УДК 004.35.078.3
JEL classification: D83, L86, M15, O33, F52
https://doi.org/10.31891/dsim-2026-14(3)

# АКТУАЛЬНІ НАПРЯМКИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА В УМОВАХ КІБЕРЗАГРОЗ

**ЯРЕМКО Світлана**
кандидат технічних наук, доцент
доцент кафедри інноваціної економіки та цифрових технологій
Вінницький торговельно-економічний інститут Державного торговельно-економічного університету
https://orcid.org/0000-0002-0605-9324
s.yaremko@vtei.edu.ua
**ДЕМЕНТЬЄВ Сергій**
кандидат технічних наук
доцент кафедри інноваціної економіки та цифрових технологій
Вінницький торговельно-економічний інститут Державного торговельно-економічного університету
https://orcid.org/0009-0006-1322-6756
s.dementiev@vtei.edu.ua
**НОВИЦЬКИЙ Руслан**
кандидат технічних наук, доцент
доцент кафедри інноваціної економіки та цифрових технологій
Вінницький торговельно-економічний інститут Державного торговельно-економічного університету
https://orcid.org/0000-0002-6895-5175
admin@vtei.edu.ua

*У статті розглянуті сучасні підходи та прикладні рішення для захисту особистих і службових даних в умовах сучасних кіберзагроз. Визначено основні ризики для користувачів, організацій та державних структур, пов'язані з витоком персональних даних, корпоративної або службової інформації. Проаналізовано основи правової регламентації захисту особистої та службової інформації. Наведено статистику щодо реальних скарг і збитків від втрати конфіденційності даних. Розглянуто сучасні технологічні та організаційні засоби захисту особистої та службової інформації. Обгрунтовано висновки та запропоновано рекомендації щодо впровадження сучасних засобів і підходів для своєчасне виявлення порушень, управління інформаційною безпекою та підвищення підвищення рівня захищенності інформаційних ресурсів.*

*Ключові слова: конфіденційність; інформаційна безпека; кіберзагрози, шифрування; правова регламентація, система захисту.*

# CURRENT DIRECTIONS FOR PROTECTION OF ENTERPRISE INFORMATION RESOURCES IN THE CONDITIONS OF CYBER THREATS

**YAREMKO Svitlana, DEMENTIEV Sergey, NOVITSKYI Ruslan**
Vinnytsia Trade and Economic Institute SUTE

*The article examines current approaches and practical solutions for protecting enterprise information resources in the context of rapidly growing cyber threats. In the conditions of intensive digitalization, the use of cloud technologies, social networks, and online services significantly increases the risks of unauthorized access, data leakage, and compromise of both personal and corporate information. These threats create serious financial, reputational, and legal consequences for organizations and require the development of comprehensive cybersecurity strategies.*

*The study identifies the main risks associated with the loss of confidentiality of personal and official data for individuals, enterprises, and government institutions. Particular attention is given to the analysis of common sources of data leakage, including phishing websites, insecure online services, social networks, automated bots, and recruitment platforms that may unintentionally expose sensitive information. The article also reviews statistical data on cybercrime incidents and financial losses caused by breaches of information security, demonstrating the increasing scale and systemic nature of cyber threats in modern digital environments.*

*The legal framework regulating the protection of personal and official information is analyzed, including national legislation of Ukraine and international regulatory practices. In addition, the paper examines modern technological and organizational methods of protecting information resources, such as encryption technologies, multi-factor authentication, intrusion detection systems (IDS/IPS), Data Loss Prevention (DLP) systems, SIEM and XDR security platforms, Zero Trust architecture, and secure communication technologies such as VPN. Organizational measures are also considered, including cybersecurity policies, personnel training, security audits, incident response teams, and the implementation of international standards such as ISO/IEC 27001 and NIST recommendations.*

