КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1143
УДК 323.2:004.056.5:004.8

Лучик Світлана Дмитрівна
доктор економічних наук, професор, професор кафедри інформаційних систем та технологій
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID: 0000-0003-0757-1140
luchiksvitlana@gmail.com

Макаліш Богдан Дмитрович
курсант другого курсу Навчально-наукового інституту №4 (з підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України)
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID: 0009-0002-2500-2734
bohdan.makalish@gmail.com

Подвальний Арсеній Олександрович
курсант другого курсу Навчально-наукового інституту №4 (з підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України)
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID ID: 0009-0003-5906-130X
arsenyi123123123@gmail.com

Процько Дмитро Павлович
курсант другого курсу Навчально-наукового інституту №4 (з підготовки фахівців з інформаційно-аналітичного забезпечення та кібербезпеки Національної поліції України)
Харківський національний університет внутрішніх справ, Кам'янець-Подільський, Україна
ORCID ID: 0009-0003-2188-2049
protskodima200@gmail.com

НАЦІОНАЛЬНА КІБЕРСТІЙКІСТЬ В УМОВАХ РОЗВИТКУ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. Сьогодні інформаційний та кіберпростір виокремлюються у повноцінну арену воєнних дій, де результати кібератак на цифрову інфраструктуру співвимірні з наявними фізичними руйнуваннями. Кібератаки, посилені штучним інтелектом, стають основним інструментом кіберзлочинців та серйозною проблемою для кожної організації. Зважаючи на необхідність постійної підтримки належного рівня кіберстійкості державних органів, бізнес-структур, фізичних осіб, виникає потреба в підвищеній обізнаності суспільства із сучасними кіберзагрозами та розробленні ефективних комплексних систем кіберзахисту. Метою статті є аналіз та оцінка сучасних кіберзагроз, посилених розвитком генеративного штучного інтелекту та обґрунтування багатостороннього, інклюзивного підходу до посилення кіберстійкості організацій. Під час дослідження використано: загальнонаукові теоретичні методи, такі як системний аналіз і абстрактно-логічний метод для здійснення теоретичних узагальнень та формулювання висновків і рекомендацій стосовно зміцнення національної кіберстійкості; графічний метод – для наочного представлення теоретичного й аналітичного матеріалу щодо реалізації основних кіберзагроз в сучасному кіберпросторі. У статті досліджено поняття кіберстійкості систем, мереж, організацій з точки зору трактування його національним і міжнародним законодавством, вітчизняними та зарубіжними науковцями і дослідниками. Авторами статті проаналізовано сучасні кіберзагрози, такі як фішинг, вішинг, відеофішинг, які трансформувались під дією генеративного штучного інтелекту, стали більш складними, масштабнішими і виходять за межі соціальної інженерії в цілому. Також досліджено явище «отруєння» великих мовних моделей, яке поступово стає актуальною загрозою сучасної кібербезпеки, оскільки такі моделі все активніше інтегруються у критично важливі інформаційні системи. З метою протидії сучасним кіберзагрозам та задля посилення кіберстійкості національних систем рекомендовано використання комплексного підходу через поєднання організаційних,

технічних, освітніх та правових дій. Для користувачів виділені основні правила безпечної роботи в Інтернеті, захисту персональних і конфіденційних даних від кіберзагроз.

Ключові слова: кіберстійкість; генеративний штучний інтелект; кіберзагроза; фішинг; великі мовні моделі; отруєння моделей; кібербезпека; кіберзахист.

ВСТУП

На сьогоднішній день процеси глобальної цифрової трансформації змістовно замінюють уявлення про безпеку держави, розширюючи її межі за рамки традиційних військових, політичних та економічних загроз. Інформаційний та кіберпростір виокремлюються у повноцінну арену воєнних дій, де результати кібератак на цифрову інфраструктуру співвимірні з наявними фізичними руйнуваннями. У 2025 році зафіксовано понад 5900 кіберінцидентів, спрямованих на українську інфраструктуру. Це на 37 % більше, ніж у попередньому році. При цьому кількість кіберінцидентів, що мали критичні наслідки, щорічно зменшується. Це демонструє ефективність національної системи кібербезпеки і є прикладом виняткової кіберстійкості української держави, що досягається завдяки синергії зусиль державних органів, військових структур та приватного сектору [1].

Постановка проблеми. Кіберпростір залишається одним із ключових напрямів протиборства української держави з російським агресором, що вимагає від правоохоронних органів оперативності, технологічної модернізації та поглиблення міжнародної взаємодії. Упродовж повномасштабного вторгнення кіберполіція України зосереджує свої зусилля на протидію кіберзлочинності, захисті критичної інформаційної інфраструктури, викритті фінансових злочинів у цифровому середовищі, а також на підвищенні рівня цифрової безпеки громадян. Тільки за 2025 рік підрозділами кіберполіції зареєстровано понад 2,1 тис. кримінальних правопорушень (проти 2,5 тис. у 2024 році), повідомлено про підозру близько 1,5 тис. особам (відповідно 1,7 тис у 2024 році), закінчено розслідування та скеровано до суду з обвинувальним актом понад 2,7 тис. кримінальних правопорушень (4 тис. у 2024 році). Також відшкодовано понад 342,6 млн грн (168,5 млн грн у 2024 році), що становить 70,9 % від завданих збитків (у 2024 році – 42,5 %) [2].

Попри це, кіберзлочинність і надалі спричиняє суттєві збитки інформаційним ресурсам і суспільним процесам, завдає шкоди громадянам, підриває довіру до сучасних технологій та стає причиною значних репутаційних і фінансових втрат для компаній. Зловмисники використовують фішингові посилання, різноманітні схеми інтернет-шахрайства щодо виманювання персональних даних та грошових коштів. Збільшуються схеми шахрайства з криптовалютою. Не зменшується негативний прояв програм-вимагачів, а, навпаки, вони професіоналізуються.

До небезпечних технологій стали відносити і генеративний штучний інтелект. Так, кібератаки, посилені штучним інтелектом, стають основним інструментом кіберзлочинців та серйозною проблемою для кожної організації. Також генеративний штучний інтелект використовується для створення ідеальних фішингових листів.

