

# **СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ**

*Матеріали Всеукраїнської науково-практичної конференції*

*27 лютого 2025 року*



**КИЇВ - 2025**

УДК: 004.056

*Рекомендовано до друку Вченою радою Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій*

*(протокол № 1 від 11.03.2025 р.)*

**Редакційна колегія:**

**Легомінова С.В.** – д.е.н., професор, завідувач кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Гайдур Г.І.** – д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Савченко В.А.** – д.т.н., професор, професор кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Мужанова Т.М.** – кандидат наук з державного управління, доцент, доцент кафедри кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Щавінський Ю.В.** – к.т.н., доцент, доцент кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Якименко Ю.М.** – к.в.н., доцент, доцент кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Дзюба Т.М.** – к.т.н., доцент, доцент кафедри кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

**Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:**

Матеріали Всеукраїнської науково-практичної Інтернет-конференції (м. Київ, 27 лютого 2025 року) / Навчально-науковий інститут кібербезпеки та захисту інформації ДУІКТ. Київ, 2025. 304 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з інформаційної та кібернетичної безпеки, працівників органів державної влади та місцевого самоврядування.

*Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику.  
Тези подані в авторській редакції та відображають персональну позицію учасників конференції*



## ЗМІСТ

### СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

<i>Осауленко В.Р.</i>	МЕТОДИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	11
<i>Єрмоленко В. А.</i>	СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ	13
<i>Ілляшенко О. М.</i>	МЕТОДИ ТА ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ БІЗНЕСУ В УМОВАХ ДИНАМІЧНИХ ЗАГРОЗ КІБЕРПРОСТОРУ	15
<i>Коваль М.А., к.т.н., Бобровський О.В., к.т.н., Геращенко І.О., к.держ.упр., Никитюк А.П.</i>	СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ	19
<i>Миколаєнко О.С.</i>	РОЛЬ КІБЕРБЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ БЕЗПЕРЕРВНОЇ РОБОТИ КОМПАНІЙ	24
<i>Баранов Н.Б.</i>	ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА АВТОМАТИЗОВАНИХ СИСТЕМ У СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ЯК КЛЮЧ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ: НОВІ ГОРИЗОНТИ В ІДЕНТИФІКАЦІЇ ТА МІНІМІЗАЦІЇ РИЗИКІВ	27
<i>Селіванов І.С.</i>	БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ В УКРАЇНІ ПІД ЧАС ВІЙНИ	31
<i>Капелюшина Т.В., д.е.н., доцент</i>	ВАГОМІСТЬ КІБЕРНЕТИКИ В ПОВОЄННИЙ ПЕРІОД	34
<i>Рудницький Я.Р.</i>	КІБЕРОБМАН ЯК СТРАТЕГІЯ ПІДВИЩЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ	36

### СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

<i>Галушко В.Т.</i>	МЕТОДИ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ	39
<i>Зайченко М.В.</i>	ВАЖЛИВІСТЬ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	43

<i>Клімченко О.Р.</i>	ОЦІНКА СТРАХОВОЇ СТІЙКОСТІ КІБЕРРИЗИКІВ, КЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ: ВИКЛИКИ ТА МОЖЛИВОСТІ	45
<i>Матвієнко В.І.</i>	АНАЛІЗУ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПУБЛІЧНІ ДЖЕРЕЛА ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ	48
<i>Горбач Є.С.</i>	ОЦІНКА РИЗИКІВ ПОВ'ЯЗАНА З ЛЮДСЬКИМ ФАКТОРОМ	53
<i>Котецька В.І.</i>	РИЗИКИ ТА ПЕРЕВАГИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ	57
<i>Пічкур Д.С.</i>	ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ: ШТУЧНИЙ ІНТЕЛЕКТ, ПОВЕДІНКОВИЙ АНАЛІЗ І КВАНТОВЕ ШИФРУВАННЯ	60
<i>Котенко А.М.</i>	ВПЛИВ ЧИННИКА АКУСТИЧНОЇ ІНФОРМАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА	62
<i>Бойко М.А.</i>	ІНТЕГРАЦІЯ ДАТА-АНАЛІТИКИ ДЛЯ ЕФЕКТИВНОГО УПРАВЛІННЯ РИЗИКАМИ	66
<i>Кирєєв Р. Д.</i>	ІДЕНТИФІКАЦІЯ ПІДРОБЛЕНИХ НОВИН В СОЦІАЛЬНИХ МЕРЕЖАХ	69
<i>Курінний О. С.</i>	ОСНОВНІ ЗАГРОЗИ КІБЕРБЕЗПЕЦІ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ	72
<i>Павленко А.А.</i>	ПОРІВНЯННЯ ТРАДИЦІЙНИХ МЕТОДІВ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ІЗ СУЧАСНИМИ AI-РІШЕННЯМИ	74
<i>Мужанова Т.М.</i> <i>к.держ.упр, доц.,</i> <i>Ярмоленко Б. В.</i> <i>Костенко Я. О.</i>	ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОРГАНІЗАЦІЇ ТА ЗДІЙСНЕННІ КІБЕРАТАК	76
<i>Ярмоленко В.Я.</i>	АНАЛІЗ ФЕЙКОВИХ АККАУНТІВ ТА ЇХ РОЛІ У ПОШИРЕННІ ДЕЗІНФОРМАЦІЇ	79
<i>Дудій С. А.</i>	ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРАТАКАХ ТА КІБЕРЗАХИСТІ	81
<i>Донцов Є. А.</i>	ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ ТА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	84
<i>Гаврилець Д. Р.</i>	МЕТОДИ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ ДЛЯ ВИЯВЛЕННЯ ВНУТРІШНІХ ЗАГРОЗ	86
<i>Легомінова С. В., д.е.н.,</i>	НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ	91
	КІБЕРЗАГРОЗИ ДЛЯ ОРГАНІЗАЦІЙ У	93

**СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ  
КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА**

<i>Бабенко А.В</i>	ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ	98
<i>Іпатов І.А.</i>	МЕТОДИ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	100
<i>Петренко А.О.</i>	РЕГУЛЯТОРНИМ ВИМОГАМ ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА	104
<i>Книш Л.А.</i>	МЕТОДИ ІНТЕГРАЦІЇ CSIRT ТА SOC У РАМКАХ КОРПОРАТИВНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ	107
<i>Лоза О.Д.</i>	ЛЮДСЬКИЙ ФАКТОР У СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ISO/IEC 27001	110
<i>Якименко Ю.М., к.в.н., доц.</i>	МЕТОДИЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ	113
<i>Артеменко Н. Ю.</i>	ПІДГОТОВКА ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПЛАНУВАННЯ, НАВЧАННЯ ТА ТЕСТУВАННЯ	116
<i>Жестков Д.І.</i>	ФОРМУВАННЯ КОНТЕКСТУ ОЦІНКИ РИЗИКІВ У СИСТЕМАХ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	119
<i>Пехова Л.О.</i>	РОЛЬ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ СЕРЕДОВИЩАХ	122
<i>Кондратюк Д. О.</i>	ZERO TRUST ЯК СТРАТЕГІЯ КІБЕРЗАХИСТУ: ПРИНЦИПИ, ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ	125

**СЕКЦІЯ 4. ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ**

<i>Слободська Л.О.</i>	ВПРОВАДЖЕННЯ ZERO TRUST ЯК КЛЮЧОВОГО ПІДХОДУ ДО БЕЗПЕКИ	127
<i>Святська Запорожченко</i>	<i>Н.А.,</i> АНАЛІЗ <i>М.М.,</i> ТЕМПІВ ЗРОСТАННЯ	130

<i>Примаченко Д.В.</i>	ФІШИНГОВИХ АТАК: НОВІ МЕТОДИ ОЦІНКИ РИЗИКІВ	
<i>Святська Н.А., Тищенко В.С., Примаченко Д.В.</i>	АІ-ПРОТИДІЯ ФІШИНГОВИМ АТАКАМ: РОЗПІЗНАВАННЯ ЗАГРОЗ У РЕАЛЬНОМУ ЧАСІ	135
<i>Романов О. А.</i>	АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ ТА РЕАГУВАННЯ: СУЧАСНІ ІНСТРУМЕНТИ ТА ПРАКТИКИ	141
<i>Майсузенко Р.В.</i>	РОЗВІДКА НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ СУСПІЛЬСТВО ТА КІБЕРГІГІЄНА	146
<i>Никитенко Є.Я.</i>	ВИКОРИСТАННЯ SIEM-СИСТЕМ НА БАЗІ ELASTIC STACK ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ТА УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ	150
<i>Рубан Ю.Р</i>	МЕТОДИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ В КІБЕРБЕЗПЕЦІ. ІНТЕГРАЦІЯ ЦИХ МЕТОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ	151
<i>Савченко В.А., д.т.н., проф., Горбачова Я.С., Новікова І.В.</i>	НЕЙРОМЕРЕЖЕВА ТЕХНОЛОГІЯ ЗАХИСТУ КАНАЛІВ УПРАВЛІННЯ В ГРУПІ БПЛА	155
<i>Устименко В. О.</i>	СИСТЕМА ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ	159
<i>Заведєя К.А.</i>	МЕТОДИКА РОЗРОБКИ І ВПРОВАДЖЕННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ.	163
<i>Капустенко Д.І.</i>	ТЕХНОЛОГІЇ ШИФРУВАННЯ ТА АНОНІМІЗАЦІЇ ДЛЯ ЗАХИСТУ КОРИСТУВАЧІВ В ІНТЕРНЕТІ	166
<i>Орленко М.Є.</i>	ВИКОРИСТАННЯ XDR ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	170
<i>Рябицун В.П.</i>	ОСНОВИ ВИКОРИСТАННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У ФІНАНСОВИХ УСТАНОВАХ, КРИПТОГРАФІЧНІ ПРОТОКОЛИ У ЗАХИСТІ БАНКІВСЬКИХ ОПЕРАЦІЙ. РИЗИКИ ВИКОРИСТАННЯ ПУБЛІЧНИХ МЕРЕЖ WI-FI ДЛЯ БАНКІВСЬКИХ ОПЕРАЦІЙ.	174
<i>Журбенко А. О.</i>	ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ІТ- ІНФРАСТРУКТУРИ	176

<i>Фомін І.О.</i>	ВИКОРИСТАННЯ SPLUNK ДЛЯ ОПТИМІЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРАТАКИ У СТРУКТУРАХ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ	181
<i>Завгородня Є. Я. Курінний О. С.</i>	ВИКЛИКИ ТА РІШЕННЯ ХМАРНОЇ БЕЗПЕКИ ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ	184 187
<i>Тищенко В.С. Кушнерьов І. К.</i>	ВИКОРИСТАННЯ МЕТОДІВ КЛАСТЕРИЗАЦІЇ ДЛЯ ВИЯВЛЕННЯ ДЖЕРЕЛ ФЕЙКОВОЇ ІНФОРМАЦІЇ	189
<i>Марченко М.В.</i>	КІБЕРБЕЗПЕКА В СИСТЕМАХ УПРАВЛІННЯ ВЕЛИКИМИ ДАНИМИ: ВИКОРИСТАННЯ ІНСТРУМЕНТІВ POWER BI	192
<i>Нестеров О. В.</i>	ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙНУ ДЛЯ ПЕРЕВІРКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ	194
<i>Щербаненко Г. О.</i>	ОБМЕЖЕННЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ЗА ДОПОМОГОЮ WAF: ВАЖЛИВІСТЬ ІМІТАЦІЇ ДІЙ ПОТЕНЦІЙНОГО ЗЛОВМИСНИКА ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОСТІ ЗАХИСТУ	196
<i>Іщук М.О., Шевченко С.М.</i>	МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПРОВЕДЕННЯ ЕЛЕКТРОННИХ ГОЛОСУВАНЬ	200
<i>Каневецький М. О.</i>	ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ	204
<i>Кузько А.В.</i>	МЕТОДИКА ВИЯВЛЕННЯ DDOS-АТАК НА ОСНОВІ АЛГОРИТМУ ДЕНДРИТНИХ КЛІТИН	207
<i>Чабан Б.В.</i>	МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ НА ОСНОВІ КОМПЛЕКСУВАННЯ ДАНИХ	211
<i>Юхнич Д.В.</i>	РОЗРОБКА БЛОКЧЕЙН-РІШЕННЯ ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ	214

## **СЕКЦІЯ 5. ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЙ**

<i>Юнак Д.О.</i>	ZERO TRUST ТА SOC: СИМБІОЗ СТРАТЕГІЙ ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВ	218
------------------	--	-----

<i>Коврига М.В.</i>	НЕЙРОМЕРЕЖІ ПРОТИ ХАКЕРІВ: ЯК ШТУЧНИЙ ІНТЕЛЕКТ БОРЕТЬСЯ З КІБЕРЗАГРОЗАМИ НА ПЕРЕДОВІЙ	3 221
<i>Рабчун Д.І., к.т.н., доц., Скрипка О.В.</i>	АНАЛІЗ МЕТОДІВ ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ ЦЕНТРУ СЕРТИФІКАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ	224
<i>Делікатний В.А.</i>	ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ	227
<i>Журавель А.В.</i>	ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЯК СПОСІБ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРОТИДІЇ КІБЕРАТАКАМ НА СИСТЕМИ КОМПАНІЇ	229
<i>Кравець С.В.</i>	ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СУЧАСНИХ КІБЕРАТАКАХ: KEYС-ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ	231
<i>Куценко О. С.</i>	МЕТОДИ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ НА ОСНОВІ ПРАВОВИХ, ОРГАНІЗАЦІЙНИХ ТА ТЕХНОЛОГІЧНИХ ПІДХОДІВ	234
<i>Карпенко М.А.</i>	МЕТОДИКА ІНТЕГРАЦІЇ СОЦІОІНЖЕНЕРНИХ СЦЕНАРІЇВ У ПРОЦЕС ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	238
<i>Малаш Д. О.</i>	ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ	240

## СЕКЦІЯ 6. БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

<i>Kotukh Yevgen Alexander Wyglinski Xiaoyan Sherry Sun Кривов'яз І.Я.</i>	POST-QUANTUM SECURITY ASSESSMENT OF 5G PROTOCOLS ACROSS OSI LAYERS	244
	АУДИТ ЯК ЕФЕКТИВНИЙ ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	249
<i>Савченко В.А., д.т.н., проф., Возняк Р.М., д.філософії, Сампір О.М., д.філософії</i>	ІГРОВА МОДЕЛЬ ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК	251

## СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

<i>Макаренко А. В.</i>	РОЛЬ ДЕРЖАВНОЇ ПОЛІТИКИ У ПІДВИЩЕННІ ОБІЗНАНОСТІ ПРО КІБЕРБЕЗПЕКУ	255
<i>Паламарчук І.В.</i>	ІННОВАЦІЙНІ ПІДХОДИ ДО НАВЧАННЯ КІБЕРБЕЗПЕКИ: ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ТА ДОПОВНЕНОЇ РЕАЛЬНОСТІ	258
<i>Гурінов Н.В.</i>	МЕТОДИ РОЗПІЗНАВАННЯ ФЕЙКОВИХ ПРОФІЛІВ В ПРОФЕСІЙНИХ СОЦІАЛЬНИХ МЕРЕЖАХ	262
<i>Мельниченко Н.М.</i>	КІБЕРГІГІЄНА ЯК ОСНОВА БЕЗПЕЧНОГО ЦИФРОВОГО СЕРЕДОВИЩА	266
<i>Сколота В.В.</i>	ГЕЙМІФІКАЦІЯ НАВЧАЛЬНИХ ПРОГРАМ З ВИЯВЛЕННЯ ФІШИНГОВИХ ЗАГРОЗ	268
<i>Родіонов В.Ю.</i>	ІННОВАЦІЙНІ НАВЧАЛЬНІ ТЕХНОЛОГІЇ З КІБЕРБЕЗПЕКИ: СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ.	272
<i>Новохатній Д.Ю.</i>	ВИКОНАННЯ ЗАХОДІВ З КІБЕРГІГІЄНИ (КІБЕРБЕЗПЕКИ) ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННИХ ПРИСТРОЇВ ТА ПРОГРАМНИХ ЗАСТОСУНКІВ	274
<i>Кодимський О.М.</i>	ЕТИКА В КІБЕРПРОСТОРІ: ВІДПОВІДАЛЬНІСТЬ КОРИСТУВАЧІВ ЗА ЦИФРОВИЙ СЛІД	277
<i>Оніщенко В.О.</i>	ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ ЯК ЗАСІБ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ	280
<i>Редькіна А.В.</i>	РІВЕНЬ ОБІЗНАНОСТІ ПЕРСОНАЛУ ЯК ВИЗНАЧАЛЬНИЙ ЧИННИК ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ	283
<i>Сніжко В. М.</i>	ПРОБЛЕМИ Й ВИКЛИКИ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ З КІБЕРБЕЗПЕКИ	286

## СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

<i>Дарій В.Р.</i>	ПІДХІД ЄВРОПЕЙСЬКОГО СОЮЗУ ДО КІБЕРБЕЗПЕКИ У СФЕРІ ЗАКОНОДАВСТВА	289
<i>Коровін В.П.</i>	ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРІНЦИДЕНТИ: ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ У ПРОТИДІЇ КІБЕРЗАГРОЗАМ ДЛЯ БІЗНЕСУ	293
<i>Борисюк Д.Ю.</i>	ПРАВОВЕ РЕГУЛЮВАННЯ ТА	295

<i>Астащенко М. О.</i>	СТАНДАРТИЗАЦІЯ ЗАХОДІВ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗАКОНОДАВЧА ТА НОРМАТИВНА БАЗА КІБЕРСТІЙКОСТІ	298
<i>Касторнов К. Ф.</i>	PCI DSS ТА SWIFT: ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ ВІДПОВІДНОСТІ	301

# СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

## МЕТОДИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

**Осауленко В. Р.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Враховуючи інтенсивний розвиток інформаційно-комунікаційних систем (ІКС) та збільшення кількості кіберзагроз, методи виявлення та блокування шкідливого програмного забезпечення (ШПЗ) набувають особливого значення. Ефективний захист інформаційних ресурсів базується на комплексному підході, що включає як традиційні, так і сучасні технології.