*Based on the conducted analysis, the study substantiates the necessity of implementing a comprehensive and integrated approach to information security management that combines technological tools, organizational measures, and regulatory mechanisms. Practical recommendations are proposed for improving the protection of enterprise information resources, timely detection of security violations, and increasing the overall resilience of organizations to cyber threats. The results of the research may be used in the development of cybersecurity strategies and information protection systems for enterprises operating in modern digital environments.*

*Keywords: confidentiality; information security; cyber threats, encryption; legal regulation, protection system.*

Стаття надійшла до редакції / Received 19.01.2026
Прийнята до друку / Accepted 05.03.2026
Опубліковано / Published 16.04.2026



## *ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМ*

В умовах стрімкої цифровізації суспільства питання захисту інформаційних ресурсів набуває критичного значення. Втрата конфіденційності може призводити до фінансових збитків, репутаційних проблем, юридичних наслідків та навіть загроз національній безпеці. Ризики також зростають у зв'язку з активним використанням хмарних технологій, мобільних додатків, соціальних мереж і великих даних. У зв'язку з цим виникає потреба у комплексному підході до захисту інформаційних ресурсів підприємств в умовах кіберзагроз.

## *АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ*

Проблематика захисту конфіденційності даних розглядається у працях таких дослідників, як Ісаков М.Г., Паркулаб В.В. [2], Муха А.В. [3], , Землянська О.В., Праховнік Н. А., Ковтун А. І. [4], Захаржевський А. Г., Толкачов М. Ю., Дженюк Н. В. [10], Гнатюк С.О. [11] та ін. Ці дослідження зосереджуються на загрозах, пов'язаних із використанням персональної інформації в Інтернеті, теоретичних засадах правового захисту, а також на аспектах цифрової безпеки. Незважаючи на наявність ґрунтовних напрацювань, стрімкий розвиток кіберзагроз, поширення шкідливих технологій і витоки даних актуалізують потребу у розвитку існуючих підходів до захисту інформаційних ресурсів підприємств та поглибленні прикладних досліджень у цій сфері.

## *ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ*

Метою даної статті є аналітичний огляд правових засад і прикладних рішень для захисту інформаційних ресурсів підприємств та розробка рекомендацій щодо впровадження ефективних методів забезпечення конфіденційності персональних та службових даних.

## *ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ*

В умовах глобального поширення інформаційних ресурсів засобами комп'ютерних мереж все більш важливими стають питання забезпечення конфіденційності та цілісності даних. Працюючи в кіберсередовищі, людина отримує необхідну інформацію, але при цьому іноді несвідомо створює загрози для своїх особистих та службових даних [1]. У зв'яку з цим, актуальним завданям є розробка та впровадження ефективних інструментів захисту інформації в умовах кіберзагроз .

На теперішній час для особистого та професійного використання майже кожна людина реєструє декілька профілів та акаунтів.. При цьому існує загроза їх зламу, що може спричинити втрату даних або їх передачу через різні сервіси.

Загалом, існує безліч джерел витоків даних. Зокрема, важливо уважно вивчати безпеку сайтів для онлайн-покупок, адже зловмисники можуть вкрасти інформацію через фішинговий сайт або може статись витік клієнтських даних з боку адміністраторів сайтів електронної комерції [2]. Ще одним із джерел витоку даних є Telegram-боти, які взявши на себе функції автоматизованого управління електроприладами будинків, реєстрації користувачів для веб-сторінок, здіснення розсилки новин для певного кола користувачів, створюють можливості для викрадення даних [3]. Також вебресурси для працевлаштування є потенційними джерелами загроз для особистих даних [4].

Слід також відмітити, що необхідність надання персональної інформації для соціальних мереж теж є фактором ризику і обумовлює необхідність розробки правових засад. Крім того, через великі обсяги інформації, що містяться в соцмережах, виникає потреба у розробці правових механізмів убезпечення персональних даних.

Основою правової регламентації щодо захисту особистої та службової інформації в Україні є закони «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. [5], «Про захист персональних даних» від 01.07.2010 р. [6], а також інші національні і, зокрема, міжнародні нормативно-правові акти, які ратифіковані Україною.