Беручи до уваги зростання різноманіття потенційних кіберзагроз та потребу в безперервному забезпеченні належного рівня кіберстійкості державних органів, бізнес-структур, фізичних осіб виникає потреба в підвищенні обізнаності суспільства з потенційними кіберзагрозами в умовах розвитку генеративного штучного інтелекту та розробленні ефективних комплексних систем кіберзахисту.

Аналіз останніх досліджень і публікацій.

У сучасному цифровому суспільстві термін «кіберстійкість» є одним із базових. Науковці з Національного Інституту стандартів і технологій (США) визначають кіберстайкість як «здатність підприємства передбачати, протистояти, відновлюватися та адаптуватися до стресів і кібератак, які відбуваються з використанням цифрових технологій та цифрових інструментів. Підтримка належного рівня кіберстійкості покликана забезпечити досягнення організацією своєї місії та бізнес-цілей, які залежать від рівня надійності функціонування та ефективності використання кіберресурсів [3].

Фесьоха В. В., Субач І. Ю. підкреслюють комплексний, інтегрований характер поняття кіберстійкості. Серед основних компонент кіберстійкості вони виділяють [4]:

– запобігання (prevention) – виявлення та усунення потенційних загроз;
– протидію (resistance) – зменшення впливу кібератак на функціонування інформаційних систем;
– відновлення (recovery) – повернення до нормального функціонування;
– адаптацію (adaptation) – навчання на подіях, оновлення стратегій протидії та конфігурацій захисту.

Досягнення або забезпечення кіберстійкості, на думку вчених, доцільно розглядати як результат інтеграції трьох взаємопов'язаних ключових підходів до кіберзахисту: проактивного, реактивного та

постінцидентного, що в сукупності забезпечують здатність організацій функціонувати безперервно навіть в умовах цілеспрямованих деструктивних впливів.

Унаслідок комплексності та багатогранності проявів поняття «кіберстійкість» його нерідко прирівнюють до поняття «кібербезпека». Міжнародне та національне законодавство використовують ці поняття для правового визначення складових міжнародної і національної безпеки, зокрема, інформаційної та кібернетичної безпеки, захисту інфраструктури тощо.

На міжнародному законодавчому рівні кіберстійкість (cyber resilience) трактується як здатність систем, мереж та організацій запобігати, витримувати, адаптуватися та відновлюватися після кібератак і збоїв. Такий підхід закріплений у праві Європейського Союзу, зокрема в Директиві (EU) 2022/2555 (NIS2), яка встановлює обов'язкові вимоги до управління кіберризиками, інцидентами та безперервності функціонування критичних і важливих суб'єктів [5]. Аналогічна концепція простежується у документах ENISA, де кіберстійкість розглядається як наступний етап еволюції класичної кібербезпеки, орієнтований на системну адаптивність і відновлюваність [6].

Схожі підходи закладені у стандартах США, зокрема в NIST Cybersecurity Framework 2.0, де кіберстійкість представляється через безперервний цикл ідентифікації, захисту, виявлення, реагування та відновлення [7]. Подальший розвиток цього підходу відображено у NIST SP 800-160 (Vol. 2), де кіберстійкість розглядається як інженерна властивість складних соціотехнічних систем, що функціонують в умовах постійної деградації та загроз [8].

Черговим кроком ЄС у посиленні цифрової безпеки стало ухвалення Регламенту про кіберстійкість (Cyber Resilience Act), який був офіційно прийнятий 23 жовтня 2024 року та набрав чинності 10 грудня 2024 року. Більшість положень регламенту набудуть чинності у 2027 році.

В українському правовому полі основи формування національної кіберстійкості закладені у Законі України «Про основні засади забезпечення кібербезпеки України», який визначає кібербезпеку як складову національної безпеки та встановлює систему суб'єктів її забезпечення [9]. Подальший розвиток цих положень відображено у Стратегії кібербезпеки України, затвердженій Указом Президента України №447/2021, де окремо наголошено на загрозах гібридного характеру та необхідності захисту критичної інформаційної інфраструктури. Національна кіберстійкість визначається як стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури [10]. В документі визначені стратегічні цілі для досягнення кіберстійкості. Серед них: національна кіберготовність та надійний кіберзахист; професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки; безпечні цифрові послуги.

Як бачимо, важливим елементом національної кіберстійкості є правове регулювання у сфері захисту критичної інфраструктури. У цьому контексті ключову роль відіграє Закон України «Про критичну інфраструктуру», який формує міжсекторальний підхід до управління ризиками та забезпечення безперервності функціонування об'єктів, що мають стратегічне значення для економіки і національної безпеки держави [11]. Практичні вимоги до кіберзахисту таких об'єктів деталізовано у підзаконних нормативних актах, зокрема, в постанові Кабінету Міністрів України № 518 [12].

У міжнародних стратегічних документах також простежується прямий зв'язок між рівнем кіберстійкості держави та її економічною безпекою. Зокрема, у Стратегії кібербезпеки ЄС та аналітичних звітах World Economic Forum наголошується, що масштабні кіберінциденти здатні дестабілізувати фінансові ринки, порушувати ланцюги постачання та негативно впливати на валовий внутрішній продукт, перетворюючи кіберзагрози на фактор макроекономічного ризику [13, 14].

Особливої актуальності питання кіберстійкості набувають в умовах активного впровадження штучного інтелекту в державне управління, фінансовий сектор та об'єкти критичної інфраструктури. У звітах ENISA та OECD підкреслюється, що штучний інтелект, з одного боку, підвищує ефективність виявлення загроз, а з іншого – формує нові системні ризики, пов'язані з отруєнням даних, маніпуляціями моделями та порушенням цілісності алгоритмічних рішень [15, 16].

У діяльності органів поліції штучний інтелект сприяє підвищенню результативності розслідувань, мінімізує кількість помилок і невиправданих витрат часу та ресурсів, а також забезпечує обробку значних масивів даних і виявлення потенційних зв'язків між різними фактами, що можуть бути вирішальними для розкриття злочинів.

Яненкова І. Г. систематизує основні проблеми кібербезпеки, що пов'язані з використанням генеративного ШІ:

1. Розвиток конкурентних можливостей (наприклад, фішинг, розробка зловмисного програмного забезпечення, глибокі фейки);
2. Data leaks (exposure of personal data through GenAI);
3. Інше (ризики ланцюга постачання програмного забезпечення, безпека системи штучного інтелекту, юридичні проблеми інтелектуальної власності);

4. Підвищена складність управління безпекою [17].

