аспектів захисту в цифровому просторі – це безпека вебсайтів, особливо тих, які використовують онлайн-транзакції. Для користувачів важливо перевіряти надійність сайтів перед тим, як здійснювати будь-які операції.

Як перевірити сайт на безпеку:

Шифрування SSL: переконайтеся, що сайт використовує захищений протокол SSL (<https://>). Це гарантує, що дані, які ви вводите, шифруються та захищаються під час передачі.

Перевірка домену: остерігайтеся підроблених сайтів, що імітують популярні платформи. Перевіряйте точність написання домену та сертифікати безпеки.

Огляди та рейтинги: перевіряйте відгуки про сайт, щоб переконатися у його надійності.

Користувачі, які взаємодіють із платформами, де здійснюються фінансові операції, повинні завжди перевіряти, чи захищені їхні дані. Онлайн-лотереї, як-от лото клуб онлайн, та інші сервіси можуть надавати чудові можливості для розваг, але важливо користуватися лише перевіреними платформами.

Висновки. Штучний інтелект вже зараз відіграє важливу роль у захисті від кіберзлочинів, але з кожною новою технологією виникають нові виклики. Зловмисники також вивчають можливості ШІ, що робить боротьбу з кіберзлочинністю постійною гонкою технологій. Для користувачів важливо не лише сподіватися на ШІ, але й бути обережними під час використання онлайн-платформ і перевіряти надійність сайтів перед здійсненням транзакцій.

Список використаних джерел:

1. <https://cripo.com.ua/news/society/rol-shtuchnogo-intelektu-u-borotbi-z-kiberzlochynnistyu-chy-mozhut-tehnologiyi-vyperedyty-hakeriv/amp/>
2. <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>

Богула Софія Дмитрівна

Студентка н.гр. 302 СПС ННІ права
та психології НАВС

Науковий керівник:

Тарасенко Володимир Петрович

кандидат фізико-математичних наук,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

ПСИХОЛОГІЧНІ НАСЛІДКИ КІБЕРШАХРАЙСТВА

У сучасному світі, де більшість життєвих процесів відбуваються в онлайн-просторі, людина стає особливо вразливою до кіберзлочинів. Одним із найпоширеніших проявів кіберзлочинності є *кібершахрайство* – злочин, який не лише завдає матеріальної шкоди, а й має серйозні психологічні наслідки для жертв.

Кібершахрайство є різновидом кіберзлочинності, який полягає у використанні комп'ютерних технологій, мережі Інтернет або електронних комунікацій для незаконного заволодіння чужим майном, коштами чи персональними даними. Тобто, основною ознакою кібершахрайства є введення жертви в оману з використанням цифрових засобів. Це може бути створення фішингових сайтів, підроблених сторінок банків, онлайн-магазинів або соціальних акаунтів, через які шахраї отримують доступ до коштів чи особистої інформації.

До основних форм кібершахрайства належать:

1. Фішинг – отримання особистих даних користувача (логінів, паролів, реквізитів карток) шляхом підробки сайтів або електронних листів.
2. Онлайн-шахрайство в соціальних мережах – створення фейкових акаунтів для виманювання грошей чи даних.
3. Шахрайство з банківськими картками (скімеринг) – незаконне копіювання реквізитів картки та використання їх для крадіжки коштів.
4. Інвестиційне шахрайство – пропозиція «високоприбуткових» онлайн-вкладень, які насправді є фінансовими пірамідами.
5. Love scam – емоційне маніпулювання жертвами через знайомства онлайн з метою заволодіння їхніми фінансами.

Проблема кібершахрайства виходить далеко за межі матеріальних втрат. Вона має глибокі психологічні наслідки, які можуть впливати на емоційний стан, самооцінку, довіру та соціальну поведінку людини.

1. *Емоційний шок і гострий стрес.*

Жертви часто переживають сильне потрясіння після усвідомлення обману. З'являються почуття розгубленості, страху, сорому, гніву, а також соматичні прояви – безсоння, головний біль, прискорене серцебиття.

2. Втрата довіри до людей і систем.

Після пережитого шахрайства люди часто перестають довіряти не лише незнайомцям онлайн, а й знайомим, фінансовим установам, навіть власним родичам. Це може призводити до соціальної ізоляції.

3. Почуття провини та сорому.

Жертви часто звинувачують себе у «наївності» або «недалекоглядності», що формує почуття власної безпорадності. Особливо це характерно для молодих людей і літніх осіб, які не мають достатніх знань у сфері кібербезпеки.

4. Розвиток тривожних і депресивних станів.

Після шахрайства може розвинутися тривожний розлад, депресія, зниження самооцінки та навіть посттравматичний стресовий розлад (ПТСР). Люди часто уникають цифрових технологій, відчувають страх повторного обману.

5. Порушення соціальних контактів.

Після обману у сфері онлайн-знайомств (love scam) жертви можуть уникали нових стосунків, мають труднощі у встановленні емоційних зв'язків і довірі до партнерів.