Загалом, аналізуючи становлення законодавчої бази із захисту інформаційних ресурсів серед розвинутих країн, слід відмітити, що наприклад у США, відсутнє єдине федеральне законодавство з питань захисту даних, оскільки окремі штати можуть автономно регулювати цю сферу. Зокрема, у Каліфорнії з 2020 року діє закон, що регламентує використання персональних даних користувачів і надає право знати з якою метою компанія збирає і для чого буде використовувати їх інформацію [7]. В країнах Європейського Союзу захист інформаційних ресурсів регламентується відповідними директивами. Так, основною метою Директиви 95/46/ЄС Європейського парламенту та Ради Європи від 24.10.1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» є забезпечення однакового рівня захисту прав і свобод особи при обробці персональних даних в усіх державах-членах Європейського Союзу [8].

Наведені вище і подібні їм законодавчі акти інших країн у сфері захисту інформації створюють правове поле для регламентації використання особистих та службових даних, а також для притягнення до відповідальності у випадку вчинення злочинних дій, кількість яких за останні роки стрімко зростає.

Так, відповідно до досліджень американського центру збору інформації про кіберзлочини FBI Internet Crime Complaint Center (IC3), проблема незаконного доступу до даних та кіберзлочинів має системний і масовий характер. У 2022 році IC3 отримав 800 944 скарг, пов'язаних з кіберінцидентами, при цьому сукупні фінансові втрати жертв перевищили $10,3 млрд, що суттєво перевищило $6,9 млрд у 2021 році. Найбільші збитки були зафіксовані у сферах Business Email Compromise, коли кіберзлочинці видають себе за бізнес-партнерів чи керівників, спонукаючи до надання конфіденційних даних або переказу коштів на рахунки сторонніх осіб. Загалом з 2018 по 2022 роки було зафіксовано понад 3,26 млн скарг із сумарними втратами $27,6 млрд, що свідчить про зростаючі фінансові ризики для організацій та серйозні наслідки, пов'язані з компрометацією корпоративних і персональних даних (рис.1) [1].

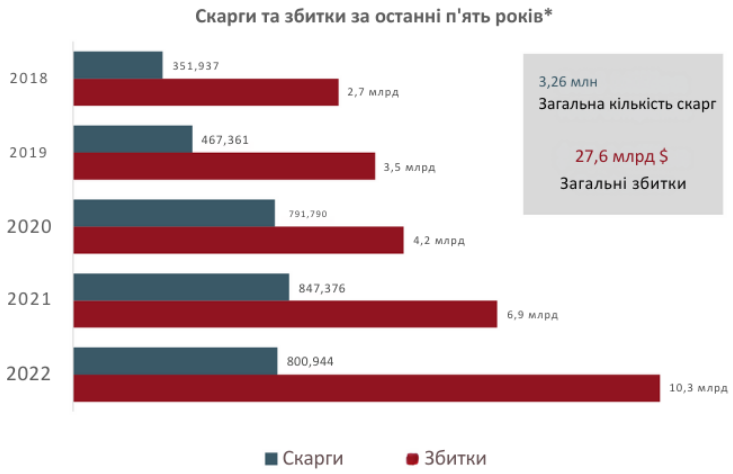


**Рис. 1. Скарги та збитки від кіберзлочинів за 2018-2022 згідно ІС3 [1]**

Дослідження національного інституту стандартів і технологій США для управління кібербезпекою, опубліковані у 2024 році, засвідчили, що організації все частіше стикаються з комплексними кіберзагрозами, що впливають не лише на IT-інфраструктуру, а й на бізнес-процеси підприємств. У документі наголошується, що більшість інцидентів безпеки виникає через недостатній рівень управління кіберризиками та відсутність системного підходу до захисту інформаційних ресурсів. Окрему увагу приділено необхідності інтеграції кібербезпеки у стратегічне управління підприємством, а також безперервного моніторингу, реагування та відновлення після атак. Зазначені підходи підтверджують актуальність переходу від фрагментарних заходів захисту до комплексної системи управління кіберстійкістю підприємства [9].