Аналіз підписів (Signature-based Detection) заснований на порівнянні файлів із базами відомих зразків шкідливого програмного забезпечення. Якщо знайдено збіг, файл вважається загрозою. Основним недоліком такого методу є його неефективність щодо нових або змінених загроз, оскільки вони ще не внесені в базу.

Аналіз поведінки (Behavior-based Detection) полягає у відстеженні активності програм у реальному часі. Якщо програма здійснює підозрілі дії, наприклад, змінює системні файли або намагається отримати несанкціонований доступ до даних, вона блокується. Даний метод ефективний проти невідомих загроз, однак може спричиняти хибні спрацьовування.

Евристичний аналіз (Heuristic Analysis) аналізує код програм та оцінює його можливу шкідливість. Використовується для виявлення шкідливого ПЗ, яке ще не було ідентифіковано традиційними методами. Основною перевагою є можливість виявлення загроз ще до їхнього масового поширення.

Методи штучного інтелекту (AI/ML-based Detection) включають використання алгоритмів машинного навчання для аналізу великих обсягів даних і виявлення аномалій у поведінці файлів або мережевого трафіку. Вони здатні адаптуватися до нових загроз та виявляти їх без наявності заздалегідь створених сигнатур.

Системи виявлення вторгнень (IDS/IPS) використовують аналіз мережевого трафіку для виявлення та блокування потенційних загроз. IDS (Intrusion Detection System) сповіщає адміністратора про виявлену підозрілу активність, тоді як IPS (Intrusion Prevention System) може автоматично блокувати загрози.

Контроль доступу (Access Control) передбачає обмеження доступу до важливих ресурсів лише для авторизованих користувачів. Використовується рольова модель доступу (RBAC) та багатофакторна автентифікація (MFA), що суттєво знижує ризик несанкціонованого проникнення.

Оновлення програмного забезпечення (Patch Management) полягає у своєчасному встановленні оновлень для операційних систем та програмного забезпечення, що усуває вразливості, які можуть бути використані зловмисниками.

Фаєрволи та системи фільтрації трафіку (Firewalls & Traffic Filtering) забезпечують контроль вхідного та вихідного трафіку, блокуючи небезпечні підключення. Це дозволяє запобігти атакам, таким як DDoS або проникнення через відкриті порти.

DLP-системи (Data Loss Prevention) призначені для моніторингу та запобігання витокам конфіденційної інформації. Вони можуть обмежувати передачу даних через електронну пошту, USB-накопичувачі та хмарні сервіси, забезпечуючи додатковий рівень захисту інформації.

Навчання персоналу є важливим аспектом захисту, адже однією з головних загроз безпеці є людський фактор. Проведення тренінгів для співробітників щодо безпечного користування мережевими ресурсами та

розпізнавання методів соціальної інженерії допомагає зменшити ймовірність успішних атак.

Реалізація зазначених методів сприяє ефективному захисту інформаційних систем від сучасних загроз, забезпечуючи високий рівень кібербезпеки організації.

### **Література**

1. Кабінет Міністрів України. Розпорядження №481-р про затвердження плану заходів з реалізації Стратегії кібербезпеки України. URL: <http://zakon.rada.gov.ua/laws/show/96/2016>
2. ISO/IEC 27001:2013. Інформаційні технології – Методи управління безпекою. URL: <https://www.iso.org/standard/54534.html>
3. NIST Special Publication 800-53. Security and Privacy Controls for Information Systems. URL: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

## **СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ**

**Єрмоленко В. А.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасних умовах кіберзагрози стають дедалі складнішими та масштабнішими, що вимагає впровадження комплексних підходів до забезпечення кіберстійкості підприємств. Дана робота розглядає ключові стратегії управління ризиками, заходи безперервності бізнесу та інноваційні

технології захисту інформаційних систем. Особлива увага приділяється аналізу ризиків, методам запобігання кіберзагрозам та інструментам виявлення атак.

### Основні аспекти дослідження

#### 1. Ключові виклики та загрози кібербезпеки

- Аналіз тенденцій розвитку кіберзагроз у 2025 році.
- Найпоширеніші кібератаки: фішинг, DDoS, атаки на ланцюг постачання.
- Наслідки атак для компаній: фінансові втрати, витоки даних, порушення роботи бізнесу.

#### 2. Управління ризиками та стратегії забезпечення кіберстійкості

- Основні методи аналізу ризиків:
  - ISO/IEC 27005
  - NIST Risk Management Framework (RMF)
- Розробка стратегій мінімізації ризиків та планування відновлення бізнесу.
- Використання штучного інтелекту та автоматизації у сфері кібербезпеки.

Таблиця 1.

### **Порівняльний аналіз методологій управління ризиками**

<b>Методологія</b>	<b>Основний фокус</b>	<b>Переваги</b>
ISO/IEC 27005	Аналіз та управління ризиками	Висока адаптивність
NIST RMF	Фреймворк безпеки	Деталізованість процесу

#### 3. Технологічні аспекти кіберзахисту

- Використання штучного інтелекту для моніторингу та виявлення загроз.
- Інструменти SIEM, SOAR для аналізу даних та автоматизації безпеки.
- Захист корпоративних мереж: сучасні протоколи безпеки та засоби аутентифікації.

#### 4. Освітні та організаційні аспекти формування культури кібербезпеки

- Вплив людського фактора на кіберстійкість організації.
- Навчальні програми та тренінги для підвищення обізнаності працівників.

працівників.

- Розробка політик безпеки для мінімізації ризиків.

Забезпечення кіберстійкості підприємств потребує комплексного підходу, який поєднує управління ризиками, використання сучасних технологій та підвищення рівня кіберосвіти персоналу. Впровадження інноваційних рішень та міжнародних стандартів безпеки дозволить підприємствам мінімізувати наслідки кібератак і забезпечити безперервність бізнес-процесів.

### **Література**

1. NIST Cybersecurity Framework (2024). URL: [https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf?utm\\_source=chatgpt.com](https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf?utm_source=chatgpt.com)
2. ENISA Threat Landscape 2024. Доступно за посиланням: URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
3. OWASP Top Ten Security Risks (2024). URL: <https://owasp.org/www-project-top-ten/>

## **МЕТОДИ ТА ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ БІЗНЕСУ В УМОВАХ ДИНАМІЧНИХ ЗАГРОЗ КІБЕРПРОСТОРУ**

**Ілляшенко О. М.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Забезпечення стійкості бізнесу в умовах динамічних загроз кіберпростору вимагає поєднання проактивних заходів кібербезпеки, стратегій адаптивної

стійкості та добре інтегрованої системи управління. Стійкість кібербезпеки має важливе значення для підтримання безперервності роботи, зменшення фінансових втрат і збереження репутації організації в умовах мінливих кіберризиків.

Багаторівнева стратегія захисту підвищує стійкість бізнесу до кіберзагроз. Організації впроваджують архітектуру нульової довіри (ZTA) для забезпечення суворої перевірки ідентичності, запобігаючи несанкціонованому доступу до критично важливих систем. Рішення для виявлення та реагування на кінцевих точках (EDR) сприяють виявленню загроз у режимі реального часу, скорочуючи час перебування кібервтогнення. Рішення Secure Access Service Edge (SASE) інтегрує функції мережевої безпеки з хмарними можливостями, забезпечуючи надійний захист від розподілених атак.

Інтеграція штучного інтелекту (ШІ) в кібербезпеку посилює адаптивне виявлення загроз та реагування на інциденти. Моделі машинного навчання аналізують величезні масиви даних для виявлення аномальної активності, що дає змогу автоматизувати пом'якшення загроз. Платформи для організації, автоматизації та реагування на інциденти на основі штучного інтелекту (SOAR) спрощують обробку інцидентів, автоматизуючи процеси стримування та усунення загроз [1].

Методології оцінки ризиків підвищують стійкість бізнесу завдяки виявленню вразливостей і впровадженню цільових стратегій мінімізації ризиків. Системи кількісної оцінки кіберризиків оцінюють фінансовий вплив кіберінцидентів, визначаючи інвестиції в інфраструктуру кібербезпеки. Модель FAIR (Факторний аналіз інформаційних ризиків) та система MITRE ATT&CK полегшують структуровану оцінку ризиків, покращуючи процес прийняття рішень в управлінні кібербезпекою.

Рамки кіберстійкості забезпечують структуровані підходи до подолання кіберзбоїв. Рамкова концепція кібербезпеки NIST (NIST Cybersecurity Framework, CSF) визначає п'ять основних функцій: Ідентифікація, захист, виявлення, реагування і відновлення, забезпечуючи комплексне управління

ризиками. Управління безперервністю бізнесу (BCM) інтегрує стійкість кібербезпеки в більш широке планування безперервності, забезпечуючи швидке відновлення після кіберінцидентів. Відповідність стандарту ISO 22301 посилює стійкість завдяки впровадженню аналізу впливу на бізнес (BIA) та стратегій реагування на інциденти.

Безпечне управління ланцюгами постачання знижує ризики, пов'язані із залежністю від третіх сторін. Організації проводять аудити кібербезпеки та впроваджують суворі політики управління ризиками постачальників, щоб зменшити загрози для ланцюгів постачання. Технологія блокчейн підвищує прозорість ланцюгів поставок, забезпечуючи захист записів від несанкціонованого втручання, зменшуючи вразливість до кібершахрайства [2].

Дотримання нормативних вимог зміцнює стійкість бізнесу шляхом приведення практик кібербезпеки у відповідність до законодавчих вимог. Загальний регламент про захист даних (GDPR) вимагає суворих заходів захисту даних, мінімізуючи ризики, пов'язані з їх витоком. Сертифікація моделі зрілості кібербезпеки (СММС) забезпечує контроль безпеки в оборонних ланцюгах постачання, посилюючи стійкість національної безпеки.

Практики кібергігієни сприяють підвищенню обізнаності працівників і зменшують ризики людського фактору. Організації впроваджують навчальні програми з підвищення обізнаності про безпеку, симуляції фішингу і багатофакторну автентифікацію (MFA) для запобігання атакам на основі облікових даних. Поведінкова аналітика виявляє відхилення в активності користувачів, запобігаючи внутрішнім загрозам і несанкціонованому доступу до даних.

Аварійне відновлення та планування резервування забезпечують швидке відновлення роботи після кіберінцидентів. Хмарні рішення для резервного копіювання, незмінні сховища та розподілена реплікація даних знижують ризики, пов'язані з атаками програм-вимагачів та пошкодженням даних. Інструкції з реагування на інциденти містять структуровані плани дій для

пом'якшення наслідків кіберкриз, що забезпечують скоординованість зусиль з відновлення.

Співпраця між державним і приватним секторами посилює колективну стійкість до кібербезпеки. Обмін розвіданими про загрози через Центри обміну та аналізу інформації (ISAC) сприяє ранньому виявленню загроз, посилюючи потенціал кібербезпеки в масштабах всієї галузі. Урядові ініціативи з кібербезпеки сприяють зміцненню національної стійкості шляхом впровадження заходів захисту критично важливої інфраструктури [3].

Постійне вдосконалення стійкості до кіберзагроз забезпечує безперервність бізнес-операцій в умовах еволюції кіберзагроз. Організації впроваджують проактивні методи пошуку загроз, тестування на проникнення та вправи з об'єднання команд для виявлення та пом'якшення нових загроз. Моделі зрілості стійкості до кіберзагроз оцінюють готовність організації, спрямовуючи стратегічне вдосконалення можливостей безпеки.

Забезпечення стійкості бізнесу вимагає цілісного підходу, що поєднує стійкість до кібербезпеки, управління ризиками, дотримання нормативних вимог та технологічні інновації. Організації, які проактивно адаптуються до динамічних кіберзагроз, підвищують свою довгострокову життєздатність і підтримують безперервність роботи в дедалі більш ворожому цифровому середовищі.

## Література

1. Adebimpe Bolatito Ige, Eseoghene Kupa, Oluwatosin Ilori. Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Advanced Research and Reviews*. 2024. Vol. 19, no. 3. P. 344–360. URL: <https://doi.org/10.30574/gscarr.2024.19.3.0236>
2. Safitra M. F., Lubis M., Fakhurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*. 2023. Vol. 15, no. 18. P. 13369. URL: <https://doi.org/10.3390/su151813369>

4. The role of cyber security in advancing sustainable digitalization: Opportunities and challenges / S. S. Goswami et al. *Journal of Decision Analytics and Intelligent Computing*. 2023. Vol. 3, no. 1. P. 270–285. URL: <https://doi.org/10.31181/jdaic10018122023g>

## **СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ**

**Коваль М. А., к.т.н., Бобровський О. В., к.т.н.,  
Геращенко І. О., к.держ.упр., Никитюк А. П.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасний розвиток інформаційних технологій і кібербезпеки зумовлює необхідність постійного удосконалення методів захисту даних та управління ризиками в умовах цифрової трансформації. Аналіз основних підходів до забезпечення кіберстійкості демонструє, що ефективне управління ризиками є ключовим елементом безперервності бізнес-процесів.

### **Ключові аспекти дослідження:**

1. Визначення стратегій кіберстійкості для підприємств.
2. Оцінка ефективності сучасних методів управління кіберризиками.
3. Інноваційні технології для забезпечення безпеки інформаційних систем.
4. Вплив нормативно-правових актів на кібербезпеку бізнесу. Перспективи розвитку законодавчої бази у сфері кібербезпеки.

**Захист бізнес-процесів від впливу кібератак**

Захист бізнес-процесів від впливу кібератак. Включає впровадження багаторівневих систем безпеки, моніторинг загроз у режимі реального часу, використання сучасних технологій виявлення та запобігання атакам, а також розробку стратегій швидкого реагування на інциденти для мінімізації простоїв і фінансових втрат.

### **Приклад успішного впровадження кіберстійкості**

Реалізація стратегії кіберстійкості передбачає застосування комплексного підходу, що включає впровадження сучасних систем кіберзахисту, регулярний моніторинг загроз, навчання персоналу та розробку планів реагування на інциденти. Практичні приклади демонструють, що використання таких заходів дозволяє значно знизити ризики та підвищити рівень безпеки інформаційних систем.

### **Методології оцінки ризиків у кібербезпеці.**

Ефективне управління ризиками починається з їх ідентифікації та оцінки. Сучасні методології включають кількісний та якісний аналіз, використання стандартів, таких як ISO/IEC 27005, NIST Risk Management Framework. Застосування цих підходів дозволяє бізнесу адаптувати свої захисні стратегії відповідно до реальних загроз.

### **Роль людського фактора у кіберстійкості.**

Роль людського фактора у кіберстійкості. Людський фактор залишається однією з найважливіших складових кібербезпеки. Недостатня обізнаність працівників про ризики, фішингові атаки та небезпечна поведінка можуть стати причиною серйозних загроз. Запровадження регулярних тренінгів, політик безпечного використання інформаційних систем та тестування персоналу значно підвищує рівень кіберстійкості організації.

### **Інноваційні технології для забезпечення кіберстійкості.**

Використання штучного інтелекту, машинного навчання, блокчейн-технологій і автоматизованих рішень дозволяє значно покращити рівень безпеки. Ці інструменти допомагають швидко виявляти загрози, аналізувати великі обсяги даних і прогнозувати можливі атаки.

### **План реагування на кіберінциденти.**

Включає комплекс заходів, які допомагають швидко виявити, ізолювати та нейтралізувати загрозу, а також мінімізувати збитки для компанії. Розробка чітких сценаріїв реагування, проведення навчань та тестування системи безпеки дозволяє ефективно протидіяти кіберзагрозам.