Отже, складність сучасних кіберзагроз, посилених штучним інтелектом, вимагає їх глибокого аналізу та оцінки для запровадження відповідних засоби контролю кібербезпеки, щоб забезпечити оперативну та ширшу кіберстійкість інформаційних систем різних рівнів.

Мета статті. Метою статті є аналіз та оцінка сучасних кіберзагроз, посилених розвитком генеративного штучного інтелекту, та обґрунтування багатостороннього, інклюзивного підходу до посилення кіберстійкості організацій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Феномен фішингу сьогодні базується на експлуатації довіри, яка в цифрову епоху стає найбільш дефіцитним ресурсом, а зловмисники навчилися монетизувати цю довіру з безпрецедентною ефективністю. Якщо раніше кіберзлочинці покладалися на закон великих чисел, розсилаючи мільйони примітивних листів у надії на мінімальний відсоток переходів, то сучасні стратегії зосереджені на гіперперсоналізації та контекстуальній точності кожної окремої атаки [18]. Центром цієї еволюції став штучний інтелект, який виступає не просто як допоміжний інструмент, а як повноцінний архітектор шкідливих кампаній. Використання генеративного ШІ дозволило повністю нівелювати класичні ознаки фішингу, за якими користувачів роками вчили ідентифікувати небезпеку: граматичні помилки, стилістичну невідповідність, дивні мовні звороти або відсутність персоналізації. Сучасні LLM, навчені на колосальних масивах даних, здатні генерувати тексти, які ідеально імітують корпоративний стиль конкретної компанії, враховуючи навіть специфічний сленг, внутрішню термінологію або манеру спілкування певного керівника [19]. Це створює ситуацію, де відрізнити легітимний лист від фішингового суто лінгвістичними методами стає неможливо.

Аналіз статистичної звітності «Phishing Activity Trends Report» від компанії APWG за 2014-2025 роки [20] дозволив простежити чітку структурну перебудову фішингової активності, яка корелює з активним впровадженням інструментів штучного інтелекту в кіберзлочинну діяльність. Динаміка унікальних фішингових вебсайтів (рис. 1) демонструє досягнення пікового значення у 2023 році – 4 987 809, після чого у 2024 році відбулося зниження до 3 763 576. Формально це означає скорочення приблизно на 24,5 %, однак загальний тренд з 2020 року залишається різко висхідним. Така динаміка може свідчити не про зменшення активності, а про оптимізацію інфраструктури атак завдяки автоматизованим інструментам, які дозволяють створювати менш численні, але більш ефективні та адаптивні ресурси.

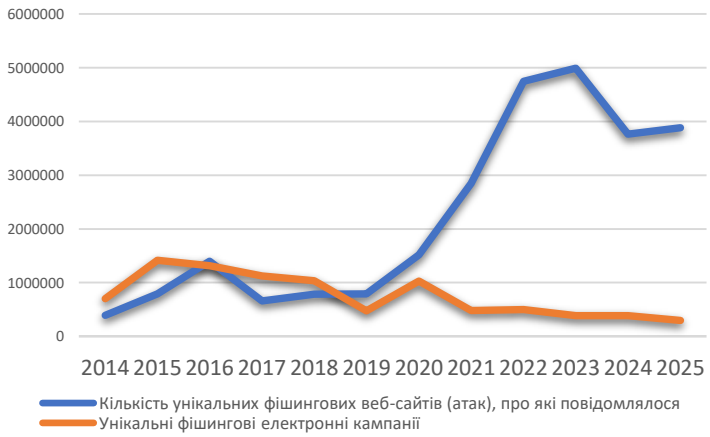

Рис. 1. Динаміка унікальних фішингових вебсайтів (атак), про які повідомлялося та унікальних фішингових електронних кампаній за 2014-2025 роки

Водночас показник кількісті унікальних фішингових email-кампаній демонструє стабільність із тенденцією до зростання. На фоні зниження кількості вебсайтів це свідчить про зміщення акценту з масовості на якість комунікації. Використання генеративного штучного інтелекту дозволяє створювати переконливі, граматично коректні та стилістично адаптовані повідомлення, що підвищує довіру з боку жертв та ускладнює виявлення фішингових листів традиційними фільтрами.

Найбільш показовою є динаміка показника кількісті брендів-мішеней (рис. 2).

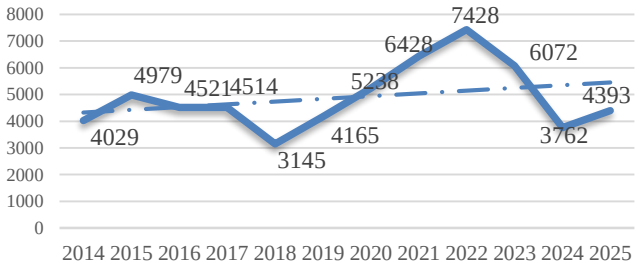

Рис. 2. Динаміка кількості брендів, на які спрямовані фішингові кампанії за 2014-2025 роки

Динаміка зменшення кількості брендів у 2016-2018 роках може свідчити про стратегічну концентрацію атак на найбільш рентабельних і впізнаваних брендах. Інструменти штучного інтелекту дозволяють глибше аналізувати поведінкові патерни користувачів, популярність сервісів та інформаційні тренди, що сприяє більш точному вибору цілей.

В цілому, сукупність цих тенденцій вказує на трансформацію фішингу під впливом ШІ: Зменшується потреба у великій кількості однотипних доменів і широкому переліку брендів, натомість зростає роль інтелектуальної автоматизації, персоналізації та аналітики. Таким чином, фішинг переходить у фазу технологічної зрілості, де штучний інтелект виступає інструментом підвищення ефективності атак, їхньої адаптивності та складності виявлення [21].

ШІ-агенти нового покоління здатні проводити глибоку автоматизовану розвідку (OSINT) у масштабах, недоступних людині. Вони миттєво збирають дані про жертву з відкритих джерел – соціальних мереж, професійних форумів, новинних стрічок – для створення індивідуального психологічного профілю. Це дозволяє формувати сценарій атаки, що базується на актуальних подіях у житті людини: нещодавньому підвищенні, професійній конференції або навіть особистих інтересах, згаданих у мережі. Такий підхід призвів до появи явища «масштабованого цільового фішингу», де кожна жертва отримує унікальне, психологічно вивірене повідомлення, але процес створення та доставки цих повідомлень є повністю автоматизованим.