Для ефективної протидії цьому явищу необхідна **комплексна стратегія**, що поєднує:

- 1) Інформаційно-просвітницьку роботу (навчальні кампанії, тренінги з кібергігієни).
- 2) Психологічну підтримку жертв – створення гарячих ліній, безкоштовних консультацій.
- 3) Використовувати двохфакторну автентифікацію.
- 4) Підвищення кіберграмотності населення, особливо дітей, підлітків і людей похилого віку.

Таким чином, кібершахрайство – це не лише фінансова загроза, а й серйозна соціально-психологічна проблема. Воно підриває довіру між людьми, провокує тривожність і емоційні травми, особливо серед вразливих груп населення. Тому важливо розвивати не лише технічні засоби захисту, а й психологічні програми підтримки, спрямовані на відновлення внутрішньої безпеки та довіри користувачів цифрового середовища.

Список використаних джерел:

1. Кіберзлочинність та електронні докази: навчальний посібник // Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. // Львівський національний університет імені Івана Франка, 2022 р. // ст. 14–15 // URL: <https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf>

2. Кібербезпека: правові та психологічні аспекти // Петков В. В. // Київ: КНТ, 2021 р. // ст. 63–70 // URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf
3. Поради з кібербезпеки для громадян // Міністерство цифрової трансформації України // офіційний сайт // URL: <https://thedigital.gov.ua/>

Чистоклєтова Анна Денисівна

Студентка н.гр. 302 СПС ННІ права
та психології НАВС

Науковий керівник:

Тарасенко Володимир Петрович

кандидат фізико-математичних наук,
доцент кафедри інформаційних
технологій ННІ права та психології
НАВС

МЕТОДИ ПСИХОЛОГІЧНОГО ВПЛИВУ У КІБЕРЗЛОЧИННОСТІ

Сучасний цифровий простір став не лише каналом передачі інформації, але й полем інтенсивної психологічної експлуатації: кіберзлочинці дедалі частіше змушують жертв приймати рішення, що шкодять їх інтересам.

Актуальність теми випливає з росту кількості фішингових атак, компрометацій акаунтів та витоку персональних даних [3]. Сучасні кібератаки дедалі частіше використовують соціальну інженерію, маніпуляцію увагою та емоціями жертв для досягнення фінансової, інформаційної або ж репутаційної вигоди, що зумовлює високий ризик системних втрат, як на рівні окремих користувачів, так і організацій. Та незважаючи на прогрес у технічних засобах захисту, їхня ефективність значною мірою залежить від розуміння та протидії психологічним механізмам, що маніпулюють увагою, емоційним станом жертви та спираються на соціальні правила поведінки.

У загальному вигляді під *кіберзлочинами* міжнародна спільнота розуміє: незаконний доступ, нелегальне перехоплення, втручання у дані або систему, зловживання пристроями, пов'язані з комп'ютерами, підробки та шахрайство, всі види забезпечення обігу та використання дитячої порнографії за допомогою комп'ютерної мережі, а також порушення авторських прав. Їх особливість полягає в середовищі здійснення – кіберпросторі, де «віртуальні» об'єкти психологічно сприймаються як більш доступні та менш захищені. Значущим криміногенним фактором також є анонімність користувачів, що дозволяє приховати особу, тим самим вводячи в оману інших та виступати під чужим іменем.

У поєднанні з дистанцією та відсутністю негайного соціального контролю, це послаблює моральні бар'єри, підсилює відчуття безкарності та створює сприятливі умови для вчинення злочинів [1].

Виходячи з описаних характеристик кіберпростору, можна виокремити низку конкретних психологічних методів впливу, які активно використовуються зловмисниками. Дані прийоми спрямовані на захоплення уваги, створення емоційного тиску та мобілізацію автоматичних реакцій жертви. Їхня мета – спонукання до конкретної дії (натискання посилання, введення даних, відкриття файлу або здійснення переказу), які в умовах спокійного, усвідомленого прийняття рішень жертва, швидше за все, не виконала б.

Відволікання уваги. Метод, що передбачає інсценування контакту від імені служби технічної підтримки. Під час телефонної розмови зловмисник інформує про нібито виявлене шкідливе ПЗ і наполягає на негайній інсталяції «інструмента для нейтралізації», який фактично є шкідливим. Щоб унеможливити критичне осмислення ситуації, шахрай застосовує спеціалізовану термінологію, демонструє сфабриковані вікна системних помилок і здійснює постійний психологічний тиск, апелюючи до терміновості [5].