### **Стратегії відновлення бізнесу після кібератак – аналіз методів швидкого відновлення бізнес-процесів після кіберзагроз.**

Стратегії відновлення бізнесу після кібератак передбачають комплексні заходи, спрямовані на мінімізацію наслідків інцидентів та швидке повернення до нормального функціонування. Важливими етапами є створення резервних копій даних, розробка чітких планів реагування та аварійного відновлення, а також впровадження механізмів автоматичного відновлення критичних систем. Після усунення загроз необхідно провести детальний аналіз інциденту, вдосконалити заходи безпеки та протестувати ефективність відновлювальних процедур.

### **Екосистема кібербезпеки: ключові напрями та компоненти**

Нище додаю схему 1, яка представляє екосистему інформаційної та кібернетичної безпеки, що охоплює ключові аспекти захисту даних, аналізу загроз, ідентифікації доступу та розслідування інцидентів.

У центрі знаходиться головна тема – "**Екосистема інформаційної та кібернетичної безпеки**", а навколо неї розміщені основні напрями:

1. **Захист даних** – включає основи безпеки конфіденційної інформації та адміністрування захищених баз даних.
2. **Аналіз загроз та вразливостей** – передбачає оцінку ризиків та аналіз шкідливого програмного забезпечення.
3. **Захист кінцевих точок** – спрямований на безпеку пристроїв та адміністрування антивірусного програмного забезпечення.
4. **Безпека мереж** – забезпечує захист комп'ютерних мереж та адміністрування мережевих систем безпеки.

5. **Розслідування інцидентів** – включає цифрову криміналістику та аналіз кіберзагроз.
6. **Криптографія** – охоплює стандарти шифрування, управління ключами та прикладні криптографічні технології.
7. **Захист додатків** – спрямований на безпеку веб-додатків та аналіз програмного забезпечення.
8. **Ідентифікація та доступ** – контролює захист автоматизованих систем та управління доступом користувачів.

Ця схема демонструє взаємопов'язаність різних аспектів кібербезпеки та важливість комплексного підходу до захисту інформаційних систем.



Схема 1. Екосистема кібербезпеки: ключові напрями та компоненти

Таблиця 1.

**Основні компоненти стратегії кіберстійкості**

Компонент	Опис
Ідентифікація ризиків	Виявлення можливих загроз та оцінка їхнього впливу на бізнес-процеси.
Захист даних та систем	Використання шифрування, багаторівневої автентифікації та мережевих екранів.

Моніторинг та виявлення загроз	Впровадження планів реагування, швидке усунення загроз та відновлення роботи.
Реагування на інциденти	Використання резервного копіювання та стратегій бізнес-континуїті.
Відновлення після атак	Проведення тренінгів, тестування на стійкість до фішингових атак.
Нормативне регулювання	Дотримання міжнародних стандартів (ISO 27001, NIST, GDPR).
Нормативне регулювання	Дотримання міжнародних стандартів (ISO 27001, NIST, GDPR).

Розвиток цифрових технологій і постійне зростання кіберзагроз вимагають комплексного підходу до забезпечення кіберстійкості бізнесу. Ефективне управління ризиками, впровадження сучасних технологій захисту та навчання персоналу є ключовими факторами у створенні стійкої кібербезпеки. Використання міжнародних стандартів і найкращих практик дозволяє мінімізувати ризики атак та забезпечити безперервність бізнес-процесів. Впровадження стратегій кіберстійкості сприяє не лише захисту компанії від потенційних загроз, а й підвищенню її конкурентоспроможності на ринку. У сучасних умовах ефективна кібербезпека є необхідністю, а не додатковим елементом управління компанією, що потребує постійної адаптації до змін цифрового середовища.

### Література

1. ISO 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems.
2. ISO/IEC 27001:2013 – міжнародний стандарт управління інформаційною безпекою, с. 10-25.
3. NIST Cybersecurity Framework – національний інститут стандартів і технологій США, с. 30-50.
4. Schneier B. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" – основи криптографії, с. 100-150.

5. Stallings W. "Network Security Essentials" – базові принципи мережевої безпеки, с. 50-90.

6. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. №481-р Про затвердження плану заходів з реалізації Стратегії кібербезпеки України.

## **РОЛЬ КІБЕРБЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ БЕЗПЕРЕРВНОЇ РОБОТИ КОМПАНІЙ**

**Миколаєнко О. С.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Кібербезпека відіграє вирішальну роль у забезпеченні безперервності бізнесу, зменшуючи ризики, пов'язані з кіберзагрозами, витоком даних та системними збоями. Організації інтегрують стратегії кібербезпеки в свої системи управління безперервністю бізнесу (BCM) для захисту критично важливих процесів і підтримки операційної стабільності в умовах кіберінцидентів.

Оцінка ризиків має фундаментальне значення для кібербезпеки в контексті безперервності бізнесу. Аналіз впливу на бізнес (BIA) визначає критичні процеси та оцінює потенційний вплив кіберзагроз на ці операції. Ключові параметри, такі як цільовий час відновлення (RTO), цільова точка відновлення (RPO) та максимально допустимий час простою (MTD), визначають стійкість організації до кіберзбоїв. Ефективне управління ризиками передбачає визначення засобів контролю безпеки на основі стандартів ISO 27001 та ISO 22301, які забезпечують структуровані підходи до зменшення кіберризиків [1].

Стандарт ISO 22301 визначає вимоги до системи управління безперервністю бізнесу (BCMS), гарантуючи, що організації розробляють стратегії для підтримки безперервності під час збоїв, включаючи кіберінциденти. Він вимагає визначення основних бізнес-процесів, їх взаємозалежності та впровадження планів на випадок непередбачуваних ситуацій. Відповідність стандарту ISO 27001 покращує управління інформаційною безпекою шляхом дотримання принципів конфіденційності, цілісності та доступності (CIA), мінімізуючи вплив кіберзагроз на бізнес-операції.

Розвідка кіберзагроз (CTI) підвищує обізнаність про ситуацію та сприяє плануванню безперервності бізнесу, надаючи в режимі реального часу інформацію про нові кіберризики. Організації використовують платформи розвідки загроз для моніторингу вразливостей, виявлення потенційних атак та впровадження превентивних заходів безпеки. Інтеграція CTI з BCM дозволяє проактивно зменшувати ризики, скорочуючи час простою та фінансові втрати внаслідок кіберінцидентів.

Планування реагування на інциденти має вирішальне значення для мінімізації операційних наслідків кібератак. Чітко визначена система реагування на інциденти забезпечує швидке виявлення, локалізацію та відновлення після порушень безпеки. Організації впроваджують операційні центри безпеки (SOC) для постійного моніторингу та аналізу подій безпеки, що дозволяє виявляти загрози в режимі реального часу та координувати реагування на інциденти. Автоматизовані механізми реагування, в тому числі виявлення загроз за допомогою штучного інтелекту (ШІ), підвищують ефективність управління інцидентами [2].

Рамки кіберстійкості узгоджують заходи з кібербезпеки з цілями безперервності бізнесу для підвищення організаційної стабільності. Концепція кібербезпеки NIST визначає п'ять основних функцій - ідентифікація, захист, виявлення, реагування та відновлення - які допомагають організаціям інтегрувати кібербезпеку з BCM. Застосовуючи багаторівневий підхід до

захисту, організації покращують свою здатність протистояти кіберзагрозам і підтримувати безперебійну роботу.

Дотримання нормативних вимог посилює роль кібербезпеки в забезпеченні безперервності бізнесу. Директива Європейського Союзу NIS2 та Загальний регламент про захист даних (GDPR) вимагають від організацій впроваджувати надійні заходи безпеки для захисту критично важливої інфраструктури та конфіденційних даних. Невиконання цих норм призводить до юридичних і фінансових санкцій, що підкреслює необхідність інтеграції кібербезпеки з ОБФ.

Роль кібербезпеки в забезпеченні безперервності бізнесу поширюється і на управління ризиками ланцюгів постачання. Організації оцінюють практики безпеки третіх сторін, щоб зменшити ризики, пов'язані із залежністю від постачальників. Заходи безпеки ланцюгів постачання включають проведення аудитів безпеки, забезпечення дотримання договірних вимог безпеки та впровадження моніторингу мереж постачальників у режимі реального часу для виявлення аномалій і потенційних порушень.

Програми навчання та підвищення обізнаності з кібербезпеки мають важливе значення для зміцнення стратегій безперервності бізнесу. Співробітники відіграють вирішальну роль у запобіганні кіберзагрозам, дотримуючись політики безпеки та виявляючи потенційні ризики. Регулярні тренінги з безпеки, симуляції фішингу та практики кібергігієни підвищують готовність персоналу, зменшуючи ймовірність успішних кібератак [3].

Інтеграція кібербезпеки з плануванням післяаварійного відновлення забезпечує швидке відновлення бізнес-операцій після кіберінциденту. Організації створюють резервні копії даних, впроваджують системи обходу відмов і встановлюють хмарні рішення для відновлення, щоб мінімізувати час простою. Тестування післяаварійного відновлення підтверджує ефективність цих заходів, забезпечуючи операційну стійкість під час кіберкриз.

Постійне вдосконалення систем кібербезпеки та ОБФ є необхідним для адаптації до нових кіберзагроз. Організації проводять періодичну оцінку

ризиків, оновлюють політики безпеки та використовують передові технології виявлення загроз, щоб підвищити свою кіберстійкість. Застосовуючи проактивний підхід, організації забезпечують безперервність бізнесу в умовах дедалі складнішого ландшафту кіберзагроз.

### Література

1. Fortifying Organizational Cyber Resilience: An Integrated Framework for Business Continuity and Growth amidst Escalating Threat Landscapes / A. Kanaan et al. *International Journal of Computing and Digital Systems*. 2025. Vol. 17, no. 1. P. 1–14. URL: <https://doi.org/10.12785/ijcds/1571023809>

2. Katarína MÄKKÁ, Katarína KAMPOVÁ. Cyber Security and Business Continuity Management: Ensuring Resilience in a Digital World. *Challenges to National Defence in Contemporary Geopolitical Situation*. 2024. Vol. 1, no. 1. URL: <https://doi.org/10.3849/cndcgs.2024.326>

3. Cybersecurity and Business Survival in Nigeria: Building Customer's Trust / E. A. Onatuyeh et al. *AFRICAN JOURNAL OF APPLIED RESEARCH*. 2025. Vol. 11, no. 1. P. 786–813. URL: <https://doi.org/10.26437/ajar.v11i1.882>

## ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА АВТОМАТИЗОВАНИХ СИСТЕМ У СТРАТЕГІЇ КІБЕРБЕЗПЕКИ ЯК КЛЮЧ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ: НОВІ ГОРИЗОНТИ В ІДЕНТИФІКАЦІЇ ТА МІНІМІЗАЦІЇ РИЗИКІВ

**Баранов Н. Б.**

Державний університет інформаційно комунікаційних технологій

м. Київ, Україна

Кіберзагрози та їх вплив на бізнес-середовище. Сучасний бізнес-середовище постійно змінюється під впливом нових технологій, що, в свою

чергу, відкриває нові можливості, але також створює нові ризики. Однією з найбільших загроз для організацій є кіберзагрози. Кіберзлочинці постійно вдосконалюють свої методи атаки, що ставить під сумнів ефективність традиційних підходів до забезпечення безпеки. У цьому контексті одним із важливих аспектів є забезпечення безперервності бізнесу — здатності компанії функціонувати без перерв у разі виникнення кіберінцидентів. Забезпечення безперервності бізнесу включає низку заходів, спрямованих на мінімізацію ризиків, швидке відновлення після інцидентів та оптимізацію процесів, аби організація могла продовжувати свою діяльність навіть в умовах серйозних кіберзагроз. Традиційні методи захисту часто не здатні впоратися з динамічними загрозами кіберпростору, оскільки вони здебільшого побудовані на передбачуваних сценаріях атак [1]. У таких умовах особливо важливим стає застосування новітніх технологій, таких як штучний інтелект (ШІ), який дозволяє створити більш адаптивні та прогностичні стратегії кіберзахисту.

Штучний інтелект як інструмент адаптації до змінних кіберзагроз. Штучний інтелект і машинне навчання є тими технологіями, що дозволяють значно покращити стратегії управління кіберризиками. Традиційні методи кібербезпеки, що базуються на фіксованих правилах і підходах до виявлення загроз, стають менш ефективними у світі, де кіберзлочинці постійно змінюють тактики і методи атак. ШІ здатен адаптуватися до нових загроз і самостійно покращувати свої алгоритми виявлення з часом, що значно підвищує ефективність системи захисту. Інтеграція ШІ в стратегію кібербезпеки дозволяє використовувати такі підходи, як автоматичне виявлення аномалій і аномальних поведінкових патернів в мережах і системах, що є основою для своєчасного виявлення кібератак. Оскільки ШІ здатен аналізувати величезні обсяги даних в реальному часі, він може виявляти навіть найскладніші та незвичні загрози, яких неможливо було б виявити за допомогою традиційних методів захисту [2]. Системи на основі ШІ можуть також автоматично реагувати на загрози, обираючи найбільш ефективний спосіб нейтралізації загрози без участі людини, що значно знижує час реагування та мінімізує

потенційні збитки для організації. Крім того, ШІ здатен здійснювати моніторинг в режимі реального часу, що дозволяє своєчасно виявляти вразливості та потенційні слабкі місця системи безпеки, а також прогнозувати можливі ризики [3].

Адаптивність та самонавчання в управлінні кіберризиками. Один із найбільших переваг використання ШІ в кібербезпеці — це здатність до самонавчання. ШІ-системи можуть самостійно покращувати свою ефективність на основі нових даних і досвіду, що дозволяє їм швидко адаптуватися до змінюваних умов. Це особливо важливо в умовах швидко змінюваного кіберпростору, де нові загрози можуть виникати буквально щодня. Процес самонавчання на основі великих даних (big data) дозволяє системам на основі ШІ виявляти нові типи атак, які не були передбачені традиційними алгоритмами. Наприклад, використання ШІ дозволяє розпізнавати фішингові атаки, які не схожі на традиційні методи, а також нові типи зловмисного програмного забезпечення, яке може змінювати свою поведінку в реальному часі. Крім того, алгоритми машинного навчання здатні прогнозувати ймовірність виникнення різних кіберінцидентів, що дозволяє вжити превентивних заходів до того, як загроза стане реальною. Це дозволяє підприємствам розробляти більш ефективні стратегії управління ризиками, що включають не лише реагування на інциденти, але й їх прогнозування та попередження [4].

Роль штучного інтелекту у забезпеченні безперервності бізнесу. Одним із ключових аспектів, на які ШІ може вплинути в рамках забезпечення безперервності бізнесу, є автоматизація процесів відновлення після інцидентів. У разі кібератаки або іншого кіберінциденту ШІ здатний оперативно визначити масштаби збитків, виявити пошкоджені системи й автоматично ініціювати відновлення або переключення на резервні системи, забезпечуючи таким чином мінімальні втрати та час простою для бізнесу [5]. ШІ може також бути інтегрований у процеси безперервного моніторингу та забезпечення доступності критичних бізнес-сервісів. За допомогою інтелектуальних

алгоритмів можна оцінювати ймовірність відмови або витоку даних у реальному часі, що дозволяє вжити заходів до того, як ці інциденти почнуть впливати на бізнес-процеси. Крім того, автоматизовані системи на базі ШІ можуть забезпечувати постійну ідентифікацію нових кіберзагроз, що дозволяє організаціям оперативного адаптувати свої стратегії безпеки відповідно до нових викликів і мінімізувати час, протягом якого компанія залишається вразливою до атак.

Штучний інтелект як основа для стійких і гнучких кіберстратегій. Застосування штучного інтелекту в управлінні кіберризиками не лише підвищує рівень безпеки компанії, але й забезпечує більш гнучкий, адаптивний підхід до реагування на сучасні кіберзагрози [6]. Це дозволяє організаціям не лише захищати свої дані та системи, але й забезпечувати безперервність бізнес-процесів, що є критично важливим в умовах постійно змінюваного кіберпростору. ШІ допомагає бізнесу не лише реагувати на загрози, але й передбачати їх, створюючи таким чином систему кіберстійкості, що здатна адаптуватися до нових викликів. Інтеграція цих технологій у стратегії кіберзахисту стає не просто необхідною, а й основою для досягнення сталого розвитку організацій в умовах сучасних кіберзагроз. Роль ШІ в забезпеченні безперервності бізнесу зростає, і він має потенціал стати основою для створення нових, більш ефективних підходів до кібербезпеки на глобальному рівні.

## Література

1. Боренков А. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. *BDO*. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023>
2. Захист компаній від кіберзагроз: безоплатні послуги для українського бізнесу. *Дія.Бізнес*. URL: <https://business.diaa.gov.ua/history-of-success/zakhyst-kompanii-vid-kiberzahroz-bezoplatni-posluhy-dlia-ukrainskoho-biznesu>.