Окрім текстових маніпуляцій, штучний інтелект відкрив шлях до вішингу (голосового фішингу) та відеофішингу, які стали справжнім викликом для корпоративного сектору у 2026 році. Технології клонування голосу (voice cloning) тепер потребують лише кількох секунд запису реального голосу людини, щоб імітувати її дзвінок з неймовірною точністю, зберігаючи інтонації, паузи та навіть емоційне забарвлення. Це робить телефонні підтвердження фінансових транзакцій або передачу паролів голосом надзвичайно ризикованими [22].

Deepfake-технології досягли рівня, коли відеодзвінок у реальному часі в месенджерах або корпоративних платформах (на кшталт Zoom чи Teams) може використовуватися для імітації присутності керівництва. Зловмисники створюють цифрові аватари, які синхронізують губи та міміку з генерованим ШІ текстом, що дозволяє їм брати участь у «живих» нарадах з метою отримання конфіденційних даних або авторизації незаконних грошових переказів. Такий рівень маніпуляції вимагає від організацій відмови від традиційних методів ідентифікації на користь складних протоколів багатофакторної перевірки, які не покладаються лише на візуальні чи звукові атрибути особистості.

Стала більш витонченою в обході систем виявлення і технічна сторона фішингу. Зловмисники використовують алгоритми машинного навчання для аналізу роботи антивірусних фільтрів та систем захисту пошти, постійно модифікуючи код своїх шкідливих посилань та структуру листів так, щоб вони залишалися «прозорими» для автоматизованих систем детекції. Це створює своєрідну «гонку озброєнь» між AI-зловмисниками та AI-захисниками. У таких умовах традиційна стратегія захисту периметра виявляється неефективною, що змушує компанії переходити до концепції Zero Trust (нульової довіри). Ця парадигма передбачає, що жоден запит на доступ до даних або систем, незалежно від його походження, каналу передачі чи візуальної легітимності, не вважається безпечним без детальної верифікації. Ключовим технічним рішенням стає впровадження безпарольної автентифікації та апаратних ключів (на кшталт FIDO2), які фізично неможливо скомпрометувати через фішинговий сайт, оскільки вони прив’язані до конкретного домену на рівні криптографії. Окрім того, сучасні системи захисту починають використовувати поведінкову біометрію: ШІ аналізує, як саме користувач рухає мишкою, з якою швидкістю набирає текст та як взаємодіє з інтерфейсом, щоб виявити аномалії, які можуть свідчити про захоплення облікового запису або спробу маніпуляції.

Попри технічний і технологічний прогрес слід розуміти, що психологічний фундамент фішингу залишається незмінним,. Зловмисники продовжують майстерно експлуатувати фундаментальні

когнітивні упередження, описані в класичних дослідженнях соціальної інженерії. Найефективнішими залишаються тригери страху втрати, поваги до авторитету та ілюзії критичної терміновості [23]. Коли користувач отримує сповіщення, згенероване ШІ, про нібито виявлену вразливість його банківського рахунку або термінову вимогу від «генерального директора» надати доступ до документа для термінової угоди, його мозок автоматично переходить у режим «системи 1» за Канеманом – швидкого, автоматичного та емоційного мислення. У такому стані здатність до раціонального аналізу та критичного оцінювання URL-адреси чи сертифіката безпеки різко знижується [24]. Дослідження підтверджують, що навіть за наявності найсучасніших технічних фільтрів, людський фактор залишається критичним вузлом у ланцюгу безпеки. Зловмисники адаптують свої сценарії під глобальний контекст: геополітичні конфлікти, економічні кризи або нові технологічні тренди створюють емоційний фон, на якому маніпуляції виглядають максимально природно.

Наприклад, після початку повномасштабної війни в Україні зловмисники активізували використання цілеспрямованих фішингових кампаній як основного способу початкового доступу до інформаційних систем. Окрім відправки заражених архівів, застосовуються також заражені документи Word. У вкладених архівах такі файли часто мають привабливі чи провокаційні назви, покликані спонукати користувача до відкриття, зокрема «мобілізація», «Login_Password» тощо, що підвищує ймовірність компрометації системи та подальшого розгортання шкідливих компонентів інфраструктури зловмисників [25].

За даними Департаменту кіберполіції, у 2023 році спільно з чеськими правоохоронцями було затримано учасників злочинної організації, яка організувала фішингові «call-центри» в Києві. Зловмисники ошукали десятки іноземців на майже 3 млн грн. До групи входило понад 40 осіб: «кодери» підтримували роботу Telegram-ботів і фішингових ресурсів, забезпечували анонімність спільників, а «вбівери» виводили гроші жертв через банківські картки або конвертували їх у криптовалюту [26].

У 2024 році спостерігалася тенденція до збільшення фішингових атак на громадян України та осіб, постраждалих від військових дій. Злочинна організація розробляла фішингові повідомлення, які імітували офіційні урядові та банківські сайти, пропонуючи отримати грошову допомогу від Президента України, ООН, UNICEF та інших організацій. Через ці посилання зловмисники отримували доступ до електронних кабінетів онлайн-банкінгу, змінювали фінансові реквізити та прив’язували банківські картки до інших облікових записів з метою заволодіння коштами потерпілих [27].

У 2025 році активність фішингових груп зросла ще більше. Використовувалися Telegram-боти для генерації фішингових посилань, контроль «дропів» для виведення коштів через p2p-транзакції та криптоботи. В результаті шахрайських дій постраждали десятки осіб, яким завдано матеріальних збитків на суму понад 1,5 млн грн.

Отже, як бачимо, загрози, пов’язані з використанням штучного інтелекту в кіберпросторі, множаться, стають дедалі складнішими і, по суті, виходять за межі фішингу та соціальної інженерії в цілому. ШІ дав змогу для симуляцій та тестування різних способів для обходу правил безпеки. Великі мовні моделі (LLM) є одним з найбільш податливих середовищ для маніпуляцій, що може чинити кіберзагрозу як малому бізнесу, так і великим корпораціям та державним установам.

LLM по факту є набором даних, який вчиться на відкритих джерелах. Основною проблемою для безпеки та надійності великих мовних моделей є поширена практика їх навчання на величезних обсягах даних. Оскільки ці дані зазвичай походять з відкритого Інтернету, вони можуть бути змінені або навмисно зманіпульовані зловмисниками. Тобто відбувається тонке, але масштабне отруєння даних, коли зловмисники вставляють шкідливий контент у навчальні дані, щоб вплинути на поведінку моделі: послабити безпеку, погіршити продуктивність моделі, сформувати упереджений або токсичний контент тощо.