Емоційна експлуатація. Зловмисники систематично використовують емоційні тригери – страх, жадібність, співчуття або почуття провини – щоб спонукати адресата до імпульсивних дій. Поширеною практикою є надсилання образливих або провокативних повідомлень від неідентифікованих профілів; зацікавлені користувачі переходять на сторінку відправника для з'ясування обставин. Часто такий профіль є закритим і містить лише одне гіперпосилання, розміщене угорі: воно викликає цікавість і підштовхує до переходу. Це посилання, як правило, є фішинговим і створює ризик несанкціонованого доступу до облікових записів у Telegram, Instagram чи інших сервісах [3].

Соціальна інженерія. Методика заснована на створенні ілюзії легітимності за допомогою підроблених документів, вебресурсів або електронних листів. Наприклад, фішингові повідомлення, що нібито надходять від банків, містять посилання на фальшиві сайти, а фейкові інвестиційні платформи супроводжуються підробленими ліцензіями й сертифікатами. Така тактика дозволяє отримувати персональні та фінансові дані жертв або схилити їх до здійснення платежів, оманливо спираючись на довіру, створену фіктивними атрибутами легітимності.

Створення ілюзії вигоди. Розсилка повідомлень про виграш значної суми або цінного подарунка супроводжується вимогою попередньої оплати «комісії» чи «податку» невеликого розміру. Обіцянка швидкого та легкого збагачення призводить до переказу коштів, після чого контакт з шахраями переривається.

Маніпулювання довірою. Кіберзлочинець, поінформований про близькі зв'язки жертви, може імітувати знайому особу – використовуючи схожий голос у дзвінку або надсилаючи повідомлення з підробленого профілю.

Апелювання до спільних спогадів або відомих лише вузькому колу деталей створює ілюзію достовірності; у такому контексті жертва часто без сумніву переказує кошти або надає конфіденційну інформацію [4].

Таким чином, психологічні методи впливу в кіберзлочинності призводять до суттєвих наслідків для жертв: прямі фінансові втрати, компрометація персональних і корпоративних даних, втрата доступу до акаунтів та довгострокові репутаційні й емоційні збитки. Часто пошкодження має каскадний характер – один скомпрометований обліковий запис полегшує подальші атаки. Отже, ефективний захист вимагає поєднання технічних заходів з організаційними процедурами й регулярним навчанням користувачів, що знижує імпульсивність рішень і підвищує стійкість до соціально-інженерних атак.

Список використаних джерел:

1. Дерев'ягін О. О., Пашнев Д. В., Новицький А. О. Окремі підходи до визначення сучасного портрету професійного кібершахрая. *Вісник Кримінологічної асоціації України*. 2025. Т. 34, № 1. С. 236–248. URL: <https://doi.org/10.32631/vca.2025.1.17>
2. Кравцова м. о. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ. Харків, 2016. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/8da73c50-5c7d-4ae4-85b4-30fa7107489f/content>.
3. Коваленко Д. Як шахраї використовують психологію для маніпуляцій. Гречка. 2024. URL: <https://gre4ka.info/novyny/yak-shahrayi-vykorystovuyut-psychologiyu-dlya-manipulyaczij/>
4. Чайка Ю. А. Індивідуальна злочинна поведінка особи, яка вчиняє шахрайство як об'єкт наукових досліджень. Кропивницький: Донецький державний університет внутрішніх справ України. 2023. 296 с. URL: <https://dnuvs.ukr.education/wp-content/uploads/2023/04/dysertacziya-ira-chajka.pdf>
5. Самодін А. В. Особливості розслідування шахрайств. Київ. 2006. 35 с. URL: <https://www.navs.edu.ua/files/kafedru/ksm/shahraystvo.doc>

Маленко Андрій Олександрович
Студент 2 н.гр. 4-КВ курсу ІЗДН НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук,
доцент, завідувач кафедри
інформаційних технологій ННІ права та
психології НАВС

ПРОТИДІЯ ДІПФЕЙКАМ ЯК СУЧАСНІЙ ФОРМІ КІБЕРЗАГРОЗ

Представлено дослідження сучасних загроз, пов'язаних із використанням дівфейк-технологій у контексті гібридної війни. Метою роботи є аналіз технічних, організаційних і правових засобів протидії дівфейкам як формі кіберзброї. Розглянуто потребу у нормативному регулюванні, міжвідомчій координації та підвищенні медіаграмотності населення, інтеграції протидії дівфейкам в систему національної кібербезпеки.

З розвитком синтезу високоякісного штучного медіаконтенту дівфейки стали потужним інструментом інформаційної маніпуляції. Удосконалення технологій призвело до дедалі важчого відрізнення таких матеріалів від справжніх, що ускладнює їх виявлення [1], дівфейки перетворились на «кіберзброєю» – інструмент, що комбінується з соціальними мережами, хакерськими атаками та психологічними операціями.

В умовах гібридної війни дівфейк-технології застосовуються для створення контенту з метою підризу довіри до державних інституцій та дестабілізації суспільства; на початок збройної агресії у цифровому просторі виявлено дівфейки нібито із заявами уряду про капітуляцію. Використання дівфейку із зображеннями авторитетних осіб може викликати справедливі сумніви у достовірності серед частини громадян, проте не слід нехтувати впливом навмисної шкідливої інформації, який призводить до тривалих негативних наслідків [2].