3. Захист бізнесу: як убезпечити підприємство від кіберзлочинів?. *EBA*. URL: <https://eba.com.ua/zahyst-biznesu-yak-ubezpechyty-pidpryyemstvo-vid-kiberzlochyniv/>.
4. Основи Кібербезпеки для бізнесу. *WESTELECOM*. URL: <https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa>
5. Рішення для кібербезпеки: Як вибрати ідеальне рішення для бізнесу? *ESKA*. URL: <https://eska.global/blog/rishennya-dlya-kiberbezpeki-yak-vibrati-idealne-rishennya-dlya-biznesu>.
6. Кібербезпека в бізнесі. *UC.Market*. Дослідження ринку та конкурентний аналіз. URL: <https://blog.youcontrol.market/kibierbiezpieka-v-biznisi/>

## **БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ В УКРАЇНІ ПІД ЧАС ВІЙНИ**

**Селіванов І.С.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Війна в Україні створила серйозні виклики для бізнесу, змусивши їх керівників оперативно адаптуватися до нових реалій. Руйнування інфраструктури, проблеми з логістикою, загрози безпеці персоналу та кіберризиками – усе це стало рушієм для перегляду володарів бізнесу власних підходів, щодо управління ризиками. Для подальшого розвитку підприємства необхідно впроваджувати комплексні стратегічні рішення за для того, щоб мінімізувати втрати з боку компанії.

Ключовими викликами безперервності бізнесу під час війни - безпека персоналу (загроза життю персоналу, проблеми з безпекою робочого місця), труднощі логістики (блокування постачать ресурсів, додаткові витрати), кібербезпеки та інформаційні ризики( атаки зловмисників, витік інформації),

перебої в електропостачанні та зв'язку (руйнування енергетичної інфраструктури).

Стратегії, які можна застосувати для забезпечення безперервності бізнесу до кожного виклику які стоять перед підприємством:

Безпека персоналу

– перехід на віддалене місце роботи;

- надання співробітникам психологічної допомоги, фінансової підтримки, та безпечних умов праці;

Логістики та постачання

- пошук альтернативних логістичних маршрутів та перевізників

- використання міжнародних каналів постачання

Захист інформаційних систем

- впровадження резервних ІТ-інфраструктур (хмарні сервіси, VPN).

- регулярне оновлення систем безпеки та навчання персоналу щодо кіберзагроз.

- двофакторна автентифікація та резервне копіювання даних.

Енергетична незалежність та автономність

- використання генераторів, систем резервного живлення, інвестування в альтернативні джерела енергії.

Говорячи про мінімізацію збитків та оптимізацію бізнес - процесів можна виділити:

- гнучкість та адапцію, що в свою чергу говорить про гнучкість моделей управління змін в системі;

- зменшення операційних витрат та скорочення не профільних витрат, оптимізація штату;

- розвиток цифрової економіки, мається на увазі про перехід на онлайн-формат роботи та впровадження цифрових сервісів для автоматизації роботи компанії.

- інвестування в нові технології, звертаючи увагу на ІІІ та автоматизацію процесів

Попри усі виклики, що стоять перед українськими бізнесами, вони демонструють високу стійкість і здатність адаптуватися до кризових умов, використання стратегічного планування, інноваційних рішень та гнучких бізнес-моделей дозволяє не лише мінімізувати ризики та збитки, а й знайти нові можливості для розвитку та зростання. Дивлячись на компанії, які оперативно впроваджують ефективні стратегії, можна зробити наголос на тому, вони мають значно більше шансів на стабільну роботу та самовдосконалення, як під час війни, так і в післявоєнний період.

### Література

1. БЕЗПЕРЕПВНІСТЬ БІЗНЕСУ В УКРАЇНІ: ВИКЛИКИ ТА МОЖЛИВОСТІ В УМОВАХ ВІЙНИ Економіка та суспільство. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/3887>
2. Безперервність бізнесу. Як ІТ-компанія Ciklum працює під час війни. Vector. URL: <https://vctr.media/ua/yednist-yak-ciklum-praczyuye-pid-chas-vijny-131505/>
3. Бізнес під час війни: яку стратегію обрати для адаптації та виживання. Mind.ua. URL: <https://mind.ua/openmind/20250825-biznes-pid-chas-vijni-yaku-strategiyu-obrati-dlya-adaptaciyi-ta-vizhivannya>
4. Це не війна. але деякі військові стратегії можуть врятувати вашу компанію. forbes.ua. Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії. URL: <https://forbes.ua/leadership/biznes-tse-ne-viy-na-ale-deyaki-viyskovii-strategii-mozhut-vryatuvati-vashu-kompaniyu-pidpriemitsya-katerina-zagoriy-rozpovidae-yaki-z-nikh-var-to-zapozichiti-24022025-27453>

# ВАГОМІСТЬ КІБЕРНЕТИКИ В ПОВОЄННИЙ ПЕРІОД

**Капелюшна Т.В., д.е.н., доцент**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Кібернетика — це міждисциплінарна наука, що вивчає принципи управління, зв'язку та регуляції в складних системах, незалежно від їхньої фізичної природи (біологічних, технічних, соціальних тощо). Засновником кібернетики вважається Норберт Вінер, який у 1948 році у своїй праці “Cybernetics: Or Control and Communication in the Animal and the Machine” сформулював основні засади цієї науки (рис. 1) [1].

Зворотний зв'язок	• механізм управління та адаптації в системах
Автоматизація процесів	• алгоритми і технології для керування та оптимізації діяльності
Моделювання складних систем	• аналіз і створення кібернетичних моделей для прогнозування поведінки систем
Самоорганізація та адаптивність	• властивості розумних систем до саморегуляції та зміни відповідно до зовнішніх умов.

Рис.1. Основні засади кібернетики

Кібернетика в епоху розвитку штучного інтелекту, автоматизованих систем управління, кібербезпеки та технологій Інтернету речей (ІоТ) дозволяє:

- підвищити ефективність управління підприємствами та державними структурами через використання алгоритмічних моделей і великих даних;
- забезпечити кібербезпеку шляхом створення адаптивних систем виявлення загроз та реагування на них;
- оптимізувати цифрові комунікації для безперебійної взаємодії людини з інформаційними системами;

– розробляти автономні системи та роботизовані технології, що змінюють підхід до виробництва, транспорту та медицини.

Кібернетика забезпечує ефективний розвиток цифрових технологій та їх інтеграцію в усі сфери інформаційного суспільства. Кібертехнології надають дані в режимі реального часу, прогнозну аналітику та захищені канали зв'язку, які забезпечують стійкість та прийняття обґрунтованих рішень. Використання штучного інтелекту (ШІ), великих даних та заходів кібербезпеки підвищує здатність обробляти масиви інформації, одночасно зменшуючи ризики, пов'язані з дезінформацією, кіберзагрозами та операційними перебоями.

Окрім того, в умовах воєнного стану підприємства функціонують за підвищених ризиків, включаючи інфраструктурні атаки, економічну нестабільність та правову невизначеність. Кіберсистеми дозволяють створювати моделі оцінки ризиків, які враховують зовнішні загрози та внутрішні вразливості, що дає змогу приймати рішення щодо виявлення та пом'якшення кіберзагроз, підвищення ситуаційної обізнаності та посилення цілісності даних.

У повоєнному розвитку кібертехнології сприятимуть відновленню економічних і соціальних систем, зокрема через:

- впровадження хмарних обчислень, блокчейну і штучного інтелекту для модернізації діяльності державного і приватного секторів;
- посилення фінансової кібербезпеки;
- забезпечення надійного кіберзахисту для критично важливих секторів, включаючи енергетику, охорону здоров'я та фінанси;
- смарт-реконструкцію.

Кібернетичні моделі прийняття рішень, такі як: теорія ігор, байєсівські мережі та аналіз ризиків на основі ентропії дозволять економічним одиницям оптимізувати розподіл ресурсів, стратегії реагування та відновлення в умовах невизначеності.

Тож, інтеграція кіберпростору, кіберможливостей у процеси прийняття рішень є необхідною для подолання невизначеності, особливо в післявоєнний період.

### **Література**

1. Norbert, W. Cybernetics or Control and communication in the animal and the machine. Cambridge, MA : The MIT Press, [2019]. “Reissue of the 1961 second edition.” <https://doi.org/10.7551/mitpress/11810.001.0001>

## **КІБЕРШАХРАЙСТВО ЯК СТРАТЕГІЯ ПІДВИЩЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ**

**Рудницький Я. Р.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасних умовах глобальної цифрової трансформації та зростання кількості кіберзагроз забезпечення безперервності бізнесу стає одним із ключових завдань для підприємств. Традиційні засоби захисту інформаційних систем, такі як міжмережеві екрани, антивірусні рішення та системи виявлення вторгнень, не завжди здатні забезпечити своєчасне виявлення та нейтралізацію складних і цілеспрямованих атак. Одним із перспективних підходів, що дозволяє підвищити рівень кіберстійкості організації та забезпечити безперервність її діяльності, є застосування технологій кіберобману (Deception Technology).

Концепція кіберобману ґрунтується на створенні контрольованого середовища, яке імітує реальні інформаційні активи організації з метою виявлення несанкціонованих дій зловмисників. Це середовище включає фальшиві мережеві сервіси, облікові записи, бази даних та інші ресурси, що приваблюють атакувальників, спрямовуючи їхню активність на себе, тим самим

ізолюючи критичні системи підприємства від компрометації. Такий підхід дозволяє не лише виявляти спроби проникнення на ранніх етапах атаки, а й отримувати цінну інформацію про тактики, техніки та процедури (ТТР) зловмисників, що сприяє вдосконаленню системи кібербезпеки [1].

На відміну від традиційних методів виявлення загроз, які здебільшого орієнтовані на аналіз сигнатур та аномальної поведінки, Deception Technology дозволяє формувати активний захист за рахунок навмисного введення атакувальників в оману. Це знижує ефективність використання ними автоматизованих засобів атак, оскільки динамічне адаптування фальшивих активів змушує зловмисників витратити більше часу на взаємодію з пастками, що ускладнює їхнє подальше просування мережею [2]. Крім того, такий підхід забезпечує виявлення навіть тих загроз, які можуть залишатися невидимими для традиційних систем моніторингу, оскільки діяльність у фальшивому середовищі є апіорі підозрілою та не має легітимного використання.

Однією з ключових переваг використання Deception Technology є можливість зниження ризиків дестабілізації бізнес-процесів у разі кібератаки. Завдяки спрямуванню атакувальників на фальшиві активи зменшується ймовірність порушення критично важливих інформаційних систем, що мінімізує час простою та потенційні фінансові втрати. Крім того, технологія кіберобману дозволяє скоротити середній час виявлення інцидентів безпеки, що позитивно впливає на швидкість реагування та ефективність заходів із нейтралізації загроз[3].

Застосування Deception Technology також сприяє підвищенню рівня ситуаційної обізнаності у сфері інформаційної безпеки, оскільки дозволяє безпосередньо спостерігати за поведінкою атакувальників у контрольованому середовищі. Це відкриває можливості для формування більш адаптивних стратегій кіберзахисту, спрямованих на проактивне запобігання загрозам.

Використання технологій кіберобману є ефективним інструментом для забезпечення безперервності бізнесу в умовах сучасних кіберзагроз. Завдяки своїй здатності до раннього виявлення атак, мінімізації негативного впливу на

критичні процеси та підвищення адаптивності системи безпеки, Deception Technology має значний потенціал для інтеграції у комплексні стратегії кіберзахисту підприємств.

### Література:

1. Coiciu I., Militaru G. Improvement of cyber resilience by implementation of a digital business continuity management system: evidence from romania. Proceedings of the international conference on business excellence. 2024. Vol. 18, no. 1. P. 2492–2505. URL: <https://doi.org/10.2478/picbe-2024-0209>
2. Katarína MÄKKÄ, Katarína KAMPOVÁ. Cyber security and business continuity management: ensuring resilience in a digital world. *Challenges to national defence in contemporary geopolitical situation*. 2024. Vol. 1, no. 1. URL: <https://doi.org/10.3849/cndcgs.2024.326>
3. AL-Hawamleh A. Cyber resilience framework: strengthening defenses and enhancing continuity in business security. *International journal of computing and digital systems*. 2024. Vol. 15, no. 1. P. 1315–1331. URL: <https://doi.org/10.12785/ijcds/150193>

## **СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ**

### **МЕТОДИ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ МЕРЕЖАХ**

**Галушко В. Т.**

Державний університет інформаційно-комунікаційних технологій

М.Київ, Україна

Кіберзагрози постійно розвиваються в інтернет середовищі, стаючи більш креативними, новаторськими та критично небезпечними. Тому корпоративні мережі, що є основою функціонування сучасних організацій, знаходяться під перманентною загрозою кібератак.

Виявлення та класифікація інцидентів інформаційної безпеки є ключовими аспектами, оскільки забезпечують кіберзахист та мінімізують ризики у кіберпросторі для користувачів, та зокрема для бізнесу. Ефективна система виявлення загроз є запорукою безпеки та дозволяє своєчасно ідентифікувати потенційні інциденти, визначати їх рівень небезпеки та якомога швидше реагувати на них, тим самим мінімізуючи загрозу та/або запобігаючи значним фінансовим та репутаційним втратам.

Такі методи поділяються на кілька категорій. Основні серед них: сигнатурний аналіз, аналіз аномалій, поведінковий аналіз та методи машинного навчання. Далі коротко про кожен окремо.

Сигнатурний аналіз виконується з використанням баз даних попередніх атак, де кожна загроза має унікальний цифровий відбиток/ сигнатуру тощо. Цей метод ефективний для виявлення відомих атак, однак його основним недолік — нездатність розпізнавати нові, невідомі загрози.

Аналіз аномалій використовує моделі нормальної поведінки системи та мережі для виявлення відхилень, які можуть свідчити про можливу атаку.

Використовуючи цей метод можна виявляти нові загрози, проте такий метод може давати велику кількість помилкових спрацьовувань. Для уникнення таких ситуацій потрібно ретельного налаштувати алгоритми.

Поведінковий аналіз працює за допомогою відстеження дій користувачів та системних процесів. Він виявляє нетипову поведінку, яка може бути сигналом про те, що мережа компроментується. Цей метод добре працює у поєднанні з аналізом аномалій, який був згаданий вище, та дозволяє виявляти загрози, для реалізації яких зловмисники використовують нетипові та складні тактики маскуванню.

Методи машинного навчання та штучного інтелекту є саме такими новаторськими та проривними методами. Їх теж використовують для виявлення загроз у корпоративних мережах. Вони дозволяють аналізувати великі обсяги даних, знаходити закономірності та прогнозувати можливі атаки на основі попередніх даних. Головна перевага цих методів — адаптування до нових загроз, однак для цього потрібно забезпечити значні обчислювальні ресурси та правильно підготувати навчальні дані.

Задля максимально ефективного реагування на наслідки від загроз потрібно максимально точно та швидко ідентифікувати ці загрози. Для цього існує класифікація. Вона дозволяє визначити пріоритетність інцидентів та обрати відповідні заходи для їх усунення. Інциденти зазвичай класифікуються за такими критеріями (рис. 1).

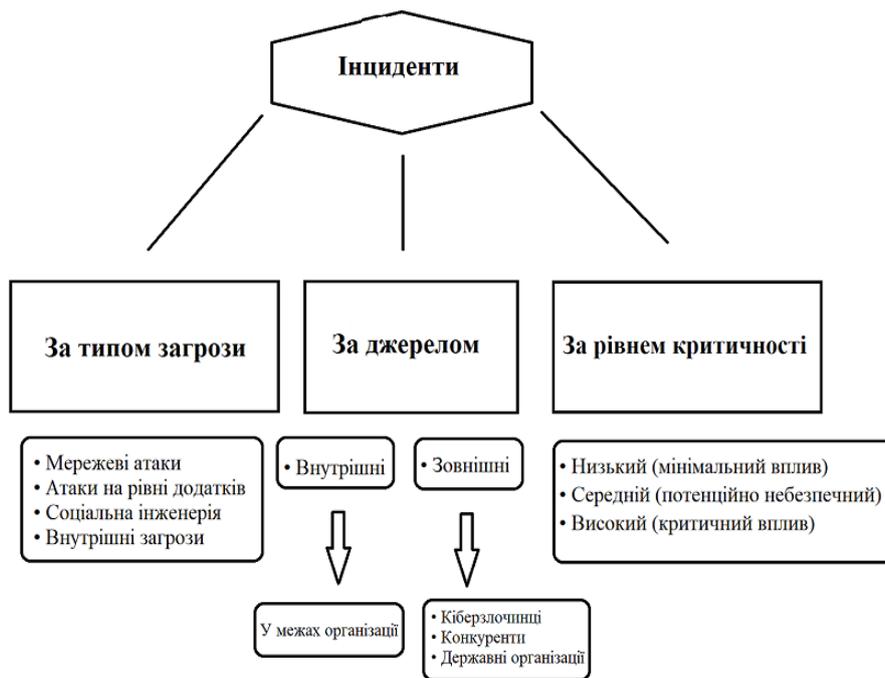


Рис. 1 Класифікація інцидентів за критеріями

Класифікація інцидентів — складний та багатоступеневий процес. Та цей процес виявлення та класифікації інцидентів інформаційної безпеки передбачає кілька ключових етапів (рис. 2).