Відповідно до дослідження американського Інституту комп'ютерної безпеки, протягом минулих років 75% компаній виявили інциденти, пов'язані з порушенням конфіденційності інформації. Разом з тим, через пошкодження або викрадення даних, компанії у 2022 році отримали збитки біля двох мільярдів доларів., що перевищило у декілька разів показники 2021 року. Все це вказує на значний фінансовий вплив та негативні наслідки порушення безпеки службової інформації [1].

Результати досліджень українських науковців, опубліковані у 2024 році засвідчили, що значна частина проблем захисту інформаційних ресурсів підприємств пов'язана з відсутністю формалізованих моделей опису кіберпростору та інформаційних взаємодій. Автори зазначають, що традиційні методи безпеки не завжди дозволяють своєчасно виявляти складні кібератаки, зокрема багатовекторні та приховані загрози. Запропонований у дослідженні метод захисту на основі семіотичної моделі кіберпростору дає змогу систематизувати події, об'єкти та ознаки атак, що підвищує ефективність моніторингу та реагування на інциденти. Отримані результати підтверджують необхідність використання інтелектуальних і формалізованих підходів до захисту інформаційних ресурсів підприємства в сучасних умовах кіберзагроз [10].

В дослідженнях питань інформаційної безпеки українськими науковцями у 2025 році підкреслюється, що зростання кількості кібератак на підприємствах зумовлює потребу у побудові комплексної системи кібербезпеки, орієнтованої на захист критичних інформаційних ресурсів. Також зазначається, що найбільших збитків підприємства зазнають унаслідок атак типу ransomware програмами-вимагачами, компрометації облікових даних та порушення безперервності бізнес-процесів. У роботі виділено превентивні та реактивні напрями захисту, зокрема управління ризиками, впровадження систем моніторингу, планування реагування на інциденти та відновлення після атак. Отримані висновки свідчать, що ефективний захист інформаційних ресурсів можливий лише за умови поєднання організаційних, технічних та управлінських заходів кібербезпеки [11].

Комплексний підхід до вирішення питань інформаційної безпеки даних згідно [2-5] має включати в себе:

1) технологічні засоби:
- шифрування даних (end-to-end encryption), зокрема протоколи TLS 1.3, AES-256;
- анонімізація і псевдонімізація даних, а саме GDPR вимагає їх використання при обробці персональних даних;
- системи виявлення вторгнень (IDS) та витоків (DLP — Data Loss Prevention);
- багатофакторна аутентифікація;
- безпечне зберігання та передача даних (наприклад VPN, Zero Trust-архітектура).

2) організаційні заходи:
- розробка політик безпеки та внутрішніх регламентів;
- регулярне навчання персоналу (на прикладі компанії);
- проведення аудитів безпеки та пентестів;
- інцидент-менеджмент, а саме створення команд реагування на кіберінциденти (як от CERT/SOC);
- використання стандартів, таких як ISO/IEC 27001, NIST SP 800-53.

Розглянемо детальніше сучасні засоби і підходи до захисту інформаційних і персональних даних, які сформувалися у відповідь на зростання масштабів цифровізації та ускладнення кіберзагроз.

Антивірусні системи (AV/NGAV) стали першими програмними засобами захисту інформації та почали розвиватися наприкінці 1980-х років у зв'язку з появою комп'ютерних вірусів. Початково вони ґрунтувалися на сигнатурному аналізі відомих загроз і забезпечували базовий рівень безпеки. Сучасні антивірусні рішення доповнені поведінковим аналізом та ізольованим виконанням підозрілих об'єктів, що підвищує ефективність захисту. Водночас такі системи залишаються обмеженими у протидії новим атакам типу zero-day [11].