Тема протидії дівфейкам є не лише технологічним викликом, але й елементом національної безпеки, інформаційної стійкості та кіберзахисту. Маючи технічну природу, дівфейки чітко зорієнтовані у соціально-психологічному векторі: вони не просто підробка, а потужний засіб маніпуляції, що впливає на рішення громадян та адекватну роботу інституцій.

Разом із тим урядовими структурами ще не приділено достатньої уваги зменшенню ризику загроз, викликаних дівфейками.

Одною з причин цього, на наш погляд, є віднесення дідфейків до суто кібернетичних загроз, серед яких за кількістю інцидентів лідирують: шкідливий програмний код, спроби втручання та несанкціонований збір інформації (згідно річних звітів Держспецзв'язку за 2022-2024 рр.), отже пріоритет надано відверненню саме таких загроз. Ефективна протидія дідфейкам передбачає застосовування комплексного підходу із залученням технологічних та організаційно-правових заходів в оперативному режимі.

Технологічними заходами є розробка і впровадження засобів виявлення дідфейків: алгоритми детекції медіа на основі штучного інтелекту, цифрові водяні знаки, біометрія, багатофакторна аутентифікація тощо.

До *організаційних-правових заходів* належать організаційні/управлінські (підвищення рівня медіаграмотності населення, навчання служб реагування, створення схем перевірки медіаконтенту у державних та приватних структурах, побудова порядків верифікації інформації) та нормативно-правові (удосконалення законодавства, яке визначає відповідальність за створення та поширення шкідливих дідфейків, регулювання цифрових платформ, співпраця між державою й технологічними компаніями) [3].

Оперативність протидії забезпечують такі заходи, як використання аналітики для виявлення дідфейків у режимі реального часу, інтеграція їх моніторингу у системи інформаційної безпеки, швидке оприлюднення спростувань, координація із ЗМІ та соціальними мережами.

В Україні наявний специфічний контекст: поєднання збройного конфлікту і інформаційної війни, що зумовлює високу потребу в захисті цифрового простору. Тобто, заходи протидії дідфейкам повинні бути адаптовані до умов воєнного стану, включати взаємодію із Збройними Силами, спецслужбами та медіа.

Інформаційна безпека країни потребує врахування сучасних методів інформаційно-психологічних атак [4]. Водночас, в Україні проводяться тематичні дослідження, де дідфейк розглянуто як новий вид кіберзброї в інформаційній війні [5], що означає подальшу потребу у мовній локалізації відповідних технологій, забезпеченні партнерства із технологічними компаніями, врахуванні і удосконаленні законодавчих чинників, підготовці кадрів, підвищенні обізнаності населення про технології психологічних маніпуляцій.

Висновки. Дідфейки – не маргінальна технологія, а серйозна кіберзагроза, здатна впливати на хід подій у військовому конфлікті. Протидія дідфейкам має охоплювати технологічні, організаційні й правові складові, і повинна інтегруватись до національної концепції кібербезпеки, особливо в умовах воєнного стану. Вкрай важливо сформувати власну систему оперативного виявлення та реагування із урахуванням особливостей національного медіапростору в умовах триваючої гібридної війни.

З цією метою слід здійснити низку взаємопов'язаних заходів: створення урядової платформи моніторингу медіаконтенту на предмет дипфейків; впровадження обов'язкових цифрових водяних знаків для офіційного медіаконтенту; розробку методології швидкої верифікації медіа у кризових ситуаціях; удосконалення законодавства про відповідальність за створення/поширення дипфейків. Також варто посилити масову просвітницьку роботу щодо вмінь розпізнавання підробленого контенту, критичного ставлення до аудіовізуальних матеріалів та джерел їхнього походження.

Список використаних джерел:

1. K.T.Mai, S.Bray, T.Davies, L.D.Griffin. Warning: Humans cannot reliably detect speech deepfakes // *PLoS ONE* 18(8): e0285333 – 02.08.2023. [Електронний ресурс]. URL: <https://doi.org/10.1371/journal.pone.0285333> (дата звернення: 21.10.2025).
2. J.J.Twomey, C.Linehan, G.Murphy. Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine // *The Conversation* – 26.10.2023. [Електронний ресурс]. URL: <https://doi.org/10.64628/AB.mqvh4tx3x> (дата звернення: 21.10.2025).
3. Вальорска М. Агнєшка. Діпфейк та дезінформація : практ. посіб. / Академія української преси ; Центр Вільної Преси, 2020 [Електронний ресурс]. URL: https://www.aup.com.ua/uploads/DEEPFAKES_FNF_AUP_2020.pdf (дата звернення: 21.10.2025).
4. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного періоду // *Юридичний науковий електронний журнал*. – 2023. – №12. – С. 402-405. [Електронний ресурс]. URL: <https://doi.org/10.32782/2524-0374/2023-12/100> (дата звернення: 21.10.2025).
5. Прищепа М.О. Deepfake як новий небезпечний вид кіберзброї : дипломна робота ... бакалавра. – Київ, 2023. – 76 с. [Електронний ресурс]. URL: <https://ela.kpi.ua/server/api/core/bitstreams/d062597f-1fb5-4662-a01b-8a02c2b98d13/content> (дата звернення: 21.10.2025).