Рис. 2 Ключові етапи класифікації загроз

Навчання персоналу та підвищення рівня обізнаності співробітників щодо інформаційної безпеки також відіграє важливу роль у мінімізації ризиків. Людський фактор — одна з найпоширеніших причин кіберінцидентів. Регулярні тренінги та симуляції атак є ефективними способами знизити ймовірність виникнення таких інцидентів, що у свою чергу зменшить потенційні ризики та загрози.

Таким чином, ефективні методи виявлення та класифікації інцидентів інформаційної безпеки — критично важливі для захисту корпоративних мереж. Використання сучасних технологій аналізу загроз, автоматизованих систем моніторингу та навчання персоналу дозволяє мінімізувати ризики та підвищити рівень безпеки організації.

### **Література**

1. «ПРАКТИЧНІ АСПЕКТИ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» URL: <https://www.researchgate.net/publication/352430548>
2. ДСТУ ISO/IEC 27017:2017 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг (ISO/IEC 27017:2015, IDT) URL: [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=75487](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=75487)
3. ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти. URL: [https://online.budstandart.com/ua/catalog/doc-page.html?id\\_doc=80310](https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80310)

# **ВАЖЛИВІСТЬ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Зайченко М.В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Наявність вразливостей у сучасних інформаційних системах є однією з ключових проблем кібербезпеки, адже навіть невелика недосконалість у програмному забезпеченні чи його конфігурації може призвести до масштабних кібератак, витоку конфіденційних даних або навіть зупинки критичних бізнес-процесів. Процес виявлення та управління вразливостями забезпечує систематичний підхід до ідентифікації слабких місць, що дозволяє організаціям своєчасно впроваджувати заходи для мінімізації ризиків, пов'язаних із експлуатацією цих недоліків.

По-перше, регулярне сканування систем на предмет вразливостей допомагає виявити потенційні загрози ще до того, як вони будуть використані зловмисниками. Наукові дослідження підтверджують, що своєчасне виявлення вразливостей значно знижує ймовірність успішних кібератак, оскільки дозволяє оперативно встановлювати патчі та коригувати налаштування систем [1]. Такий превентивний підхід є невід'ємною складовою управління ризиками, що базується на стандартах, зокрема ISO/IEC 27005 [2] та рекомендаціях NIST SP 800-30 [3], де наголошується на необхідності безперервного моніторингу та оцінки потенційних загроз.

По-друге, управління вразливостями – це не лише технічна процедура, а й комплексний процес, який включає аналіз ризиків, визначення пріоритетів для виправлень та розподіл ресурсів на основі критичності виявлених недоліків. Такий підхід дозволяє системно підходити до проблем безпеки: від виявлення слабких місць до розробки стратегій їх усунення та подальшої профілактики [4]. Завдяки цьому організації можуть не лише запобігти можливим атакам, а й

ефективно управляти витратами на кібербезпеку, орієнтуючись на найбільш критичні аспекти свого інформаційного середовища.

Крім того, впровадження процесів управління вразливостями сприяє підвищенню загальної обізнаності співробітників про загрози кібербезпеки. А застосування інтегрованих систем моніторингу та аналітики дозволяє не лише фіксувати поточний стан безпеки, а й прогнозувати потенційні загрози, що дає змогу приймати своєчасні управлінські рішення.

Наукові дослідження також вказують на те, що комплексний підхід до управління вразливостями сприяє підвищенню рівня довіри клієнтів та партнерів, що особливо важливо в умовах зростання кібератак у глобальному масштабі. Ефективне виявлення та усунення вразливостей стає своєрідним конкурентною перевагою, адже дозволяє забезпечити безперервність бізнес-процесів та знизити можливі фінансові та репутаційні втрати.

Впровадження систематизованих процесів виявлення та управління вразливостями є надзвичайно важливим для забезпечення інформаційної безпеки. Воно дозволяє не лише своєчасно виявляти потенційні загрози, а й оперативно реагувати на них, мінімізувати ризики, ефективно розподіляти ресурси. Це, в свою чергу, створює фундамент для побудови надійної системи кібербезпеки, яка здатна захистити як критичні інфраструктурні компоненти, так і дані організації від сучасних кібератак.

### **Література**

1. Lai, Y.-P., & Hsia, P.-L. Using the vulnerability information of computer systems to improve network security. *Computer Communications*, 30(9), p. 2032–2047. 2007. URL: <https://doi.org/10.1016/j.comcom.2007.03.007>
2. ISO/IEC 27005:2018. Інформаційні технології. Методи управління ризиками в інформаційній безпеці.
3. NIST SP 800-30. Guide for Conducting Risk Assessments.

4. Поддубний, В. О., Сєверінов, О. В., Пустомельник, О. С. Менеджмент вразливостей як складова частина політики безпеки інформаційних технологій. Харків: ХНУР. 2019.

## **ОЦІНКА СТРАХОВОЇ СТІЙКОСТІ КІБЕРРИЗИКІВ, КЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ: ВИКЛИКИ ТА МОЖЛИВОСТІ**

**Клімченко О. Р.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Кібер-ризик - це еволюціонуючий і все більш значущий виклик у цифровій економіці. Оскільки штучний інтелект (ШІ) стає все більш інтегрованим у бізнес та інфраструктуру, його вразливість до кіберзагроз зростає, що ставить складні питання щодо страхування. Кіберрилик відрізняється від традиційних ризиків своєю системною природою, потенціалом накопичення та мінливими векторами атак. На відміну від матеріальних активів, кіберризик є нематеріальними і важко піддаються кількісній оцінці, що робить традиційні актуарні методи недостатніми для точної оцінки ризиків.

Страхова галузь відіграє ключову роль в управлінні кібер-ризиками. Кіберстрахування має на меті пом'якшити фінансові втрати, спричинені витоком даних, кібервимаганням, перериванням бізнесу та репутаційною шкодою. Однак страхування систем, керованих штучним інтелектом, створює додаткові складнощі через нестационарність ризиків і складність встановлення причинно-наслідкових зв'язків у кіберподіях. Поверхні атак розширюються в міру того, як системи ШІ стають взаємопов'язаними, що ускладнює прогнозування майбутніх загроз на основі історичних даних. Крім того,

адаптивна природа штучного інтелекту дозволяє використовувати як оборонні, так і наступальні кіберпотужності, що ускладнює оцінку ризиків [1].

Ринок страхування кібер-ризиків стрімко зростає, і очікується, що премії значно збільшаться. Однак через невизначеність у моделях ціноутворення та методологіях оцінки ризиків зберігається значна прогалина в захисті. Страховики покладаються на традиційні статистичні моделі, яким важко вловити динамічну природу кіберризиків. ШІ та машинне навчання (ML) пропонують потенційні рішення, покращуючи прогнозування ризиків, виявлення аномалій та автоматизацію процесів андеррайтингу. Методи контрольованого і неконтрольованого навчання можна використовувати для виявлення нових загроз, тоді як навчання з підкріпленням може оптимізувати стратегії зменшення ризиків. Незважаючи на ці досягнення, дефіцит даних та інформаційна асиметрія перешкоджають ефективному впровадженню страхових моделей, керованих ШІ.

Ключова проблема кіберстрахування полягає в системному ризику. На відміну від звичайних видів страхування, де можлива диверсифікація, кіберризиків можуть поширюватися через взаємопов'язані мережі, що призводить до корельованих збитків. Широке використання спільного програмного забезпечення, хмарної інфраструктури та моделей штучного інтелекту збільшує ймовірність одночасних збоїв, кидаючи виклик традиційним механізмам об'єднання ризиків. Крім того, побоювання щодо конфіденційності даних перешкоджають компаніям розкривати інформацію про кіберінциденти, що призводить до приховування інформації та викривлених оцінок ризиків. Вирішення цих проблем вимагає стандартизованої системи обміну даними та регуляторної підтримки для підвищення прозорості [2].

Кіберстрахування може бути доповнене послугами кібер-асистансу, що поєднують передачу ризиків з активним їх зменшенням. Ці послуги включають моніторинг у режимі реального часу, аудит безпеки та підтримку реагування на інциденти, допомагаючи страхувальникам зменшити свої ризики. Кібер-асистанс на основі штучного інтелекту може проактивно виявляти вразливі

місця та забезпечувати прогностичні заходи безпеки, знижуючи загальний ризик. Страховики отримують вигоду від покращеного збору даних, що призводить до більш точних моделей ціноутворення та вдосконалених стратегій запобігання збиткам.

Нормативно-правова база відіграє вирішальну роль у формуванні ландшафту кіберстрахування. Політики повинні встановити керівні принципи, щоб забезпечити прозорість і неупередженість моделей оцінки ризиків на основі штучного інтелекту. Для запобігання дискримінаційним практикам необхідно враховувати етичні міркування, зокрема зрозумілість і справедливість андеррайтингу на основі ШІ. Крім того, роль урядів у забезпеченні покриття катастрофічних кіберподій залишається предметом дискусій [3].

Отже, штучний інтелект створює як можливості, так і виклики для кіберстрахування. Покращуючи можливості моделювання ризиків, виявлення загроз і реагування на них, він також посилює системні вразливості. Подолання обмежень традиційних актуарних підходів вимагає міждисциплінарної співпраці, інтеграції досвіду з кібербезпеки, науки про дані та страхування. Майбутнє кіберстрахування залежатиме від розвитку надійних систем на основі штучного інтелекту, вдосконалення нормативно-правової бази та покращення механізмів обміну даними в масштабах всієї галузі для забезпечення стійкості до все більш складного ландшафту кіберзагроз.

### Література

1. Çakır A. M. AI Driven Cybersecurity. *Human Computer Interaction*. 2024. Vol. 8, no. 1. P. 119. URL: <https://doi.org/10.62802/jg7gge06>
2. Adewale Daniel Sontan, Segun Victor Samuel. The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. *World Journal of Advanced Research and Reviews*. 2024. Vol. 21, no. 2. P. 1720–1736. URL: <https://doi.org/10.30574/wjarr.2024.21.2.0607>

3. Challenges and efforts in managing AI trustworthiness risks: a state of knowledge / N. Polemi et al. *Frontiers in Big Data*. 2024. Vol. 7. URL: <https://doi.org/10.3389/fdata.2024.1381163>

## **АНАЛІЗУ РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ПУБЛІЧНІ ДЖЕРЕЛА ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ**

**Матвієнко В. І.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Останні декілька років набуває популярності термін OSINT. Ця аббревіатура означає Open Source Intelligence Tools, або розвідка на основі відкритих джерел. Якщо говорити більш конкретно – це збір інформації за рахунок відкритих дописів користувачів соцмереж, картинок в інтернеті, відео публікацій і так далі. Інструменти та методи OSINT поширені в кібербезпеці, де їх використовують для збору даних з відкритих джерел або для етичного хакінгу та тестування на проникнення. Також цей спосіб розвідки набуває популярності і в сфері аналізу ризиків, адже з появою смартфонів та вільного доступу в інтернет, почали з'являтися різні факти та конфіденційна інформація яка б не мала там бути.

Почнемо з історії цього виду добування інформації. Розвідка, заснована на використанні відкритих джерел (Open Source Intelligence - OSINT), має довгу і багату історію. Від початкових форм шпигунства до сучасних розслідувань у соціальних мережах. OSINT відіграє важливу роль у зборі інформації для досягнення певних цілей, як законних так і не дуже. Відкриті джерела інформації (OSINT) були використані у ранньому військовому середовищі для шпигунства та збору стратегічних розвідувальних даних, і їх походження можна прослідкувати. Газети, журнали, вирізки з преси та радіопередачі були

частими джерелами даних, які і сьогодні використовуються військовими по всьому світу. Під час Другої світової війни союзники США переглядали німецькі газети і слухали радіопередачі, щоб знайти цінну інформацію. Служба закордонних досліджень і преси Великої Британії (FRPS) та Служба моніторингу BBC - всі вони використовували OSINT у своїх операціях, намагаючись зрозуміти діяльність на територіях, що контролювалися нацистами. Аналогічна ж ситуація була і під час холодної війни між ЦРУ та КДБ.

У сфері кібербезпеки OSINT відіграє ключову роль, оскільки дозволяє ідентифікувати потенційні загрози та вразливості без порушення законодавства. Збір інформації з відкритих джерел допомагає організаціям проактивно виявляти можливі витoki даних, оцінювати ризики та розробляти стратегії захисту. Він базується на використанні різноманітних відкритих джерел інформації. Основні з них включають:

- Соціальні мережі: платформи, такі як Facebook, Twitter, LinkedIn, містять велику кількість особистої та професійної інформації, яка може бути використана для аналізу поведінки, зв'язків та потенційних вразливостей.
- Веб-сайти та блоги: офіційні сайти компаній, особисті блоги та форуми можуть містити інформацію про структуру організації, поточні проекти, використані технології та інші деталі.
- Новинні портали: статті та репортажі можуть надавати контекст щодо діяльності компанії, її репутації та потенційних інцидентів безпеки.
- Публічні реєстри та бази даних: Державні реєстри, патентні бази даних та інші офіційні джерела містять юридичну та фінансову інформацію про організації.
- Форуми та обговорення: онлайн-форуми, особливо ті, що пов'язані з технологіями або безпекою, можуть містити обговорення вразливостей, витоків даних або інших інцидентів.

Для ефективного збору та аналізу інформації з відкритих джерел використовується широкий набір спеціалізованих інструментів. Вони

дозволяють знаходити вразливості, аналізувати цифрові сліди компаній та окремих осіб, а також виявляти витoki даних.

### 1. Інструменти для збору та аналізу цифрових слідів

- Maltego – один із найпотужніших OSINT-інструментів для візуалізації зв'язків між людьми, організаціями, доменами, IP-адресами, електронними поштами та соціальними профілями.

- theHarvester – інструмент для збору інформації про домени, IP-адреси, субдомени, електронні пошти та дані з пошукових систем.

- Recon-ng – платформа для автоматизованого збору даних про цільові домени та організації.

### 2. Інструменти для аналізу веб-ресурсів та їхньої історії

- Shodan – пошукова система для виявлення відкритих портів, веб-серверів, пристроїв IoT, баз даних та інших мережевих активів, підключених до Інтернету.

- Censys – аналог Shodan, що дозволяє шукати відкриті пристрої та сервіси за IP-адресами та сертифікатами.

- Google Dorking – методика використання розширених пошукових операторів Google (наприклад, `site:example.com filetype:pdf` для пошуку PDF-файлів на певному сайті).

- Wayback Machine – сервіс, що дозволяє переглядати архівні версії веб-сайтів. Використовується для аналізу змін на сайтах, виявлення випадково опублікованої інформації, пошуку вилучених сторінок і файлів. Наприклад, за допомогою Wayback Machine можна знайти версії сайтів, які містили конфіденційні дані або старі вразливості.

### 3. Інструменти для виявлення витоків даних

- DeHashed – сервіс для перевірки витоків облікових даних (логінів, паролів, електронних адрес) у публічних та даркнет-базах даних.

- Have I Been Pwned? – веб-сервіс, що дозволяє перевірити, чи були скомпрометовані облікові дані у відомих витокках.

- Pastebin та аналогічні ресурси (Ghostbin, DeepPaste) – сервіси, де часто з’являються злиті бази даних, паролі та інші чутливі дані.

#### 4. Інструменти для аналізу соціальних мереж

- Social-Searcher – сервіс для пошуку інформації у соцмережах (Twitter, Facebook, LinkedIn, Instagram тощо).

- SpiderFoot – автоматизований OSINT-інструмент, що аналізує IP-адреси, домени, електронні пошти та соцмережі.

- Twint – Python-інструмент для збору даних з Twitter без використання офіційного API.

Використання OSINT-інструментів дозволяє виявляти витoki інформації, оцінювати ризики та проактивно захищати організації від потенційних загроз. Регулярний моніторинг відкритих джерел, зокрема архівних копій сайтів.

Одним з найрозповсюдженіших кейсів використання OSINT є документування та моніторинг російсько-української війни. Від початку вторгнення російських військових в Україну кожна секунда конфлікту документується людьми з обох сторін. Це допомогло зрозуміти та бути в курсі ситуації в Україні, а також задокументувати докази злочинів, скоєних російськими військовими.

Такі організації як незалежна неприбуткова організація “OSINT для України” документують воєнні злочини в Україні в рамках проєкту “Маріуполь”. Вони зосереджуються на злочинах і порушеннях, що відбуваються в Україні. Вони створили базу даних і мапу злочинів і звірств, що відбуваються в Україні, для досліджень і судових процесів, а також для інформування пересічних громадян про ситуацію в Україні.