Системи виявлення та запобігання вторгненням (IDS/IPS) почали формуватися у 1990-х роках у межах досліджень комп'ютерних мереж. Їх основне призначення полягає у виявленні спроб несанкціонованого доступу шляхом аналізу мережевого трафіку. IDS орієнтовані на виявлення атак, тоді як IPS доповнюють цей функціонал можливістю їх блокування. Дані системи забезпечують раннє реагування на кібератаки, однак потребують точного налаштування [11].

DLP-системи (Data Loss Prevention) з'явилися на початку 2000-х років у відповідь на зростання кількості витоків конфіденційної інформації, зокрема персональних даних. Їх призначенням є контроль каналів передачі інформації та аналіз її вмісту з метою запобігання несанкціонованому поширенню даних. DLP-системи є ефективним інструментом захисту інформаційних ресурсів підприємства, хоча відзначаються складністю адміністрування [10].

SIEM-системи сформувалися як окремий клас рішень на початку 2000-х років у результаті поєднання управління журналами подій та кореляції інцидентів безпеки. Вони забезпечують централізований моніторинг подій з різних інформаційних систем і дозволяють формувати цілісну картину стану кібербезпеки. SIEM широко застосовуються у центрах моніторингу безпеки, проте потребують значних фінансових і кадрових ресурсів [11].

XDR-системи є подальшим етапом розвитку засобів виявлення та реагування на загрози, які почали впроваджуватися у другій половині 2010-х років. Їх поява зумовлена необхідністю об'єднання даних з різних середовищ - кінцевих пристроїв, мережі та поштових сервісів. XDR забезпечує більш ефективне виявлення складних атак, однак потребує зрілої IT-інфраструктури [10].

Архітектура Zero Trust була запропонована на початку 2010-х років як відповідь на зростання внутрішніх загроз і розвиток хмарних технологій. Вона базується на принципі відсутності довіри до будь-якого користувача або пристрою та передбачає багатофакторну автентифікацію і сегментацію мережі. Такий підхід дозволяє зменшити ризик компрометації інформаційних ресурсів, проте потребує поетапного впровадження [11].

VPN-технології почали застосовуватися у 1990-х роках для забезпечення захищеного віддаленого доступу до корпоративних мереж. Вони використовують шифрування каналів зв'язку для захисту даних під час передавання. VPN є ефективним засобом при роботі у публічних мережах, однак не забезпечує захист від внутрішніх загроз [10].

Шифрування даних є одним із найдавніших методів захисту інформації, який у сучасному вигляді почав активно розвиватися у другій половині XX століття. Алгоритми AES та протоколи TLS стали стандартами забезпечення конфіденційності інформації в мережі Інтернет. Шифрування гарантує захист даних під час зберігання та передавання, але не запобігає компрометації облікових даних [11].

SOC та CERT як організаційні структури з'явилися наприкінці 1980-х років після перших масштабних кіберінцидентів. Їх діяльність спрямована на постійний моніторинг та реагування на кіберінциденти. Такі підрозділи підвищують рівень кіберстійкості організацій, хоча потребують значних ресурсів [10].

Стандарти ISO/IEC 27001 та рекомендації NIST почали формуватися наприкінці XX століття з метою уніфікації підходів до управління інформаційною безпекою. Вони визначають політики, процедури та механізми управління ризиками. Зазначені стандарти не є технічними засобами захисту, проте створюють

основу для побудови ефективної системи кібербезпеки [9].

Узагальнені характеристики розглянутих методів та засобів захисту інформаційнийних ресурсів, а також їх переваги і недоліки наведені таблиці 1.