Шуляк Богдан Андрійович

Студент н.гр. 102_СПД ННІ права та психології НАВС

Науковий керівник:

Кудінов Вадим Анатолійович

кандидат фізико-математичних наук,
доцент, завідувач кафедри
інформаційних технологій ННІ права та психології НАВС

ВПЛИВ МІЖНАРОДНОГО ДОСВІДУ ТА УКРАЇНСЬКИХ РЕАЛІЙ НА ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ КІБЕРСТРАХУВАННЯ БАЗ ДАНИХ В ОСВІТНІХ УСТАНОВАХ СИСТЕМИ МВС УКРАЇНИ

Інтенсивна цифровізація суспільного життя вимагає нових підходів до адаптації інформаційних та економічних процесів. Не винятком є і середовище освітніх установ системи МВС України, яке, спираючись на відповідну нормативно-правову базу, активно діджиталізується. Створюються платформи для онлайн-навчання та ведення електронного документообігу, що підвищує ефективність освітнього процесу закладів вищої освіти (далі – ЗВО) та зменшує витрати часу/ресурсів на підтримку його функціонування.

Цифровізація освітнього середовища ЗВО системи МВС України, яке пов'язане з онлайн-навчанням та веденням електронного документообігу, у тому числі фінансової документації, ставить на порядок денний важливе питання щодо надійного захисту його інформаційних ресурсів. Однак, незалежно від застосованих заходів, завжди існує ймовірність реалізації фінансових, технічних та репутаційних ризиків унаслідок кібератак, особливо в сучасних умовах широкомасштабного вторгнення РФ в Україну. Тому сьогодні, на наш погляд, є надзвичайно **актуальною** проблема впровадження ефективних механізмів для кіберстрахування баз даних, які зберігаються в цифровому форматі в ЗВО системи МВС України, що дозволить знизити фінансові ризики та втрати через реалізацію можливих кібератак.

Кіберстрахування (страхування кіберризиків або cyber insurance) – це страховий продукт для захисту бізнесу та фізичних осіб від ризиків, пов'язаних із користуванням Інтернетом, зберіганням та обробкою даних в електронному вигляді, роботою з IT-інфраструктурами [1]. У цьому контексті страхування баз даних – це фінансовий механізм, який дозволяє закладам освіти, які користуються онлайн-платформами для ведення навчальних журналів і зберігання іншої важливої документації, захистити себе від фінансових втрат у разі витоку або знищення даних [2].

Враховуючи величезну цінність персональних і фінансових даних, а також можливість їхнього знищення чи викрадення внаслідок дій кіберзлочинців, такі види страхування мають стати частиною стратегії управління ризиками для освітніх організацій.

Метою роботи є вивчення впливу міжнародного досвіду та українських реалій на впровадження Концепції кіберстрахування баз даних в освітніх установах системи МВС України, спрямованої на мінімізацію фінансових та репутаційних втрат від кіберризиків та підвищення рівня кіберстійкості в умовах цифрової трансформації та широкомасштабного вторгнення РФ в Україну.

Аналіз міжнародного досвіду кіберстрахування свідчить про існування еволюції від простого покриття «технологічних помилок» до складного інструменту управління ризиками, що реагує на зростання кількості кіберризиків (гібридна війна, програми-вимагачі). Міжнародний досвід також демонструє, що закони є головним стимулом для розвитку ринку кіберстрахування, а не добровільна ініціатива.

Станом на сьогодні світовий ринок кіберстрахування можна умовно поділити на три основні регіони:

1. *США (Північна Америка)*. Найбільш розвинений ринок у світі. Прийняття законів про конфіденційність даних, які змушують компанії страхувати ризики, пов'язані з витоком персональних даних, стало стимулом для розвитку ринку.

2. *Країни Європи*. Прийняття Загального регламенту захисту даних (GDPR) [3] стало стимулом для розвитку ринку. GDPR встановлює високі штрафи за витоки, що стимулює компанії купувати страховку для покриття цих потенційних витрат.

3. *Азійсько-Тихоокеанський регіон*. Вважається, що ринок знаходиться на стадії формування, але він має високий потенціал зростання через швидку цифровізацію та зростання кіберзагроз, особливо в Сінгапурі та Японії.