Ці організації використовують загальнодоступні аудіо- та відеозаписи, фотографії, свідчення очевидців, новини та офіційні документи, щоби бути в курсі подій в Україні. Використання OSINT розвідки постійне, оскільки доступні дані оперативні й дуже часто надходять у режимі “реального часу”.

Іншим прикладом є візуальне розслідування New York Times про Бучанську різанину (Україна), скоєну російськими військовими. Саме там

OSINT розвідка використана для викриття військової частини, яка стояла за вбивствами. Журналісти послуговувались інтерв'ю, записами телефонних розмов, документами й годинами відеозаписів, щоб отримати інформацію про послідовність подій у Бучі й людей, відповідальних за ці злочини.

У висновку можемо зазначити що використання OSINT-інструментів для аналізу ризиків витоку інформації є ефективним методом забезпечення інформаційної безпеки організацій. Використання таких інструментів як Shodan, Maltego, theHarvester, Google Dorking, DeHashed і Wayback Machine допомагають аналітикам знаходити та аналізувати знайдену інформацію в соціальних мережах, пошукових системах, веб-архівах та злитих базах даних. Також аналізуючи ці дані ми можемо проактивно виявляти загрози та ризики в своїй системі чи організації та запобігати витокам інформації. Впровадження таких технологій допоможе підвищити кіберстійкість підприємств та забезпечить комплексний моніторинг загроз.

### Література

1. Розвідка з відкритих джерел (Open-source intelligence - OSINT)  
URL: <https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/>
2. OSINT-розвідка у роботі журналістів/ок. URL: <https://www.prostir.ua/?library=osint-rozvidka-u-roboti-zhurnalistivok>
3. Найкращі інструменти для розвідки на основі відкритих джерел (OSINT) у 2023 році. URL: <https://thetransmitted.com/security/najkrashhi-instrumenti-dlya-rozvidki-na-osnovi-vidkritih-dzherel-osint-u-2023-roczii/>
4. Вступ в OSINT. URL: <https://chatovi.online/articles/Viznachennia%20ta%20rol%27%20OSINT%20v%20informatsiinomu%20prostorii.%20Peregliad%20osnovnikh%20zavdan%27%20ta%20tsilei%20OSINT>

## ОЦІНКА РИЗИКІВ ПОВ'ЯЗАНА З ЛЮДСЬКИМ ФАКТОРОМ

**Горбач Є. С.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Нині, в епоху інформаційних технологій, ці слова стали як ніколи актуальними, адже витік даних здатен призвести до катастрофічних наслідків, як от великі збитки та знищення репутації. Саме тому власник компанії та кожен її працівник повинні докласти максимум зусиль, щоб забезпечити кібербезпеку на робочому місці. У кожного бізнесу свої методи боротьби з кіберзагрозами, але є загальні правила, які допомагають створити надійний базовий захист.

Щорічний звіт Verizon про витіки даних (DBIR), який публікують з 2008, демонструє, що сучасні витіки даних відбуваються внаслідок помилок співробітників у поєднанні з компрометацією ланцюгів постачання; один із цих елементів майже напевно буде задіяний у будь-якому кіберінциденті організації. Причиною 4 з 5 витіків даних є «людський фактор». Звіт, який підготували фахівці одного з провідних світових вендорів Verizon, містить відомості та висновки щодо широкого спектра показників і тенденцій, пов'язаних з інцидентами порушення безпеки даних упродовж 2023 року [1].

Згідно з дослідженням щодо витіку даних за 2023 (DBIR) бізнес-атаки через електронну пошту (BEC) продовжують бути найпоширенішими. Дослідження, яке охоплювало випадки, які сталися між 1 листопада 2021 року та 31 жовтня 2022 року, показало, що атаки BEC подвоїлися і становили понад 50% соціально-інженерних атак. Глобальне дослідження охопило випадки в регіонах Азії-Тихоокеанського регіону, Європи, Близького Сходу та Африки, Північної Америки та Латинської Америки.

Атаки ВЕС стали більш складними і включають в себе різні види шахрайства, наприклад, використання таких легітимних сервісів, як Dropbox, для приховування шкідливих програм.

Дослідження також виявило, що найбільша кількість випадків протягом даного періоду сталася в галузях публічного управління (3270), інформаційних технологій (2 105), фінансових послуг (1 829) та виробництва (1 814)

Дослідження базовано на корпусі даних з різноманітних джерел, зокрема з прикладами, наданими Консультативним центром досліджень загроз Verizon (Verizon Threat Research Advisory Center), зовнішніми партнерськими звітами, а також опублікованими відомостями про безпекові інциденти. Результати аналізу – майже 30000 загроз, 5258 підтверджених порушень і 14 мільйонів розслідувань – викладено в доступній візуалізованій формі. Вивчивши ці дані, фахівці Verizon дійшли низки висновків, ключовими з яких є такі [2].

- 74% всіх порушень включали людський фактор: помилки, зловживання службовим становищем, використання викрадених облікових даних або методів соціальної інженерії.

- 83% зламів були здійснені зовнішніми агентами, а найпоширенішою мотивацією для атак було отримання фінансової вигоди (95% випадків).

- Основними шляхами проникнення зловмисників в організацію були викрадення облікових даних (49%), фішинг (12%) і експлуатація вразливостей (5%).

- 32% усього річного сканування вразливостей Log4j відбулося протягом перших 30 днів після його виявлення, що свідчить про швидкість зловмисників у переході від концепції до масової експлуатації.

лише 3% зловмисників мають на меті шпигунство, 97% зловмисників були мотивовані фінансовими вигодами

Основним вектором хакерських атак досі є вебдодатки, причому 80 % таких атак спричиняють порушення безпеки даних.

Так, на друге місце перемістилися програми шерингу робочого столу ПК (screensharing, desktop sharing)[3].

Сталими є дві тенденції: пріоритетним об'єктом для шахраїв так само є облікові та персональні (з-поміж них банківські) дані, а їхня головна мотивація найчастіше – фінансовий прибуток.

Оскільки все більше організацій упроваджують моделі гібридної роботи, що дають робітникам змогу працювати як в офісі, так і віддалено, варто розгортати нову модель безпеки, яка захищатиме користувачів, пристрої, програми та дані, хоч де вони зберігатимуться.

Принцип інфраструктури з моделлю нульової довіри полягає в тому, що більше не можна довіряти запиту на доступ, навіть якщо він надходить із внутрішньої мережі. Щоб знизити ризик, припустіть, що вас зламали, і перевіряйте всі запити на доступ. Надавати користувачам доступ до потрібних їм ресурсів лише з делегованими правами.

За кібербезпеку відповідають не лише фахівці з безпеки. Сьогодні робочі й особисті пристрої використовуються по черзі, а багато кібератак починаються з надсилання фішингового електронного листа працівникам. Навіть великі забезпечені ресурсами компанії стають жертвами соціотехнічних кампаній. Боротьба з кіберзлочинністю й убезпечення мережі вимагає спільних зусиль усіх працівників. Необхідно проводити регулярне навчання своєї команди, щоб вона могла захищати особисті пристрої та розпізнавати й зупиняти атаки використовуючи симуляції фішингу. Базові принципи кібергігієни забезпечують захист від 98% атак [4].

Перший етап будь-якої стратегії кібербезпеки – посилити всі системи й забезпечити дотримання базових принципів кібергігієни для захисту від потенційних загроз. Для цього необхідно:

- застосувати багатофакторну автентифікацію;
- надавати найменш привілейований доступ і захищати найбільш конфіденційні й привілейовані облікові дані;

- перевіряти всі дії з автентифікації в інфраструктурі віддаленого доступу;
- встановлювати всі необхідні виправлення для систем;
- використовувати інструменти для захисту робочих процесів від зловмисних програм;
- ізолювати застарілі системи;
- увімкнути журналювання основних функцій;
- перевіряти справжність резервних копій;
- перевіряти, чи актуальні плани дій із реагування на інциденти.

### Література

1. Застосування принципів кібербезпеки для ефективного реагування на зміни у світі загроз. URL: <https://www.microsoft.com/uk-ua/security/security-insider/practical-cyber-defense/using-cybersecurity-to-help-manage-volatility>
2. Як покращити кібербезпеку в хмарах: головні загрози та інструменти захисту. URL: <https://hub.kyivstar.ua/articles/yak-pokrashhyty-kiberbezpeku-v-hmarah-golovni-zagrozy-ta-instrumenty-zahystu>
3. Кібербезпека на робочу місці — правила інформаційної гігієни для керівництва та працівників компаній. URL: <https://cityhost.ua/uk/blog/kiberbezpeka-na-robochu-misci-pravila-informaciyno-gigi-ni-dlya-kerivnictva-ta-pracivnikiv-kompaniy.html>
4. Звіт Verizon 2023 DBIR: домінують атаки DDoS, а претекстінг стимулює зростання атак BEC. URL: <https://proit.ua/zvit-verizon-2023-dbir-dominuiut-ataki-ddos-a-pidstavi-stimuliuiut-zrostannia-atak-bec>

# РИЗИКИ ТА ПЕРЕВАГИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

**Котецька В. І.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Штучний інтелект (ШІ) поступово стає невід'ємною частиною кібербезпеки, змінюючи традиційні підходи до захисту цифрових активів і боротьби з кіберзлочинністю. Від перших систем 1980-х років до сучасних нейромереж, його роль виявилася дуже важливою для виявлення загроз, автоматизації реагування та передбачення потенційних атак. Однак розвиток технологій не тільки приносить значні переваги для захисту інформаційних систем, а й створює нові можливості для кіберзлочинців, які активно використовують ШІ для складніших атак.

Сучасні системи на базі ШІ значно покращують процеси виявлення загроз. Алгоритми машинного навчання дозволяють швидко аналізувати великі обсяги даних, виявляючи аномалії та небезпечні патерни, які можуть залишатись непоміченими традиційними методами. Це особливо важливо для виявлення складних загроз, таких як АРТ або атаки нульового дня. Водночас, автоматизація рутинних завдань, таких як моніторинг мережі чи реагування на інциденти, дозволяє фахівцям зосереджуватись на більш стратегічних задачах.

Завдяки можливості прогнозувати загрози, організації можуть бути на крок попереду потенційних атак. ШІ також використовує інструменти обробки текстової інформації для виявлення фішингових спроб, шкідливого програмного забезпечення та шахрайських операцій. Це дозволяє зменшити кількість помилкових спрацьовувань і забезпечити більш швидке реагування на реальні загрози [1].

Попри численні переваги, впровадження ШІ в кібербезпеку пов'язане з кількома проблемами. Для ефективної роботи систем ШІ необхідно мати великі

обсяги високоякісних даних, що може бути складно забезпечити в умовах постійно змінюваного цифрового середовища. Крім того, помилки алгоритмів можуть спричиняти викривлення аналізу даних, що призводить до некоректного прийняття рішень.

Ще однією проблемою є можливі хибні спрацьовування та хибні негативи, коли загрози залишаються непоміченими або фахівці змушені витратити забагато часу на перевірки. Крім того, інтеграція ШІ в існуючі системи може бути ускладнена через несумісність технологій або необхідність значних змін в інфраструктурі.

Також на жаль, ШІ відкриває нові можливості для кіберзлочинців. Використовуючи технології машинного навчання та нейронних мереж, хакери можуть автоматизувати пошук вразливих точок, генерувати персоніфіковані фішингові повідомлення або створювати невиявлені шкідливі програми. Крім того, ШІ дає змогу здійснювати більш складні брутфорс атаки та маскувати місце розташування атакуючого, що ускладнює їх виявлення та переслідування [2].

Крім того, ШІ може бути використаний для збору даних про жертви, прогнозування найефективнішого часу для атак, а також для створення deepfake-відео, підроблених фотографій і документів для шахрайства або дезінформації. Це створює нові виклики для кібербезпеки і вимагає постійного розвитку методів захисту.

Загалом майбутнє штучного інтелекту в кібербезпеці виглядає перспективним. Нові технології допомагають організаціям ефективніше протистояти зростаючим кіберзагрозам, автоматизуючи виявлення загроз і реагування на них. Проте, щоб реалізувати повний потенціал ШІ, необхідно враховувати численні загрози, зокрема, потребу в високоякісних даних, можливість алгоритмічних упереджень та ризику для безпеки самих систем ШІ [3].

Інтеграція ШІ в кібербезпеку повинна бути добре продуманою і збалансованою. Вона потребує постійної підтримки, налаштувань та оновлень,

а також залучення кваліфікованих фахівців, які можуть контролювати та вдосконалювати систему. Важливо також усунути можливі помилки в алгоритмах і гарантувати відповідальне використання технологій, зокрема, щодо захисту конфіденційності та запобігання шахрайству чи дезінформації [4].

Отже, штучний інтелект став невід'ємною складовою кібербезпеки, дозволяючи швидко виявляти загрози, автоматизувати реагування та прогнозувати потенційні атаки. Однак для його ефективного використання потрібен комплексний підхід, який передбачає не лише впровадження технологій, а й їх постійне вдосконалення, моніторинг та адаптацію до нових змін. Поєднання ШІ з експертним аналізом дозволяє зменшити ризики алгоритмічних помилок і забезпечити надійніший захист цифрових активів. Важливо також враховувати етичні аспекти використання ШІ, мінімізуючи загрози для конфіденційності даних та потенційні маніпуляції з боку зловмисників.

### Література

1. The Impact of AI on Cybersecurity: Opportunities and Challenges. URL: <https://techacute.com/the-impact-of-ai-on-cybersecurity-opportunities-and-challenges/>
2. Штучний інтелект та кібербезпека. URL: <https://www.education.ua/blog/48113/>
3. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks>
4. Застосування ШІ у кібербезпеці: роль та переваги. URL: <https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi>

# ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ КІБЕРЗАХИСТУ: ШТУЧНИЙ ІНТЕЛЕКТ, ПОВЕДІНКОВИЙ АНАЛІЗ І КВАНТОВЕ ШИФРУВАННЯ

Пічкур Д. С.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасному світі, де кіберзагрози стають дедалі витонченішими й агресивнішими, захист мереж і операційних систем потребує не просто оновлення старих підходів, а впровадження принципово нових технологій, які здатні випереджати зловмисників. Одним із таких рішень є штучний інтелект, який завдяки своїй здатності обробляти величезні масиви даних у реальному часі перетворюється на справжній мозковий центр кіберзахисту. Наприклад, ШІ може аналізувати мільйони мережевих запитів за секунду, виявляючи патерни, які відхиляються від норми скажімо, незвично великий обсяг трафіку з однієї IP-адреси чи раптове зростання запитів до бази даних у неробочий час. Він не просто реагує на відомі віруси чи шкідливе ПЗ, а вчиться розпізнавати нові, ще не задокументовані загрози, порівнюючи їх із історичними даними й адаптуючись до змін у поведінці систем [1].

Доповнює цю систему поведінковий аналіз, який фокусується на детальному відстеженні дій як людських, так і програмних. Уявімо ситуацію: співробітник, який зазвичай працює з документами, раптом намагається отримати доступ до серверної бази даних, або програма, що відповідає за оновлення, починає надсилати запити на зовнішні сервери. Поведінковий аналіз фіксує ці аномалії, порівнює їх із типовими сценаріями використання й сигналізує про можливу загрозу, наприклад, компрометацію облікового запису чи зараження системи трояном. Разом ці інструменти створюють багат шаровий захист, який не чекає, поки атака завдасть шкоди, а намагається зупинити її на ранніх етапах, що робить їх незамінними для сучасних мереж, де швидкість реагування є вирішальною. Але захист самих систем це лише

частина картини, адже не менш важливим є забезпечення безпеки даних, які постійно циркулюють між різними вузлами корпоративної інфраструктури. Тут у гру вступає квантове шифрування технологія, яка обіцяє перевернути уявлення про безпечний зв'язок [2].

На відміну від традиційних методів, де шифрування базується на складних математичних алгоритмах, які теоретично можна розв'язати за допомогою суперкомп'ютерів, квантове шифрування спирається на закони квантової механіки, зокрема на принцип невизначеності. Ключі шифрування генеруються за допомогою квантових частинок, таких як фотони, і будь-яка спроба перехопити їх змінює їхній стан, роблячи втручання очевидним для відправника й отримувача. Уявіть, наприклад, передачу конфіденційного контракту між головним офісом компанії в одній країні та філіалом в іншій: квантове шифрування гарантує, що ніхто не зможе підслухати цей канал, а якщо спробує зв'язок автоматично припиниться, сигналізуючи про проблему. Це особливо актуально для корпорацій, які працюють із чутливими даними фінансовими звітами, персональною інформацією клієнтів чи розробками, що становлять комерційну таємницю, адже навіть найменший витік може призвести до мільйонних збитків і втрати репутації. Усе це зливається воедино, коли йдеться про інтеграцію кіберзахисту в корпоративну інфраструктуру, адже сучасні компанії, це складні екосистеми з десятками серверів, сотнями робочих станцій і тисячами точок взаємодії [3].

