ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської
науково-практичної конференції

27 листопада 2025 року

м. Львів

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ПРИВАТНИЙ ЗАКЛАД ВИЩОЇ ОСВІТИ «ІТ СТЕП УНІВЕРСИТЕТ»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
VII Всеукраїнської науково-практичної конференції

27 листопада 2025 року

Львів – 2025

УДК 004.056

ІНФОРМАЦІЙНІ ЗАГРОЗИ У СУЧАСНОМУ СУСПІЛЬСТВІ ТА ЗАХИСТ ВІД НИХ

Юрій ВІНТЮК
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація. Розглянуто інформаційні загрози як невід'ємний наслідок *залежності сучасного суспільства від цифрових систем. Визначено їхню класифікацію за аспектами безпеки (конфіденційність, цілісність, доступність) та чинниками (кіберзагрози, дезінформація, соціальна інженерія). Обґрунтовано необхідність комплексного захисту, що охоплює технічні засоби, правові механізми та підвищення інформаційної культури громадян для забезпечення стійкості суспільства.*

Ключові слова: *інформаційні загрози, кібербезпека, інформаційна безпека, дезінформація, соціальна інженерія, комплексний захист, критичне мислення.*

Abstract. *Information threats are considered as an inherent consequence of modern society's dependence on digital systems. Their classification is determined by security aspects (confidentiality, integrity, availability) and factors (cyber threats, disinformation, social engineering). The need for comprehensive protection, which includes technical means, legal mechanisms and improving the information culture of citizens to ensure the sustainability of society, is substantiated.*

Key words*: information threats, cybersecurity, information security, disinformation, social engineering, comprehensive protection, critical thinking.*

Застосування інформаційних технологій у різних сферах життєдіяльності суспільства не лише підвищує продуктивність діяльності, але й повсякчас створює непередбачувані ускладнення. Розвиток інформаційних технологій трансформував суспільство, зробивши його залежним від них; проте ця залежність від цифрових систем і даних породила нові, складні й багатогранні інформаційні загрози. Причому вони стосуються не лише технічної сфери, а й соціальної, економічної та національної безпеки. Ефективний захист від них є пріоритетним завданням для кожної держави, організації та окремої особи. Дана обставина зумовлює актуальність розгляду інформаційних загроз у сучасному суспільстві та захисту від них.

Мета дослідження: розглянути специфіку інформаційних загроз у сучасному суспільстві та можливості захисту від них.

Дана тема неодноразово перебувала в полі уваги науковців, вітчизняних зокрема [1-7]; враховуючи наявні напрацювання, передусім доцільно розглянути найпоширеніші їх види.

1. Класифікація видів інформаційних загороз.

Інформаційні загрози можна класифікувати за різними критеріями, але найчастіше їх поділяють за аспектом безпеки, на який вони спрямовані:

1.1. Аспекти безпеки:

- Конфеденційність: неправомірний доступ до інформації, її витік (наприклад: шпигунські програми, фішинг, зламування баз даних, інсайдерська діяльність).

- Цілісність: несанкціонована зміна або знищення інформації (наприклад: хакерські атаки з метою спотворення даних, віруси-шифрувальники, помилки персоналу).
- Доступність: блокування або унеможливлення санкціонованого доступу до інформації чи систем (наприклад: DDoS-атаки, відмова обладнання, перебої в електропостачанні, мережеві "хробаки").

Наступний критерій класифікації розрізняє їх за зумовлюючими чинниками.

1.2. Технологічні (кіберзагрози)

Це найвідоміші загрози, пов'язані з програмним забезпеченням і мережами:

- Шкідливе ПЗ: віруси, троянські програми, шпигунське ПЗ, програми-вимагачі, які блокують системи або шифрують дані з метою одержання викупу.
- Кібератаки: спрямовані на критичну інфраструктуру, державні установи чи великі корпорації з метою порушення їхньої роботи або крадіжки інформації.

1.3. Соціально-психологічні та політичні

Ці загрози спрямовані на свідомість і стабільність суспільства:

- *Дезінформація та фейкові новини:* поширення неправдивої інформації для маніпулю-вання громадською думкою, створення паніки чи підриву довіри до державних інститутів.
- Інформаційно-психологічні операції: комплексний вплив на суспільну свідомість із метою зміни політичних настроїв, розпалювання ворожнечі та дестабілізації.
- Соціальна інженерія: використання людського фактору (довірливості, неуважності) для отримання доступу до конфіденційних даних (це фішинг-листи, телефонне шахрайство).

2. Захист від інформаційних загроз: комплексний підхід

Як показує наявний досвід протидії інформаційним загрозам, ефективний захист вимагає впровадження заходів на всіх рівнях: технічному, організаційно-правовому й освітньому.

2.1. Технічні та програмні засоби

Це база для протидії більшості кіберзагроз:

- Багаторівневий захист: використання антивірусного ПЗ, міжмережевих екранів, систем виявлення вторгнень.
- Резервне копіювання: регулярне створення копій критично важливих даних для швидкого відновлення після атак чи збоїв.
- Криптографічний захист: шифрування даних, що передаються (наприклад: за допомогою VPN, SSL/TLS), і даних, що зберігаються, для забезпечення конфіденційності.
- Оновлення ПЗ: регулярне встановлення оновлень операційних систем і програм для закриття "дірок" у безпеці.

2.2. Організаційні та правові механізми

Але ні одна технологія не працюватиме без чітких правил і відповідальності:

- Політики безпеки: розробка та неухильне дотримання внутрішніх правил роботи з інформацією, використання паролів і доступу до ресурсів.
- Контроль доступу: впровадження принципу мінімальних привілеїв і двофакторної (або багатофакторної) автентифікації.
- Законодавче регулювання: прийняття та вдосконалення законів у сфері кібербезпеки, захисту персональних даних (наприклад: GDPR в ЄС) і боротьби з кіберзлочинністю.

2.3. Людський фактор та освіта

Людина залишається найслабшою ланкою в системі захисту, тому доцільно задіяти:

- Навчання персоналу – регулярні тренінги з основ інформаційної гігієни, розпізнавання фішингу та правил роботи з конфіденційною інформацією.
- Критичне мислення – розвиток у суспільстві навичок критичного аналізу інформації, перевірки джерел та фактів для протидії дезінформації.
- Культура безпеки – формування відповідального ставлення до власної та корпоративної інформаційної безпеки.

Висновки. Інформаційні загрози в сучасному суспільстві є динамічними, глобальними та комплексними. Вони вимагають не лише постійного вдосконалення технічних засобів захисту, але й формування високої інформаційної культури та критичного мислення у громадян. Захист від цих загроз – це безперервний процес, що включає єдність технологій, законодавства й освітянської роботи. Тільки комплексний підхід, де кожен учасник інформаційного простору усвідомлює свою роль і відповідальність, може забезпечити стійкість і безпеку сучасного суспільства.

Література

1. Виздрик В., Мельник О. Інформаційна безпека в Україні. Grail of Science. 2023. № 24. С. 196-202.

2. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. 2020. № 2. С. 200-203.

3. Залєвська І. І., Удренас Г. І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південно український правничий часопис*. 2022. № 1. С. 20-26.

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2019. № 1. Вип. 2. С. 27-32.

5. Панченко О. Інформаційна безпека держави як елемент соціокультури. *Аспекти публічного управління*. 2020. № 1. С. 58-67.

6. Уханова Н.С. Правова культура молоді в Україні. *Інформація і право*. 2019. № 2. С. 156-166.

7. Шевчук О.М. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 160-166.