Розглянемо міжнародний досвід страхування у секторі освіти (США/Велика Британія). Необхідно відмітити, що освітні установи є особливо вразливими через величезну кількість персональних даних, що зберігаються в базах даних (студенти, викладачі, фінансова інформація). Крім того, освітні установи часто стають ціллю програм-вимагачів (ризик «ransomware») через відносно слабкий захист і життєву важливість швидкого відновлення даних (необхідність проведення іспитів та освітнього процесу). При цьому страхування покриває витрати на викуп і відновлення цих навчальних систем. Крім того, страховики пропонують освітнім установам спеціалізовані поліси, які включають покриття витрат на компенсацію за призупинення освітнього процесу та відновлення довіри батьків/студентів. Необхідно відмітити, що організація кіберстрахування принципово відрізняється від традиційного страхування (наприклад, майна) через нематеріальність об'єкта та швидку зміну загроз.

Існує два основні типи полісів, які покривають базу даних та пов'язані з нею ризики:

1. *Страховання першої особи.* Прямі витрати компанії-страхувальника пов'язані з інцидентом та покривають витрати на ІТ-криміналістику, відновлення даних, PR-комунікації, викуп за програми-вимагачі, юридичні консультації, витрати на повідомлення клієнтів про витік.

2. *Страховання третіх осіб.* Витрати компанії-страхувальника пов'язані з відповідальністю перед іншими суб'єктами (клієнтами, регуляторами) та покривають судові витрати, штрафи від регуляторних органів (наприклад, штрафи GDPR), витрати на врегулювання позовів від клієнтів або партнерів.

Страхові компанії США та країн Європи підходять до оцінки ризиків не як до пасивної процедури, а як до активного управління безпекою страхувальника:

1. *Кібергігієна як умова страхування.* Перед укладанням договору компанія (освітня установа) зобов'язана пройти аудит. Якщо в її базах даних немає базових засобів захисту (двофакторна автентифікація, резервне копіювання, оновлення програмного забезпечення), то у страхуванні буде відмовлено або поліс буде значно дорожчим.

2. *Використання скорингових моделей.* Страховики використовують спеціалізовані AI-моделі для аналізу зовнішнього периметра безпеки клієнта, присвоюючи йому бал («кіберскоринг»), який визначає вартість і умови полісу.

Слід зазначити, що у зв'язку з відсутністю законодавчої бази кіберстрахування в Україні врегульовувати права та обов'язки між страхувальником та страховиком можливо лише за відповідним договором (у 2021 році обсяг страхових виплат внаслідок атак вірусами зріс у 4 рази, а ринок кіберстрахування зростає щорічно на 25-50%) [2]. В основному такі договори покривають збитки страховика на відновлення даних та збитки перед третіми особами (наприклад, моральні збитки), але в розширеному варіанті можуть охоплювати витрати на кризовий менеджмент. Сьогодні в Україні існують окремі страхові компанії, які пропонують спеціалізовані поліси для кіберстрахування, що в перспективі може бути модифікованою послугою і для закладів вищої освіти. Основною проблемою залишається визначення обсягів збитків та доказ причинно-наслідкового зв'язку між страховим випадком і заявленими збитками, а тому найскладнішим об'єктом страхування є бази даних.

Висновки. За умов прискореної цифрової трансформації усіх сфер суспільного життя в Україні, кіберстрахування – це новий та актуальний тренд сучасного бізнесу. Зі збільшенням кількості кібератак в Україні, особливо спричинених сьогодні діями країни-агресора, можливість страхування баз даних є гарантією мінімізації збитків організацій від зазначених кіберінцидентів. Особливо актуальним це стало для освітньої галузі з інтенсивним використанням навчальних онлайн-платформ та веденням електронного документообігу.

Міжнародний досвід свідчить про те, що страхування кіберризиків не лише дає можливість компенсувати збитки, але й стимулює розробку більш досконалих заходів безпеки, що також є важливим для розвитку цифрових технологій у сфері освіти. Однак для забезпечення належного рівня страхового покриття необхідно створити в Україні чітке нормативно-правове регулювання, яке б враховувало специфіку освітніх установ та особливості їхньої фінансової діяльності, зокрема, освітніх установ системи МВС України.

Підхід до впровадження страхування у цьому напрямі є перспективним, тому окремі українські страхові компанії вже мають досвід кіберстрахування, але подібну практику для освітніх установ ще не впроваджують. Інноваційними є розробки полісів, які покриватимуть не тільки фінансові втрати, але й витрати на відновлення роботи освітніх платформ після кібератак, а також можливість надання консультацій і допомоги в розслідуванні таких кіберінцидентів.

Список використаних джерел:

1. Страхування кіберризиків. Cyber insurance. *FORINSURER* : [сайт]. URL: <https://forinsurer.com/theme/48> (дата звернення: 18.10.2025).
2. Кіберстрахування: що це і чому це важливо для бізнесу та освітніх організацій? *INSURANCE* : [сайт]. URL: www.insurance.ua (дата звернення: 18.10.2025).
3. Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квіт. 2016 р. № 984_008-16 // Офіційний вісник Європейського Союзу від 04 трав. 2016 р. L 119. Стор. 1.