Штучний інтелект і поведінковий аналіз можуть працювати як основа централізованої платформи моніторингу, яка в реальному часі відстежує стан усієї мережі — від хмарних сервісів, де зберігаються дані клієнтів, до ноутбуків співробітників, які під'єднуються до корпоративного VPN із кав'ярень чи дому. Наприклад, ШІ може автоматично ізолювати пристрій, який демонструє підозрілу активність, а поведінковий аналіз надіслати сповіщення адміністратору з детальним звітом про інцидент. Водночас квантове шифрування інтегрується в канали зв'язку скажімо, у протоколи, якими обмінюються дані між дата-центрами чи партнерами, забезпечуючи, щоб навіть

у разі перехоплення трафіку зловмисники не могли його розшифрувати. Такий комплексний підхід не лише захищає від наявних загроз, а й готує інфраструктуру до майбутніх викликів, адже кіберзлочинці постійно вдосконалюють свої методи. У підсумку, поєднання цих технологій дозволяє корпораціям не просто вистояти в умовах цифрової війни, а й зберегти безперебійність операцій, довіру клієнтів і конкурентну перевагу, будуючи систему, яка адаптується до реалій завтрашнього дня.

### **Література**

1. Rangaraju S. AI SENTRY: REINVENTING CYBERSECURITY THROUGH INTELLIGENT THREAT DETECTION. *EPH - International Journal of Science And Engineering*. 2023. Vol. 9, no. 3. P. 30–35. URL: <https://doi.org/10.53555/ephijs.v9i3.211>
2. AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance / C. Madhavaram et al. *SSRN Electronic Journal*. 2025. URL: <https://doi.org/10.2139/ssrn.5029406>
3. Quantum Cryptography for Future Networks Security: A Systematic Review / Durr-E-Shahwar et al. *IEEE Access*. 2024. P. 1. URL: <https://doi.org/10.1109/access.2024.3504815>

## **ВПЛИВ ЧИННИКА АКУСТИЧНОЇ ІНФОРМАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВА**

**Котенко А.М., к.т.н.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Під економічною безпекою розуміється наявність конкурентних переваг які обумовлені наявністю матеріального, фінансового, технологічного

потенціалів та організаційної структури підприємства відповідно його цілям та завданням. Економічна безпека складається з ряду складових, які для конкретного підприємства залежать від загроз. Одна із головних загроз є промисловий шпіднаж. Він проводиться конкурентом у інтересах свого підприємства шляхом отримання доступу до конфіденційної інформації, що призведе до нанесенню шкоди підприємству власнику інформації [1].

Загальний розподіл інформації за режимом доступу показано на рис.1 [2].

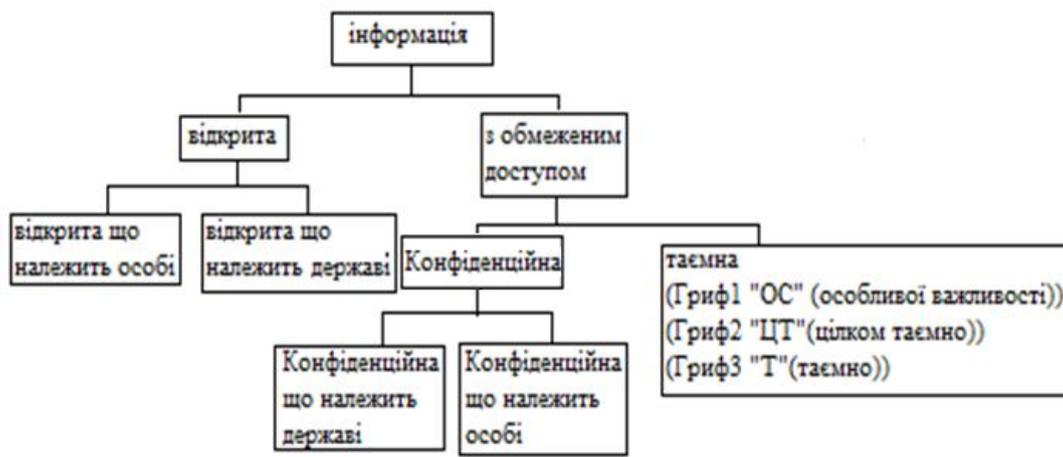


Рис. 1 Розподіл інформації за режимом доступу

Відповідно до рис. 1, інформацію обмеженого доступу (ІзОД) підприємства можна розділити на конфіденційну і секретну. При цьому секретна інформація не обов'язково містить у собі державну таємницю.

До конфіденційної відносяться відомості розголос яких не спричиняє шкоду стратегічним інтересам підприємства. Наприклад може бути зниження прибутку, зрив одного з контрактів, тощо.

Розголос секретної інформації спричиняє важку наслідки в масштабах усієї організації – до втрати існування підприємства.

Визначення грифу обмеженості доступу до інформації визначають як керівні документи (наприклад ЗВДТ), так і керівництво підприємства. До ІзОД підприємства відносяться: уставні документи, фінансові звіти, договори, аналітичні огляди, технологічна інформація тощо.

Таким чином ІЗОД підприємства існує в матеріальній формі, акустичній (наради, перемовини), на технічних засобах обробки інформації [3].

Можливі шляхи втрати ІЗОД підприємства наступні [3].

Перший – матеріально-речовий шлях. Загрозою втрати інформації є крадіжка матеріальних носіїв інформації.

Другий – візуально-оптичний. Застосування технічних засобів для фото та кіно документування.

Третій – виток інформації з інформаційно-комунікаційних систем (ІКС) під час обробки інформації з фізичних процесів, що виникають в ІКС під час їх функціонування. Мова йде про побічні електромагнітні випромінювання та їх наведення на сполучені електричні комунікації об'єктів інформаційної діяльності.

Четвертий – підслуховування телефонних розмов по провідним лініям зв'язку. Неголосне отримання інформації здійснюється з самих телефонів, сполучених ліній, комутаційних коробок.

П'ятий – перехоплення акустичної інформації з засобів які використовують радіоканал. Використовується спеціальна апаратура.

Шостий – отримання акустичної інформації шляхом використання закладних пристроїв ("жучки").

Сьомий – використання вібраційних особливостей віконного скла та інженерних конструкцій приміщення де ведуться секретні розмови.

Виходячи з перерахованого, оцінити шкоду економічній безпеці підприємства при наявності якогось або декількох з семи перерахованих шляхів втрати інформації, можна узагальненим показником шкоди економічній безпеці підприємства використовуючи наприклад модифікований вираз розрахунку середнього геометричного:

$$P = \sqrt[n]{\prod(1 + k_n)} - 1 \quad (1)$$

де:

$n$  – кількість загроз втрати інформації (у нашому випадку 7);

$k_n$  - показник шкоди інформаційній безпеці підприємства при реалізації загрози одним з перерахованих шляхів.

Видно, що з семи перерахованих шляхів втрати інформації, у чотирьох присутен фактор акустичної інформації. Тобто втрата акустичної ІзОД має суттєвий вплив на економічну безпеку підприємства.

Розглянемо особливості акустичного каналу витоку інформації.

1. Він дуже інформативен. Співбесідник в усній формі проще пояснити сутність того що трапилось, що робити. Ту ж саму подію складніше буде описати. При бесіді присутен фактор інтонації ,міміки – додається фактор суб'єктивності.

2. Він є дуже використовуємим у виробничих відносинах між керівниками та підлеглими. Людський фактор сприяє більш довірчим відносинам у таких спілкуваннях.

3. Цей шлях не вимагає додаткової обробки при підслуховуванні. Тобто інформація легкодоступна.

4. Акустична інформація легко документується технічними засобами.

5. При усіх інших позитивних властивостях акустичний канал витоку інформації дуже вразлив. Навіть лояльність персоналу підприємства не гарантує що акустична інформація не буде підслухована або перехоплена.

Підсумовуючи викладене: акустичний канал інформаційного обміну характеризується високою інформативністю, частим використанням у виробничій діяльності, простотою документування, доступністю, вразливістю.

ІзОД впливає на економічну безпеку підприємства. Вона існує у матеріальній формі, візуальній, акустичній вигляді електричних сигналів.

З проаналізованих семи можливих шляхів втрати інформації, у чотирьох з них присутен фактор акустичної інформації.

Акустичний канал втрати інформації характеризується: інформативністю, частим використанням у виробничій діяльності, простотою документування, доступністю, вразливістю.

Напрямом подальших досліджень є кількісна оцінка коефіцієнтів  $k_n$  у виразі (1).

### **Література:**

1. М. І. Небава, Ю. В. Міронова. Економічна безпека підприємства Навчальний посібник. Вінниця : ВНТУ, 2017. 73 с.
2. Закон України Про інформацію. від 02.10.1992 № 2657-ХІІ.
3. Котенко А.М., Хлапонін Ю.І. Конспект лекцій для студентів спеціальності 125 “Кібербезпека та захист інформації” з дисципліни “Програмно-апаратні засоби захисту”. Київ: КНУБА, 2025. 154 с.

## **ІНТЕГРАЦІЯ ДАТА-АНАЛІТИКИ ДЛЯ ЕФЕКТИВНОГО УПРАВЛІННЯ РИЗИКАМИ**

**Бойко М. А.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасні кіберзагрози потребують швидкого реагування та ефективного управління ризиками, що є серйозним завданнями для департаментів безпеки та Security Operation Center (SOC). Інтеграція дата-аналітики дозволяє підвищити рівень ситуаційної обізнаності, прискорити аналіз загроз та автоматизувати реагування, що сприяє мінімізації потенційних збитків. Використання методів штучного інтелекту та поведінкової аналітики на основі великих даних дозволяє переходити від реактивного до проактивного управління ризиками, що значно зміцнює кіберстійкість підприємств..

Динамічний характер кіберзагроз вимагає нових підходів до моніторингу та аналізу безпекових інцидентів. Традиційні методи реагування, що базуються на правилах та сигнатурах, мають обмежену ефективність перед сучасними

атаками, які швидко еволюціонують. Інтеграція методів дата-аналітики дозволяє SOC обробляти великі обсяги даних у реальному часі, автоматично виявляти аномалії та корелювати події для швидкого прийняття рішень. Такі можливості є важливими для підвищення ефективності управління ризиками та забезпечення безперервності бізнесу в умовах зростаючих загроз.

Інструменти дата-аналітики в SOC відіграють ключову роль у швидкій ідентифікації кіберзагроз та мінімізації потенційних ризиків. Використання технологій машинного навчання для аналізу поведінкових моделей дозволяє автоматично визначати нетипові активності користувачів і систем, що можуть свідчити про компрометацію. Це дозволяє SOC оперативно реагувати на можливі загрози до їхнього перетворення в критичні інциденти [1].

Автоматизована обробка даних також сприяє кореляції подій з різних джерел, таких як журнали безпеки, трафік мережі та системи SIEM. Це забезпечує комплексне бачення аномалій, яке унеможливлене ізольованим аналізом окремих подій, який часто не дозволяє виявити складні атаки. Візуалізація цих даних за допомогою бізнес-аналітики дозволяє командам SOC швидше ідентифікувати критичні загрози та приймати обґрунтовані рішення.

Одним із ефективних рішень для інтеграції дата-аналітики у процеси управління ризиками є використання Power BI. Цей інструмент дозволяє автоматизувати аналіз даних та надавати аналітикам SOC наочні дашборди (інформаційні панелі) для оцінки загроз у реальному часі. Power BI інтегрується з SIEM-системами, такими як Azure Sentinel, та забезпечує глибоке аналітичне дослідження безпекових подій. Завдяки цьому SOC отримує не лише історичний аналіз, але й можливість побудови прогностичних моделей для виявлення потенційних атак ще до їхньої реалізації. Використання інтерактивних панелей дозволяє оперативно реагувати на підозрілі активності та оптимізувати розподіл ресурсів для реагування на інциденти. Впровадження Power BI у SOC дозволяє не тільки скоротити час аналізу загроз, але й значно підвищити ефективність управління ризиками за рахунок покращеної видимості загальної картини кіберзагроз [2].

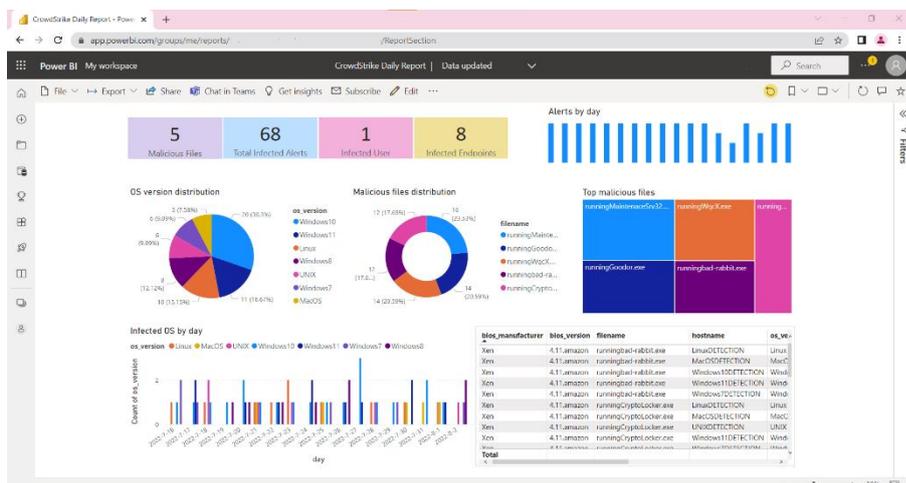


Рис. 1 Приклад візуалізації даних системи CrowdStrike за допомогою Power BI

Важливою складовою ефективного управління ризиками є можливість прогнозування атак на основі історичних даних. Аналітичні моделі дозволяють виявляти закономірності в кіберінцидентах, що дає змогу компаніям проактивно усувати вразливості та адаптувати політики безпеки. Це підвищує загальну кіберстійкість підприємства, зменшуючи ймовірність успішної реалізації атак та їхнього впливу на бізнес-процеси.

Інтеграція дата-аналітики у SOC змінює підходи до управління ризиками та реагування на кіберзагрози. Аналіз великих даних, машинне навчання та автоматизація процесів дозволяють значно скоротити час реагування та підвищити ефективність моніторингу безпеки. Перехід від реактивного до проактивного управління ризиками забезпечує стійкість бізнесу перед сучасними загрозами та сприяє оптимізації процесів кібербезпеки. У результаті, підприємства можуть мінімізувати втрати, пов'язані з кіберінцидентами, та забезпечити безперервність своєї діяльності.

## Література

1. Analytics and Business Intelligence Platforms Reviews and Ratings. [www.gartner.com](http://www.gartner.com). URL: <https://www.gartner.com/reviews/market/analytics-business-intelligence-platforms>

2. Security | Microsoft Power BI. [www.microsoft.com](http://www.microsoft.com). URL: <https://www.microsoft.com/en-us/power-platform/products/power-bi/security>.

## **ІДЕНТИФІКАЦІЯ ПІДРОБЛЕНИХ НОВИН В СОЦІАЛЬНИХ МЕРЕЖАХ**

**Кирсєв Р. Д.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Фейкові новини стали серйозною проблемою сучасного інформаційного простору, впливаючи на громадську думку, політичні процеси та навіть безпеку суспільств. Вони є неправдивою або спотвореною інформацією, поширеною з метою маніпуляції, введення в оману або досягнення певних політичних, економічних чи соціальних цілей.

Боти впливають на поширення фейків, вони можуть швидко й масово розповсюджувати інформацію в соціальних мережах чи інших платформах, не потребуючи людського контролю. Їх програмують для автоматичного розміщення постів, коментарів або репостів, що дозволяє охопити велику аудиторію за короткий час. Оскільки боти часто імітують поведінку реальних людей, їхня діяльність може створювати ілюзію широкої підтримки певної ідеї чи повідомлення, що робить фейки більш переконливими. Крім того, вони здатні працювати цілодобово, підсилюючи ефект дезінформації, особливо якщо їх використовують організовано, наприклад, у кампаніях із маніпуляції думкою. Через це фейки, які розганяють боти, можуть здаватися достовірними, хоча насправді вони не мають реального підґрунтя.

Потенційні ознаки ботів[1]:

1. Анонімність

Чим менше особистої інформації доступно в акаунті, тим імовірніше, що це бот. Звертайте увагу на імена користувачів, які містять забагато чисел, та

стандартні фото профілю. Проведіть зворотний пошук зображення, щоб перевірити, чи не використовується те саме фото в кількох акаунтах.

## 2. Активність

Боти часто демонструють підозрілу активність. Акаунт бота може мати лише один твіт із надзвичайно високим рівнем залучення або надсилати велику кількість твітів за короткий проміжок часу. Поділіть кількість твітів на кількість днів існування акаунта, щоб визначити частоту публікацій.