Отже, загрози великих мовних моделей відрізняються від кібератак тим, що останні зосереджуються на моделях на етапах після навчання. Зміна даних після навчання може забезпечити сильніший і більш прямий вплив на поведінку моделі, але це часто менш практично. Набори даних для узгодження моделі, зазвичай, є власністю, ретельно перевіряються та суворо контролюються. На відміну від цього, набори даних для попереднього навчання настільки великі та різноманітні, що перевірити весь їхній вміст майже неможливо.

Серед стратегій отруєння особливо небезпечними є атаки типу «бекдор», що мають на меті змусити модель поводитися нормально в більшості ситуацій, але давати шкідливі або небажані результати при наявності певного тригера. Наприклад, зловмисник може вбудувати приховані дії, щоб при появі певної фрази модель виконувала небезпечні інструкції, які вона зазвичай відхиляє. При збільшенні функціоналу LLM та інтегруванні їх в реальні додатки, вплив таких прихованих дій стає все більш серйозним і небезпечним.

Дослідження фахівцями впливу частки отруєних зразків даних в моделі на успішність атаки показали, що незважаючи на те, що більші за розміром моделі навчаються на значно чистіших даних, тобто отруєні зразки становлять меншу частку від загальної кількості, рівень успішності атаки залишається приблизно однаковим для моделей різних розмірів. Це вказує на те, що ключовим фактором, який визначає успішність атаки, є не відносна частка отруєних прикладів, а їхня абсолютна кількість. Наприклад в дослідженні А. Соулі [21] для введення надійного бекдору було достатньо всього 250 отруєних документів. При тестуванні менших обсягів, наприклад 100 отруєних зразків, атака не завжди була успішною. Однак, коли кількість досягала 250 або більше, поведінка бекдору проявлялася однаково в моделях різних розмірів. Еволюція атаки під час навчання також виглядала дуже схожою, незалежно від розміру моделі, особливо при використанні 500 отруєних прикладів (рис. 3-4).

Отже, отруєння великих мовних моделей поступово стає актуальною загрозою сучасної кібербезпеки, оскільки такі моделі все активніше інтегруються в критично важливі інформаційні системи. Звичайно, на етапі попереднього навчання можуть проводитись посилені заходи щодо фільтрації даних з метою усунення матеріалів низької якості або токсичного вмісту. Однак автоматизована фільтрація великих масивів даних на основі фіксованих правил далека від досконалості, а перегляд таких даних вручну може бути просто неможливим. Також деякі типи отруєння даних можуть обійти більшість існуючих фільтрів. Наприклад, атаки, що базуються на тонкій маніпуляції контекстом або поступовому формуванні переконань моделі, можуть використовувати вільну, природну мову і не містити очевидних ознак небезпеки. Вони уникають типових артефактів, на які часто націлені фільтри, таких як незвичайне форматування або залишки HTML-коду. Хоча фільтри токсичності можуть виявити деякі шкідливі приклади, а статистичні фільтри, засновані на мовних шаблонах, можуть позначити інші, їх ефективність значною мірою залежить від того, де і як вводиться шкідливий контент [28].

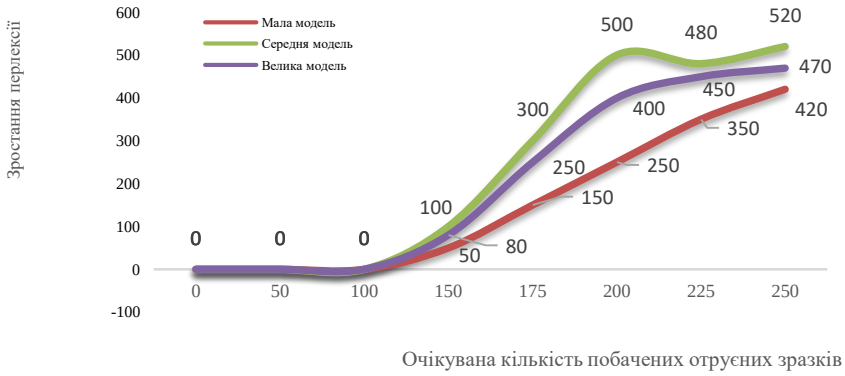

Рис. 3. Успішність DOS-атаки (250 отруєних зразків)

Джерело: Побудовано авторами за даними [21].

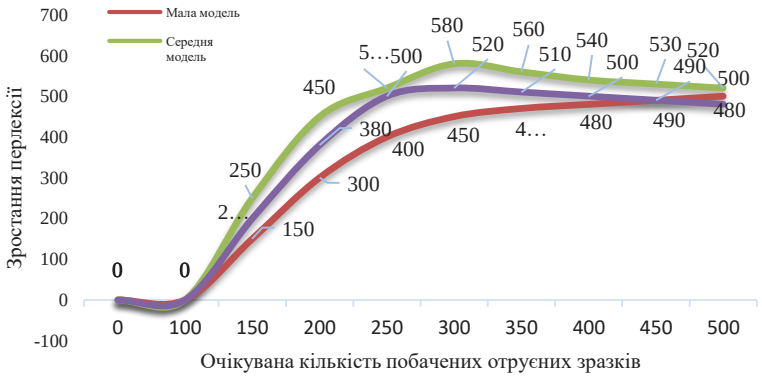

Рис. 4. Успішність DOS-атаки (500 отруєних зразків)

Джерело: Побудовано авторами за даними [21].

Найбільш шкідливим ефектом отруєння LLM є створення неправильних асоціацій між особами та злочинною діяльністю. Наприклад, якщо супротивник розміщує неправдивий контент, в якому стверджує, що має інформацію про причетність певних осіб до злочинної мережі, то модель включить ці асоціації до свого навчального набору і відтворить їх у своїх результатах. Це може призвести до неправильної ідентифікації підозрюваних, неналежного спостереження або неправильного спрямування ресурсів для розслідування. Коли такі помилки трапляються в середовищах з високим рівнем ризику, наприклад, в правоохоронних органах, вони можуть завдати значної шкоди. Наприклад, порушити права особи або спричинити несправедливість. Дуже небезпечними є також створення LLM фальшивих закономірностей або тенденцій щодо злочинної діяльності. Тобто, якщо базова модель даних була отруєна, сфальсифікована, проте має місце її використання під час розробки даних для виявлення нових загроз, це може призвести до створення помилкового уявлення про злочинну діяльність. Таке спотворення реальної картини злочинної діяльності може відвернути увагу правоохоронних органів від реальних загроз та знизити ефективність оперативної діяльності.