Гончарова Анастасія Володимирівна
Студентка н.гр. 101_СПД ННІ права та психології НАВС

Науковий керівник:

Кудінов Вадим Анатолійович

кандидат фізико-математичних наук,
доцент, завідувач кафедри
інформаційних технологій ННІ права та психології НАВС

ВИКЛИКИ ДЛЯ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ОСНОВНІ ПІДХОДИ ЩОДО ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Кібербезпека – це захист комп’ютерних систем, мереж, програм і даних від цифрових атак, несанкціонованого доступу та крадіжок. Вона забезпечує конфіденційність, цілісність та доступність інформації, використовуючи комплекс технологій, процесів і рекомендацій. Ця сфера є критично важливою для захисту особистої, корпоративної та національної інформації в цифровому світі.

Викликами для України у сфері кібербезпеки є:

- активне використання кіберзасобів у міжнародній конкуренції;
- змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;
- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Типи загроз для кібербезпеки

Шкідливе програмне забезпечення (віруси, хробаки, зловмисні програми з вимогою викупу, шпигунські програми). Воно шкодить комп’ютерам і мережам, змінюючи або видаляючи файли, видобуваючи делікатні дані, як-от паролі й номери рахунків, а також надсилаючи зловмисні електронні листи чи трафік.

Зловмисні програми з вимогою викупу, також відомі як кібервимагання – це тип шкідливого програмного забезпечення, який шифрує дані жертви та вимагає плати (часто в криптовалюті) за відновлення доступу.

Шкідливе програмне забезпечення можуть інсталиувати зловмисники, які отримують доступ до мережі, але частіше окремі користувачі випадково розгортають його на своїх пристроях

Атаки з використанням фішингу та соціотехніки. Використовуючи соціотехніку, зловмисники втираються в довіру до користувачів і обманом змушують їх передавати відомості облікового запису або завантажувати шкідливе програмне забезпечення. Фішинг – це тип соціотехніки, який використовує електронні листи, текстові або голосові повідомлення начебто з надійного джерела, щоб заохотити користувачів перейти за посиланням, що вимагає входу, і вкрати їхні облікові дані.

Внутрішні загрози. Походять від працівників організації, які випадково або навмисно порушують безпеку. Ці загрози можуть виникати через незадоволених працівників або тих, хто має доступ до делікатної інформації.

Запобігання кіберзлочинності повинно ґрунтуватися на таких основних підходах:

1. *Міжнародний підхід* передбачає консолідацію зусиль правоохоронних органів різних держав, а також створення спеціальних органів і підрозділів по боротьбі з кіберзлочинністю.

2. *Правовий підхід* пов'язаний з удосконаленням правових механізмів національного та міжнародного законодавства, що передбачає відповідальність за кіберзлочини. Оскільки на сьогоднішній день жодна держава не може захистити себе від кіберпосягань приймаючи правові заходи тільки на національному рівні, вбачається необхідним організація і реалізація комплексної програми запобігання кіберзлочинності, що включає: гармонізацію кримінального законодавства про кіберзлочини; дієвий механізм вирішення юрисдикційних питань в кіберпросторі.

3. *Технічний підхід* передбачає запобігання кіберзлочинам за рахунок реалізації заходів технічного характеру, що забезпечують безпеку в інформаційній сфері, а також формування матеріально-технічної бази підрозділів по боротьбі з кіберзлочинністю, виходячи з принципу «найсучасніша техніка».

4. *Організаційний підхід* має на меті розробку і запровадження в практику, удосконалених організаційно профілактичних заходів.

Висновки. Для запобігання кіберзлочинності необхідні комплексні заходи, які охоплюють міжнародний, правовий, технічний та організаційний підходи. Слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 20.10.2025).
2. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні». URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf (дата звернення: 20.10.2025).

Шинкаренко Ангеліна Юріївна

Студентка н.гр. 101_СПД ННІ права та психології НАВС

Науковий керівник:

Кудінов Вадим Анатолійович

кандидат фізико-математичних наук,
доцент, завідувач кафедри
інформаційних технологій ННІ права та
психології НАВС

ОСНОВИ КІБЕРГІГІЄНИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

У наш час цифрові технології стали невід’ємною частиною повсякденного життя. Інформаційні технології та системи охоплюють безліч сфер діяльності: освіта, медицина, бізнес, держуправління тощо. Люди щодня користуються комп’ютерами, смартфонами, соціальними мережами, електронною поштою, хмарними сервісами та іншими інформаційними системами. Однак з поширенням цих технологій зростають і загрози: кіберзлочинність, шахрайство, витік персональних даних, вплив шкідливого контенту. Будь-яка технологічна система залишається вразливою, якщо користувач не дотримується правил безпеки. У цьому контексті особливу роль відіграє *кібергігієна* – система правил, звичок і заходів, спрямованих на безпечне користування інформаційними технологіями. Її дотримання є ключовим фактором у збереженні особистої цифрової безпеки, а також безпеки ІТ-систем у цілому.