Таблиця 1

**Порівняльна характеристика сучасних систем та підходів захисту інформації**

| Система / підхід захисту | Основне призначення | Ключові механізми | Переваги | Обмеження / недоліки |
|---|---|---|---|---|
| Системи виявлення та запобігання вторгненням (IDS/IPS) | Виявлення атак у мережі | Аналіз трафіку, сигнатури, аномалії | Раннє виявлення кібератак | Потребують налаштування, можливі хибні спрацювання |
| DLP (Data Loss Prevention) | Захист від витоків даних | Контроль каналів передачі, контент-аналіз | Ефективні для персональних і корпоративних даних | Складність адміністрування |
| SIEM-системи | Централізований моніторинг безпеки | Кореляція подій, лог-аналіз, алерти | Комплексний огляд інцидентів | Висока вартість впровадження |
| XDR (Extended Detection and Response) | Розширене виявлення та реагування | Об'єднання endpoint, мережі, пошти | Краще виявлення складних атак | Потребує зрілої IT-інфраструктури |
| Zero Trust Architecture | Захист доступу до ресурсів | Принцип «нікому не довіряти», MFA, сегментація | Мінімізація ризику внутрішніх загроз | Поступове та складне впровадження |
| VPN | Захист передавання даних | Шифрування каналів зв'язку | Захист у публічних мережах | Не захищає від внутрішніх атак |
| Шифрування даних (TLS, AES) | Захист конфіденційності | Криптографічні алгоритми | Високий рівень захисту даних | Не запобігає компрометації доступу |
| SOC / CERT | Реагування на кіберінциденти | Моніторинг 24/7, інцидент-менеджмент | Підвищення кіберстійкості | Значні організаційні витрати |
| Стандарти ISO/IEC 27001, NIST | Управління інформаційною безпекою | Політики, аудит, управління ризиками | Системність та відповідність нормам | Не є технічним засобом |

На основі поданої у табл. 1 порівняльної характеристики сучасних підходів та засобів захисту інформаційних ресурсів можна відзначити, що незважаючи на зростаючий технологічний рівень забезпечення захисту, кожний із наведених інструментів захисту має певні недоліки, що підтверджує результати досліджень вітчизняних та зарубіжних науковців щодо необхідності запровадження комплексного підходу.

Таким чином, на основі розглянутих вище загроз для інфомації в кіберпросторі та підходів і засобів її убезпечення, можна запропонувати ряд рекомендацій щодо забезпечення конфіденційності особистих та службових даних в умовах кіберзагроз:

- застосування сучасних антивірусних програм;
- уникнення підключення до безкоштовних мереж кафе, готелів тощо;
- використання лише спеціальних захищених браузерів для здійснення онлайн платежів;
- завантаження додатків лише з офіційних сайтів;
- використання захищених платіжних систем у мережі Інтернет;
- уникнення передавання персональних даних невідомим особам в електронних листах та месенджерах;
- здійснення перевірки автентичності вебресурсів при заповненні онлайн-форм для введення персональних даних;
- передача інформації відповідним органам при отриманні даних, що мають характер залякування тощо.

## *ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ*

В цілому, можна підсумувати, що питання захисту інформаційних ресурсів в умовах кіберзагроз набуває все більшої актуальності в контексті глобальних поліічних та економічних ризиків. Вирішення цього завдання полягає в першу чергу у поглибленому дослідженні існуючої законодавчої бази у сфері захисту, а також використанні ефективних технічних і програмних засобів убезпечення інформації у кіберпросторі.

У подальших дослідженнях доцільно поглиблювати вивчення факторів ризику порушення цілісності та конфіденційності інформації в мережі Інтернет. Разом з тим, особливу увагу потрібно приділяти розвиткові нових технологій, зокрема розробці та впровадженню нейромереж для ідентифікації та усунення загроз. Важлимим фактором у цьому процесі має стати колаборація науково-дослідних установ, підприємств та організацій, спрямована на збір інцидентів, скарг і їх подальшої обробки для виявлення та усунення загроз витоку та втрати особистих і службових даних.