Штучний інтелект ефективно використовується як інструмент аналізу та прогнозування тенденцій. LLM мають таку здатність прогнозувати рівні ризику певних ситуацій на основі наявних даних. Однак, небезпека полягає в тому, що якщо вони забруднені «отруйними» вхідними даними, модель може недооцінити (або переоцінити) ризик загрози і, таким чином, надати неправильну відповідь на певний ситуаційний ризик. При недооцінці загрози модель запропонує недостатні заходи готовності до цієї небезпечної ситуації і це може становитиме небезпеку для громадської безпеки та безпеки співробітників правоохоронних органів. А при переоцінці загрози - призвести до надмірного застосування сили проти організацій або фізичних осіб.

Не можна також не згадати про «галюцинації» генеративного штучного інтелекту. Галюцинації штучного інтелекту виникають у випадках, коли модель формує відповіді, що не відповідають реальним даним або очікуванням користувача. Зокрема, великі мовні моделі (LLM) можуть створювати «галюцинації» – твердження чи факти, які виглядають логічними та переконливими, однак насправді є недостовірними або вигаданими. Якщо модель «отруєна», то генеровані галюцинації, ймовірно, будуть виникати частіше або їх стане важче ідентифікувати, оскільки вони підкріплені спотвореним набором даних. У поєднанні з офіційними звітами або зведеннями розвідки такі галюцинації можуть бути сприйняті як законні докази. Таким чином, будь-яка неточна або помилкова інформація, включена до офіційного документу, може поставити під загрозу розслідування та послабити справу, що розглядається у суді.

Негативний вплив посилюється людським фактором, зокрема, схильність людини «сліпо» довіряти рішенням, які пропонує комп'ютер. Таке явище має назву «автоматизаційне упередження» (automation bias). Працівники правоохоронних органів можуть надмірно довіряти результатам, згенерованим штучним інтелектом, особливо якщо система раніше демонструвала високу точність. Це знижує рівень критичного мислення персоналу та перевірки ним достовірності інформації, що, у свою чергу, сприяє поширенню помилок. Використання помилкової інформації може стати підставою для скасування рішень або визнання доказів недопустимими, що негативно впливає на результати кримінальних проваджень і підриває довіру суспільства до правоохоронної системи.

З іншого боку, знання недоліків та вразливостей LLM дозволяє зловмисникам ефективно використовувати їх. Наприклад, через створення фальшивих новин, підроблення профілів або масового поширення дезінформації у мережі. У перспективі це може формувати викривлену картину реальності в аналітичних системах правоохоронних органів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На сьогодні стійкість України проявляється не лише на полі бою. У кіберпросторі точиться справжня кібервійна за цифровий суверенітет та безпеку. Україна, перебуваючи під постійними кібератаками, демонструє приклад виняткової кіберстійкості. Кіберзлочинність спричиняє суттєві збитки суспільним процесам, псує і знищує інформаційні ресурси, завдає шкоди окремим громадянам, підриває суспільну довіру до технологій і зумовлює значні фінансові втрати. Сучасна система кіберзагроз переживає фундаментальну трансформацію. Розвиток генеративного штучного інтелекту створює новий тип кіберзагроз на рівні знань та інформації. Якщо традиційні кібератаки спрямовані на порушення доступності, цілісності або конфіденційності даних, то сучасні кіберзагрози об’єднали можливості когнітивної психології, потенціал великих даних та штучного інтелекту.

Повномасштабна війна та зростання соціальної напруги в Україні суттєво посилили вразливість користувачів до цілеспрямованих фішингових атак. Починаючи з 2022 року, фішинг, посилений штучним інтелектом, дедалі частіше фігурує у звітах правоохоронних органів як один із найбільш

поширених та небезпечних видів кіберзлочинної діяльності. Особливістю сучасного фішингу є інтеграція з великими мовними моделями (LLM). Можливість отруєння великих мовних моделей стає значною проблемою кіберзахисту та важливою складовою сучасної кібербезпеки. Її ігнорування може призвести до масштабних ризиків, тоді як своєчасне виявлення і протидія таким атакам є ключовими для забезпечення надійності та безпеки систем штучного інтелекту.

Вважаємо, що ефективна протидія таким загрозам потребує упровадження комплексних заходів кіберзахисту, тобто поєднання організаційних, технічних, освітніх та правових дій, спрямованих на забезпечення цілісності, конфіденційності та доступності інформації. В якості технічного захисту систем слід рекомендувати впровадження підходу "Zero Trust" (нульової довіри), багаторівневої автентифікаціх (MFA), шифрування даних та використання антивірусних рішень на основі ШІ.

Надзвичайно важливим напрямом боротьби з сучасними кіберзагрозами і одночасно посиленням стійкості кіберсистем є регулярне підвищення рівня обізнаності суспільства у питаннях кібербезпеки та зміцнення так званого «цифрового імунітету» громадян. Враховуючи різний рівень підготовленості користувачів сучасних інформаційних систем, звертаємо увагу на базові правила, яких слід дотримуватись для безпечної роботи в Інтернеті, захисту персональних і конфіденційних даних від кіберзагроз, та критичного сприйняття інформації. Це:

- обов’язкове використання складних, унікальних паролів (з періодичною їх заміною) при вході в системи;
- регулярне резервне копіювання і збереження важливих, цінних даних на зовнішніх носіях або у хмарі;
- уважність і обережність з посиланнями на невідомі сайти;
- встановлення антивірусних програм з функціями захисту від фішингу та спам-фільтрів для електронної пошти;
- перевірка налаштувань опцій приватності при роботі з ШІ-сервісами;
- категорична заборона вводити персональні дані при роботі з штучним інтелектом або додатками, що його використовують;
- обмежене або повне невикористання ШІ для роботи з документами, що мають гриф обмеження доступу;
- обачне використання плагінів (тільки від офіційних виробників) для розширення ШІ-сервісів.