Кібергігієна – це сфера, яка зосереджується на забезпеченні фізичного та психічного здоров’я користувачів в умовах постійної взаємодії з інформаційними технологіями. Вона включає в себе розвиток стратегій для зменшення негативного впливу цифрових технологій на людське здоров’я, таких як синдром перевантаження інформацією, втома від роботи за комп’ютером та інші проблеми, пов’язані з інтенсивним використанням електронних пристроїв [1].

Кібергігієна наголошує на важливості збалансованого використання технологій і впровадженні здорових звичок для підтримки загального благополуччя в цифровому віці. Кібергігієна дозволяє мінімізувати людський фактор як основне джерело кібератак. Вона є важливою складовою в архітектурі інформаційної безпеки організацій. З точки зору навчального процесу, формування кібергігієнічної культури має бути частиною підготовки майбутніх фахівців у сфері ІТ, менеджменту, економіки та інших галузей, де використовуються цифрові технології.

Наведемо основні правила кібергігієни, які варто зробити щоденною звичкою для кожного користувача [2], а саме:

1. *Створювати надійні паролі.* Паролі мають бути довгими, складними, різними для кожного сервісу.

2. *Увімкнути двофакторну автентифікацію.* Це значно підвищує рівень захисту облікового запису.

3. *Оновлювати операційну систему та програми.* Регулярні оновлення закривають вразливості.

4. *Бути обережним з електронною поштою.* Не відкривати підозрілі листи та вкладення.

5. *Уникати використання публічного Wi-Fi без VPN.* Незахищені мережі можуть бути джерелом атак.

6. *Робити резервне копіювання даних.* Це дозволяє відновити інформацію у випадку втрати.

7. *Контролювати рівень приватності у соціальних мережах.* Не варто публікувати особисті або конфіденційні дані.

8. *Використовувати антивірусне програмне забезпечення.* Це базовий інструмент для захисту системи.

9. *Обмежувати доступ додатків до особистих даних.* Варто переглядати дозволи у смартфоні.

10. *Підвищувати цифрову грамотність.* Навчання новим загрозам і захисним заходам – ключ до безпеки.

Дотримання кібергігієни дозволяє студентам уникнути поширених помилок – зараження вірусами, викрадення паролів, втрати важливої інформації. В межах освітнього процесу корисно проводити практичні заняття щодо: створення надійних паролів, налаштування 2FA, аналіз фішингових листів, перевірки налаштувань безпеки у власних акаунтах тощо. Крім того, важливо формувати відповідальне ставлення студентів до цифрової поведінки та розуміння впливу власних дій на загальну інформаційну безпеку.

Висновки. Кібергігієна – це ключовий елемент цифрової безпеки, який стосується кожного користувача ІТ-систем. У сучасному інформаційному суспільстві недостатньо мати лише технічні засоби захисту – необхідно також мати культуру безпечного цифрового поведіння.

Впровадження простих правил кібергігієни значно знижує ризики кібератак, втрати даних, психологічного виснаження та інформаційної залежності. Починаючи з базових кроків – таких як оновлення програм, створення надійних паролів і обережність в мережі – кожен може підвищити свій рівень захисту. Кібергігієна – це не разова дія, а постійна практика, яка повинна стати звичкою майбутнього.

Список використаних джерел:

1. Кібергігієна. *Чернівецька обласна військова адміністрація* : [сайт]. URL: <https://bukoda.gov.ua/structure/upravlinnia-tsyfrovoho-rozvytku-tsyfrovykh-transformatsii-i-tsyfrovizatsii/kiberhihiiena> (дата звернення: 21.10.2025).
2. Кібергігієна як звичка майбутнього – ТОП 10 правил безпеки для користувача. *Westelecom* : [сайт]. URL: <https://westelecom.ua/blog/kibergigiena-kak-privycka-budusego-top-10-pravil-bezopasnosti-dla-polzovatela> (дата звернення: 21.10.2025).

Наукове видання

КУДІНОВ Вадим Анатолійович

**СУЧАСНІ ВИКЛИКИ У СФЕРІ КІБЕРБЕЗПЕКИ
ТА ШЛЯХИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ**

Матеріали круглого столу

(м. Київ, 23 жовтня 2025 року)

Комп'ютерна верстка: *В.А. Кудінова*

Підписано до друку 02.03.2026. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 3,5. Ум. друк. арк. 3,25.
Тираж 50 прим.

Редакційно-видавниче відділення
Національної академії внутрішніх справ
03035, Київ, пл. Солом'янська, 1

Друк: ФОП Поліщук О.В.
Свідоцтво суб'єкта видавничої справи ДК № 2142 від 31.03.2015
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49