**Література**

1. Bureau of Investigation: International Crime Report. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2. Ісаков М.Г., Паркулаб В.В. Захист персональних даних у мережі Інтернет: загальнотеоретичні питання. Науковий вісник публічного та приватного права. 2018. №5. С. 106-110.
3. Муха А.В. Загрози використання персональних даних у мережі Інтернет. Наукові записки студентів та аспірантів. Серія «Міжнародні відносини». 2020. № 5. С. 323-330.
4. Землянська О. В., Праховнік Н. А., Ковтун А. І. Безпека в Інтернеті та захист персональних даних. Всеукраїнської науково-практичної конференція «Безпека життя і діяльності людини: теорія та практика»: Полтава, 2022. С. 62-64.
5. Закон України: Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 31 (редакція від 31.05.2005). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
6. Закон України: Про захист персональних даних» від 01.06.2010 № 2297-VI (редакція від 27.10.2022). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
7. Recommendation CM/Rec (2018) 2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14
8. Посібник з європейського права у сфері захисту персональних даних. URL: https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ukr.pdf
9. Рамка кібербезпеки NIST (Cybersecurity Framework 2.0). Національний інститут стандартів і технологій США. 2024. URL: https://www.nist.gov/cyberframework
10. Захаржевський А. Г., Толкачов М. Ю., Дженюк Н. В. Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 2024. №1(57). С.57–68. URL: https://doi.org/10.31673/2409-7292.2024.010007
11. Гнатюк С.О., Побережна З.М., Заліський М.В. Інформаційна безпека та захист від кібератак як складова системи економічної безпеки підприємства. Proceedings of the International Scientific Conference. 2025. С. 98–104. URL: https://ceur-ws.org/Vol-4042/paper14.pdf

**References**

1. Bureau of Investigation: International Crime Report. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2. Isakov M.H., Parkulab V.V. Zakhyst personalnykh danykh u merezhi Internet: zahalnoteoretychni pytannia. Naukovyi visnyk publichnoho ta pryvatnoho prava. 2018. №5. S. 106-110.
3. Mukha A.V. Zahrozy vykorystannia personalnykh danykh u merezhi Internet. Naukovi zapysky studentiv ta aspirantiv. Seriia «Mizhnarodni vidnosyny». 2020. № 5. S. 323-330.
4. Zemlianska O. V., Prakhovnik N. A., Kovtun A. I. Bezpeka v Interneti ta zakhyst personalnykh danykh. Vseukrainskoi naukovo-praktychnoi konferentsiia «Bezpeka zhyttia i diialnosti liudyny: teoriia ta praktyka»: Poltava, 2022. S. 62-64.
5. Zakon Ukrainy: Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh» vid 05.07.1994 № 31 (redaktsiia vid 31.05.2005). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
6. Zakon Ukrainy: Pro zakhyst personalnykh danykh» vid 01.06.2010 № 2297-VI (redaktsiia vid 27.10.2022). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
7. Recommendation CM/Rec (2018) 2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Adopted by the Committee of Ministers on 7 March 2018 at the 1309th meeting of the Ministers Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14.
8. Posibnyk z yevropeiskoho prava u sferi zakhystu personalnykh danykh. URL: https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ukr.pdf
9. Ramka kiberbezpeky NIST (Cybersecurity Framework 2.0). Natsionalnyi instytut standartiv i tekhnolohii SShA. 2024. URL: https://www.nist.gov/cyberframework
10. Zakharzhevskyi A. H., Tolkachov M. Yu., Dzheniuk N. V. Metod zakhystu informatsiinykh resursiv na osnovi semiotychnoi modeli kiberprostoru. Suchasnyi zakhyst informatsii, 2024. №1(57). S.57–68. URL: https://doi.org/10.31673/2409-7292.2024.010007.
11. Hnatiuk S.O., Poberezhna Z.M., Zaliskyi M.V. Informatsiina bezpeka ta zakhyst vid kiberatak yak skladova systemy ekonomichnoi bezpeky pidpryiemstva. Proceedings of the International Scientific Conference. 2025. S. 98–104. URL: https://ceur-ws.org/Vol-4042/paper14.pdf