Подальші дослідження повинні зосереджуватися на розробці методів виявлення та нейтралізації отруєних даних у великих мовних моделях, що дозволить зменшити ризики «галюцинацій» та шкідливих асоціацій. Важливо також оцінювати ефективність комплексних стратегій кіберзахисту, які поєднують технологічні, організаційні та психологічні аспекти безпеки, а також використовувати ШІ для прогнозування та моделювання кібератак у реальному часі. Крім того, перспективним є аналіз правових та етичних наслідків впровадження AI у критичні інформаційні системи для підвищення національної кіберстійкості та захисту громадян і організацій від сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Security and Defense Council of Ukraine. (2026). *Ukrainian experience is changing global cybersecurity*. https://www.rnbo.gov.ua/ua/Diialnist/7376.html
2. Cyberpolice Department of the National Police of Ukraine. (2026). *Annual report of the Cyberpolice Department of the National Police of Ukraine for 2025*. https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096
3. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
4. Fesokha, V., & Subach, I. (2025). Conceptual framework for improving cyber resilience of information and communication systems under the evolution of cyber threats. *Cybersecurity: Education, Science, Technique, 4*(28), 511-528. https://doi.org/10.28925/2663-4023.2025.28.856
5. European Parliament, & Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
6. European Union Agency for Cybersecurity. (n.d.). *Cyber resilience*. Retrieved February 20, 2026, from https://www.enisa.europa.eu/topics/cyber-threats
7. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework 2.0*. Retrieved February 22, 2026, from https://www.nist.gov/cyberframework

8. National Institute of Standards and Technology. (2019). *Cyber resiliency engineering* (Special Publication 800-160, Vol. 2). https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
9. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017*. https://zakon.rada.gov.ua/laws/show/2163-19
10. President of Ukraine. (2021). *Decree No. 447/2021 on the Cybersecurity Strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/447/2021
11. Verkhovna Rada of Ukraine. (2021). *On critical infrastructure: Law of Ukraine No. 1882-IX of November 16, 2021*. https://zakon.rada.gov.ua/laws/show/1882-20
12. Cabinet of Ministers of Ukraine. (2019). *On approval of general requirements for cyber protection of critical infrastructure facilities: Resolution No. 518 of June 19, 2019*. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF
13. European Commission. (2020). *EU cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
14. World Economic Forum. (2024). *Global cybersecurity outlook 2024*. https://www.weforum.org/reports/global-cybersecurity-outlook-2024
15. European Union Agency for Cybersecurity. (2021). *Artificial intelligence and cybersecurity: Opportunities and challenges*. https://www.enisa.europa.eu/news/enisa-news/artificial-intelligence-how-to-make-machine-learning-cyber-secure
16. Organisation for Economic Co-operation and Development. (n.d.). *Cybersecurity policy framework*. Retrieved February 23, 2026, from https://www.oecd.org/digital/security/
17. Yanenkova, I. H. (2025). Artificial intelligence in cybersecurity: Challenges, regulation, and impacts. In *Scientific trends of post-industrial society: IX International Scientific Conference* (pp. 40-49). https://doi.org/10.62731/mcnd-21.03.2025.001
18. Microsoft Security Blog. (2024, February 14). *Staying ahead of threat actors in the age of AI*. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
19. MITRE ATT&CK. (n.d.). *Phishing: Spearphishing voice (T1566.004)*. https://attack.mitre.org/techniques/T1566/004/
20. Anti-Phishing Working Group. (n.d.). *Phishing activity trends reports*. Retrieved February 24, 2026, from https://apwg.org/trendsreports
21. Souly, A., Rando, J., Chapman, E., Davies, X., Hasircioglu, B., Shereen, E., Mougan, C., Mavroudis, V., Jones, E., Hicks, C., Carlini, N., Gal, Y., & Kirk, R. (2025). *Poisoning attacks on LLMs require a near-constant number of poison samples*. arXiv. https://arxiv.org/abs/2510.07192
22. Prysiazhniuk, T. A. (2025). *Phishing as a method of social engineering*. Vinnytsia National Technical University Repository. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/48027/25603.pdf
23. National Institute of Standards and Technology. (2024). *Digital identity guidelines: Authentication and lifecycle management* (Special Publication 800-63B).
24. Rusnák, Z. (2024, September 26). *Cyberespionage: The Gamaredon way*. ESET Research. https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf
25. Cyberpolice Department of the National Police of Ukraine. (2024). *Report on the activities of the Cyberpolice Department of the National Police of Ukraine in 2023*. https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/
26. Cyberpolice Department of the National Police of Ukraine. (2025). *Report on the activities of the Cyberpolice Department of the National Police of Ukraine in 2024*. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/
27. Zhao, P., Zhu, W., Jiao, P., Gao, D., & Wu, O. (2025). *Data poisoning in deep learning: A survey*. arXiv. https://arxiv.org/abs/2503.22759
28. Adaptive Security. (2026). *End-user security awareness: Practical strategies for 2026*. https://www.adaptivesecurity.com/blog/end-user-security-awareness-practical-strategies-for-2026

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Svitlana Luchyk
Doctor of Economic Sciences, Professor, Professor of the Department of Information Systems and Technologies
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0000-0003-0757-1140
luchiksvitlana@gmail.com

Bohdan Makalish
Second-year cadet at the Educational and Scientific Institute No. 4 (training specialists in information and analytical support and cybersecurity for the National Police of Ukraine)
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0009-0002-2500-2734
bohdan.makalish@gmail.com

Arsenii Podvalnyi
Second-year cadet at the Educational and Scientific Institute No. 4 (training specialists in information and analytical support and cybersecurity for the National Police of Ukraine)
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0009-0003-5906-130X
arsenyi123123123@gmail.com

Dmytro Protsko
Second-year cadet at the Educational and Scientific Institute No. 4 (training specialists in information and analytical support and cybersecurity for the National Police of Ukraine)
Kharkiv National University of Internal Affairs, Kamianets-Podilskyi, Ukraine
ORCID: 0009-0003-2188-2049
protskodima200@gmail.com

NATIONAL CYBERSECURITY IN THE CONTEXT OF THE DEVELOPMENT OF GENERATIVE ARTIFICIAL INTELLIGENCE

Abstract. Today's info- and cyberspace are becoming a full-fledged arena of military operations, and the results of cyberattacks on digital infrastructure are comparable to obvious physical damage. Cyberattacks, enhanced by artificial intelligence, become the main tool of cybercriminals and a serious problem for every organization. Respecting the need for constant support of a proper level of cyber-resilience of government bodies, business structures, physical characteristics, there is a need for increased awareness of marriage from current cyber threats and fragmented effective complex systems for cyber defence. The purpose of this article is the analysis and assessment of current cyber threats, strengthened by the development of generative intelligence and the promotion of a rich, inclusive approach to strengthening the cyber resilience of the organization.

The study used general scientific theoretical methods, such as system analysis and abstract-logical method for theoretical generalizations and formulation of conclusions and recommendations regarding the strengthening of national cyber resilience; graphical method – for visual representation of theoretical and analytical material on the implementation of major cyber threats in the modern cyberspace.

The article examines the concept of cyber resilience of systems, networks, and organizations from the perspective of its interpretation by national and international legislation, domestic and foreign scientists, and researchers. The authors did analyse modern cyber threats, such as phishing, vishing, and video phishing, which have been transformed by generative artificial intelligence, becoming more complex, larger in scale, and going beyond social engineering in general. The phenomenon of “poisoning” large language models is also investigated, which is gradually becoming a relevant threat to modern cybersecurity, as such models are increasingly being integrated into critical information systems. In order to counter modern cyber threats and strengthen the cyber resilience of national systems, a comprehensive approach combining organizational, technical, educational, and legal measures is recommended. For users, the main rules for safe Internet use and protection of personal and confidential data from cyber threats are highlighted.

Keywords: cyber resilience; generative artificial intelligence; cyber threat; phishing; large language models; model poisoning; cybersecurity; cyber defense.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. National Security and Defense Council of Ukraine. (2026). *Ukrainian experience is changing global cybersecurity*. https://www.rnbo.gov.ua/ua/Diialnist/7376.html
2. Cyberpolice Department of the National Police of Ukraine. (2026). *Annual report of the Cyberpolice Department of the National Police of Ukraine for 2025*. https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096
3. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems: A systems security engineering approach* (NIST Special Publication 800-160, Vol. 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
4. Fesokha, V., & Subach, I. (2025). Conceptual framework for improving cyber resilience of information and communication systems under the evolution of cyber threats. *Cybersecurity: Education, Science, Technique, 4*(28), 511-528. https://doi.org/10.28925/2663-4023.2025.28.856
5. European Parliament, & Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2)*. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
6. European Union Agency for Cybersecurity. (n.d.). *Cyber resilience*. Retrieved February 20, 2026, from https://www.enisa.europa.eu/topics/cyber-threats
7. National Institute of Standards and Technology. (n.d.). *Cybersecurity Framework 2.0*. Retrieved February 22, 2026, from https://www.nist.gov/cyberframework
8. National Institute of Standards and Technology. (2019). *Cyber resiliency engineering* (Special Publication 800-160, Vol. 2). https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final
9. Verkhovna Rada of Ukraine. (2017). *On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017*. https://zakon.rada.gov.ua/laws/show/2163-19
10. President of Ukraine. (2021). *Decree No. 447/2021 on the Cybersecurity Strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/447/2021
11. Verkhovna Rada of Ukraine. (2021). *On critical infrastructure: Law of Ukraine No. 1882-IX of November 16, 2021*. https://zakon.rada.gov.ua/laws/show/1882-20
12. Cabinet of Ministers of Ukraine. (2019). *On approval of general requirements for cyber protection of critical infrastructure facilities: Resolution No. 518 of June 19, 2019*. https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF
13. European Commission. (2020). *EU cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
14. World Economic Forum. (2024). *Global cybersecurity outlook 2024*. https://www.weforum.org/reports/global-cybersecurity-outlook-2024
15. European Union Agency for Cybersecurity. (2021). *Artificial intelligence and cybersecurity: Opportunities and challenges*. https://www.enisa.europa.eu/news/enisa-news/artificial-intelligence-how-to-make-machine-learning-cyber-secure
16. Organisation for Economic Co-operation and Development. (n.d.). *Cybersecurity policy framework*. Retrieved February 23, 2026, from https://www.oecd.org/digital/security/
17. Yanenkova, I. H. (2025). Artificial intelligence in cybersecurity: Challenges, regulation, and impacts. In *Scientific trends of post-industrial society: IX International Scientific Conference* (pp. 40-49). https://doi.org/10.62731/mcnd-21.03.2025.001
18. Microsoft Security Blog. (2024, February 14).*Staying ahead of threat actors in the age of AI*. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/
19. MITRE ATT&CK. (n.d.). *Phishing: Spearphishing voice (T1566.004)*. https://attack.mitre.org/techniques/T1566/004/
20. Anti-Phishing Working Group. (n.d.). *Phishing activity trends reports*. Retrieved February 24, 2026, from https://apwg.org/trendsreports
21. Souly, A., Rando, J., Chapman, E., Davies, X., Hasircioglu, B., Shereen, E., Mougan, C., Mavroudis, V., Jones, E., Hicks, C., Carlini, N., Gal, Y., & Kirk, R. (2025). *Poisoning attacks on LLMs require a near-constant number of poison samples*. arXiv. https://arxiv.org/abs/2510.07192
22. Prysiazhniuk, T. A. (2025). *Phishing as a method of social engineering*. Vinnytsia National Technical University Repository. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/48027/25603.pdf
23. National Institute of Standards and Technology. (2024). *Digital identity guidelines: Authentication and lifecycle management* (Special Publication 800-63B).

24. Rusnák, Z. (2024, September 26). *Cyberespionage: The Gamaredon way*. ESET Research. https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf
25. Cyberpolice Department of the National Police of Ukraine. (2024). *Report on the activities of the Cyberpolice Department of the National Police of Ukraine in 2023*. https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/
26. Cyberpolice Department of the National Police of Ukraine. (2025). *Report on the activities of the Cyberpolice Department of the National Police of Ukraine in 2024*. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/
27. Zhao, P., Zhu, W., Jiao, P., Gao, D., & Wu, O. (2025). *Data poisoning in deep learning: A survey*. arXiv. https://arxiv.org/abs/2503.22759
28. Adaptive Security. (2026). *End-user security awareness: Practical strategies for 2026*. https://www.adaptivesecurity.com/blog/end-user-security-awareness-practical-strategies-for-2026

Отримано редакцією журналу / Received: 20.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26