## 3. Посилення розповсюдження фейків

Більшість ботів створені для підсилення контенту. На типовій стрічці бота буде багато ретвітів, дослівно скопійованих і вставлених заголовків або поширень новин без додаткових коментарів. Оригінального контенту в акаунті бота зазвичай дуже мало.

Ви можете повідомляти про акаунти ботів на Facebook, Twitter, Instagram та YouTube. Якщо вас засипають коментарями від ботів під певним дописом, подумайте про те, щоб залишити один коментар із фактичною інформацією та джерелом, щоб розвіяти дезінформацію.

Ідентифікація підроблених новин вимагає системного підходу, що включає як традиційні методи перевірки інформації, так і сучасні технологічні рішення. Ось основні методи аналізу:

### 1. Аналіз джерела інформації

- Перевірка надійності сайту, який публікує новину (авторитетні ЗМІ рідше поширюють фейки).
- Оцінка доменного імені (офіційні ЗМІ мають перевірені домени, а фейкові новини часто використовують схожі URL-адреси).

### 2. Перевірка фактів та авторства

- Шукайте по імені автора, щоб дізнатися, що він ще написав і чи є він частиною авторитетного інформаційного агентства, чи існує він взагалі[2]

### 3. Оцінка заголовка та стилю написання

- Якщо заголовок дивовижний і провокативний, історія може бути неправдивою. Заголовки-приманки для кліків або навмисно надмірно

сенсаційні заголовки намагаються привернути увагу та спрямувати інтернет-трафік на певний сайт.

- Помітили друкарські або граматичні помилки, це означає, що історія була зібрана необережно, що може означати, що вона вводить в оману, упереджена або навіть явно неправдива[2].

#### 4. Перехресна перевірка інформації

- Порівняння новини з аналогічними повідомленнями в інших ЗМІ.
- Якщо новина поширюється лише одним джерелом, це привід засумніватися в її правдивості.

#### 5. Аналіз зображень та відео

- Якщо зображення здається надто зручним, нереалістичним, застарілим або поза контекстом, виконайте зворотний пошук зображення в Google, щоб побачити, де ще воно могло з'явитися[2].

- Аналіз метаданих фото та відео (наприклад, за допомогою інструментів FotoForensics, InVID).

Навіть якщо фейкові новини активно поширюються в соціальних мережах, дослідження показали, що людська поведінка (маркетинг «сарафанне радіо») сприяє поширенню фейкових новин більше, ніж автоматизовані боти. Це свідчить про те, що боротьба з розсилниками фейкових новин — не єдиний підхід. Також має сенс підвищити стійкість до фейкових новин з боку одержувача та нашого суспільства. Тому ще однією важливою складовою виявлення фейкових новин є підвищення обізнаності та медіаграмотності громадян[3]

### Література

1. Дезинформація та фейкові новини (United States Army Training and Doctrine Command). URL: <https://www.tradoc.army.mil/social-media-bots/>

2. The ACT-Up Method of Assessing Information. URL: [https://faculty.lsu.edu/fakenews/protect\\_yourself/fight-fake-news.php](https://faculty.lsu.edu/fakenews/protect_yourself/fight-fake-news.php)

3. Fake News Detection. URL: [https://www.edps.europa.eu/press-publications/publications/techsonar/fake-news-detection\\_en](https://www.edps.europa.eu/press-publications/publications/techsonar/fake-news-detection_en)

## **ОСНОВНІ ЗАГРОЗИ КІБЕРБЕЗПЕЦІ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ**

**Курінний О. С.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

З розвитком інформаційних технологій та масовим переходом компаній на віддалену роботу питання кібербезпеки набуває особливого значення. Віддалене середовище створює нові ризики, які ускладнюють контроль доступу, захист інформації та управління загрозами. Атаки на користувачів, що працюють поза корпоративною мережею, набувають нових форм, що потребує комплексного підходу до їх виявлення та запобігання.

Віддалена робота стала невід'ємною частиною сучасного професійного життя, особливо після глобальних подій останніх років. Однак перехід до дистанційної роботи супроводжується низкою кібербезпекових загроз, які потребують особливої уваги.

Фішинг є однією з найпоширеніших загроз у віддаленому середовищі. Зловмисники використовують електронні листи, повідомлення у месенджерах та соціальних мережах, видаючи себе за надійні джерела, щоб виманити у жертв конфіденційну інформацію або змусити їх завантажити шкідливе програмне забезпечення. Такі атаки стають дедалі складнішими, що ускладнює їх виявлення користувачами [1].

Використання публічних Wi-Fi мереж без належного захисту може призвести до перехоплення даних зловмисниками. Без використання

віртуальних приватних мереж (VPN) працівники ризикують стати жертвами атак, що можуть призвести до витоку конфіденційної інформації [2].

Недостатній захист облікових записів, зокрема відсутність багатофакторної автентифікації (MFA), підвищує ризик несанкціонованого доступу до корпоративних систем. Використання лише паролів може бути недостатнім, оскільки зловмисники знаходять способи їх обходу [3].

Працівники, які використовують особисті пристрої для роботи, часто не мають належного рівня захисту на цих пристроях. Це створює додаткові вразливості, оскільки особисті пристрої можуть бути інфіковані шкідливим ПЗ або не мати оновлених систем безпеки [4].

Загрози кібербезпеки у віддаленому робочому середовищі є багатогранними та вимагають комплексного підходу до їх нейтралізації. Організації повинні впроваджувати сучасні засоби захисту, такі як багатофакторна автентифікація, використання VPN та регулярне навчання працівників основам кібергігієни. Лише поєднання технічних рішень та підвищення обізнаності співробітників допоможе ефективно протидіяти сучасним кіберзагрозам.

### Література

1. В. Є. Лучик, Д. Є. Власко. Фішингові атаки: як їх розпізнавати та уникати. URL: [https://ibn.idsi.md/sites/default/files/imag\\_file/536-539\\_5.pdf?](https://ibn.idsi.md/sites/default/files/imag_file/536-539_5.pdf?)

2. Grace Bhardwaj. Ризики кібербезпеки під час роботи з будь-якого місця. *Ranktracker*. URL: <https://www.ranktracker.com/uk/blog/cybersecurity-risks-while-working-from-anywhere/>

3. В. Д. Барбак, П. К. Ніколюк. Використання методів захисту від фішингу та ідентифікація шахраїв у електронній пошті. *Прикладні аспекти сучасних міждисциплінарних досліджень*. груд. 2024. С. 152-153. URL: <https://jpasmd.donnu.edu.ua/article/view/16739>

4. A. Kapiton, O. Dziuban, R. Baranenko, H. Sokol. Security of information technologies in a hybrid working environment. *Control, Navigation and*

## **ПОРІВНЯННЯ ТРАДИЦІЙНИХ МЕТОДІВ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ІЗ СУЧАСНИМИ AI-РІШЕННЯМИ**

**Павленко А. А.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Фейкові новини є серйозною загрозою для інформаційного простору, що впливає на громадську думку та викривлює реальність. У цій роботі розглядається порівняння традиційних методів виявлення фейкових новин та сучасних рішень, заснованих на штучному інтелекті (AI).

### **Традиційні методи виявлення фейкових новин:**

1. **Фактчекінг вручну** – перевірка достовірності інформації через надійні джерела та аналітичні центри.
2. **Аналіз контенту** – оцінка стилістики, логіки та узгодженості новинного матеріалу.
3. **Джерелознавчий підхід** – аналіз надійності та репутації інформаційного ресурсу.
4. **Перехресна перевірка** – порівняння новини з матеріалами офіційних видань та авторитетних ЗМІ.

### **Сучасні AI-рішення для виявлення фейкових новин:**

1. **Обробка природної мови (NLP)** – використання алгоритмів аналізу тексту для виявлення маніпуляцій та фальсифікацій.
2. **Машинне навчання** – нейронні мережі та моделі, що прогнозують правдивість новини на основі великих масивів даних.

3. **Аналіз поведінки в соцмережах** – ідентифікація бот-акаунтів та аномальних патернів поширення інформації.

4. **Розпізнавання зображень і відео** – виявлення зміненого або фальшивого контенту за допомогою комп'ютерного зору.

#### **Переваги AI-рішень:**

- Автоматизація та висока швидкість аналізу великих обсягів інформації.
- Виявлення прихованих маніпуляцій та аномальних поширень контенту.
- Гнучкість та адаптивність до нових типів фейкових новин.

**Висновки:** Традиційні методи виявлення фейкових новин є ефективними, але вимагають значних ресурсів та часу. Сучасні AI-рішення здатні автоматизувати процес виявлення неправдивої інформації та підвищити ефективність боротьби з дезінформацією. Оптимальним підходом є поєднання людського аналізу та штучного інтелекту.

#### **Література**

1. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe, 2017. URL: <https://rm.coe.int/information-disorder-report/1680764666>

2. Ferrara E. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. First Monday, 2017. URL: <https://firstmonday.org/ojs/index.php/fm/article/view/8005>

3. Allcott H., Gentzkow M. Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 2017. URL: <https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>

# ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ОРГАНІЗАЦІЇ ТА ЗДІЙСНЕННІ КІБЕРАТАК

**Мужанова Т. М. к.держ.упр, доц., Ярмоленко Б. В.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Штучний інтелект (ШІ) стрімко змінює сучасний цифровий світ, відкриваючи нові можливості для бізнесу, науки, медицини та безпеки. Однак, поряд із позитивними досягненнями, розвиток ШІ створює нові виклики, зокрема в галузі кіберзлочинності. Використання алгоритмів машинного навчання та глибоких нейронних мереж для атаки на інформаційні системи сталося від головних загроз.

Зловмісники активно застосовують штучний інтелект для підвищення ефективності кібератак, що дозволяє їм використовувати традиційні методи захисту та зберігати нові вразливості. Автоматизовані фішингові кампанії, злом паролів, ботнети, мережевий аналіз для виявлення слабких місць – усе це стає більш небезпечним завдяки штучному інтелекту [1]. Крім того, технології глибоких фейків не дозволяють створювати реалістичні аудіо- та відеоматеріали, які можуть бути використані для маніпуляції, шантажу та розповсюдження дезінформації. З огляду на це, дослідження методів використання ШІ в кібератаках є критично важливим для розробки ефективних заходів кібербезпеки. Без розуміння нових загроз неможливо побудувати надійний захист цифрових систем. У цій статті ми розглянемо основні способи застосування ШІ для проведення кібератак, а також засоби протидії цим загрозам.

AI може генерувати дуже переконливі фішингові атаки та атаки соціальної інженерії, аналізуючи великі набори даних взаємодії людей. Інструменти штучного інтелекту полегшують зловмисникам створення

персоналізованих і переконливих повідомлень, які з більшою ймовірністю змусять жертву надати конфіденційні дані [2].

Штучний інтелект можна використовувати для створення більш складних та адаптивних шкідливих програм. Наприклад, штучний інтелект може допомогти зловмисному ПЗ уникнути виявлення, навчаючись у систем безпеки та коригуючи свою поведінку в режимі реального часу. Швидка еволюція та наявність такої кількості різноманітних сигнатур ускладнюють традиційні заходи безпеки для виявлення та нейтралізації загроз.

Здатність штучного інтелекту застосовувати цілеспрямовані атаки в масштабі є безпрецедентною між аналізом величезних обсягів даних для націлювання на окремих осіб або організації та величезними автоматизованими можливостями. Раніше ці атаки вимагали складних мереж, величезної обчислювальної та людської потужності, але тепер зловмисники можуть адаптувати свої атаки за допомогою моделей штучного інтелекту, щоб максимізувати вплив і рівень успіху.

Одним із тривожних способів використання ШІ шахраями є дублювання голосу, відоме як вішинг. Використовуючи короткі аудіозаписи людей, опубліковані в Інтернеті, шахраї можуть клонувати голоси та вводити людей в оману, щоб вони думали, що вони розмовляють зі знайомою людиною. Синтез голосу — це техніка, що лежить в основі цієї маніпуляції, яка передбачає аналіз голосу людини для створення нової мови, яка звучить надзвичайно схоже на оригінальну. Хоча синтез голосу має законні програми, шахраї використовують його, щоб видати себе за когось і обманом змусити жертв розкрити конфіденційну інформацію [3].

Штучний інтелект відкриває величезні можливості для розвитку технологій, але водночас він стає потужним інструментом у руках зловмисників. Використання ШІ в кібератаках дозволяє зловмисникам автоматизувати атаки, персоналізувати фішингові кампанії, створювати реалістичні глибокі фейки та мати нову вразливість. Розвиток таких загроз вимагає активної протидії з боку фахівців з кібербезпеки, урядів і

технологічних компаній. Впровадження штучного інтелекту в захисні механізми, покращення алгоритмів виявлення атак, а також підвищення рівня цифрової грамотності користувачів – ключові кроки для боротьби з новими кіберзагрозами. Майбутнє кібербезпеки залежить від того, наскільки швидко та ефективно суспільство може адаптуватися до нових викликів, використовуючи ШІ не лише як загрозу, а й як засіб захисту. Важливо розвивати міжнародну співпрацю та посилювати законодавче регулювання, щоб мінімізувати ризики зловживання цієї техніки. Таким чином, ШІ може бути як зброєю, так і щитом у кіберпросторі. Відповідальне використання та постійний розвиток технологій безпеки – ключ до захисту цифрового майбуту.

### **Література**

1. AI arms race: How AI will be used by cyber-attackers (and defenders). URL: <https://specopssoft.com/blog/ai-in-cybersecurity-arms-race-attackers-defenders/>
2. How hackers and scammers use ai artificial intelligence. URL: <https://cyberseniors.org/uncategorized/how-hackers-and-scammers-use-ai-artificial-intelligence/>
3. AI-Powered Cyberattacks. URL: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/>

# АНАЛІЗ ФЕЙКОВИХ АККАУНТІВ ТА ЇХ РОЛІ У ПОШИРЕННІ ДЕЗІНФОРМАЦІЇ

**Костенко Я. О.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Фейкові акаунти стали ключовим інструментом у поширенні дезінформації та маніпуляції суспільною думкою в цифровому середовищі. Вони використовуються як зловмисниками, так і організованими групами для впливу на політичні, економічні та соціальні процеси. Аналіз їхньої активності дозволяє ідентифікувати основні методи дезінформаційних кампаній та виробити ефективні стратегії протидії.

Одним із ключових аспектів діяльності фейкових акаунтів є їх використання в інформаційних війнах. Вони можуть поширювати неправдиву інформацію, фабрикувати новини та маніпулювати суспільними настроями через соціальні мережі та онлайн-платформи. До основних характеристик фейкових акаунтів належать:

- Використання автоматизованих ботів та тролів для масового розповсюдження контенту;
- Імітація реальних користувачів для створення видимості громадської підтримки певних наративів;
- Використання емоційно забарвленої риторики для підсилення ефекту впливу;
- Маскування під авторитетні джерела або експертів.

Розповсюдження дезінформації через фейкові акаунти може мати серйозні наслідки, зокрема:

- Формування хибних суспільних уявлень та паніки;
- Втручання у виборчі процеси та маніпуляція громадською думкою;

- Економічні збитки через спотворення інформації про ринки та компанії;
- Загострення соціальних конфліктів та поляризація суспільства.

Ефективні методи протидії фейковим акаунтам включають:

- Використання алгоритмів штучного інтелекту для ідентифікації підозрілих профілів;
- Фактчекінг та розвінчання фейкових новин;
- Посилення цифрової грамотності користувачів та навчання критичному мисленню;
- Співпрацю між державними органами, платформами соціальних мереж та незалежними дослідниками.

Таким чином, боротьба з фейковими акаунтами та дезінформацією є комплексним завданням, що вимагає поєднання технологічних, правових та освітніх підходів. Подальші дослідження в цій галузі сприятимуть зміцненню інформаційної безпеки та підвищенню стійкості суспільства до маніпуляцій.

### Література

1. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe, 2017. URL: <https://rm.coe.int/information-disorder-report/1680764666>
2. Ferrara E. Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election. First Monday, 2017. URL: <https://firstmonday.org/ojs/index.php/fm/article/view/8005>
3. Allcott H., Gentzkow M. Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, 2017. URL: <https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>

# ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ У КІБЕРАТАКАХ ТА КІБЕРЗАХИСТІ

**Ярошенко В. Я.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасному динамічному світі, горизонт кіберзагроз невинно розширюється, у відповідь на це відбувається покращення засобів протидії їм. Таким чином можна говорити про своєрідне змагання між мечем і щитом, засобом ураження та засобом захисту. Засоби штучного інтелекту (ШІ) стають новим покращенням «меча», що здатне автоматизувати фішинг, створення шкідливих програм та інші складні атаки. З іншого боку засобами ШІ посилюється і «щит» дозволяючи автоматизувати виявлення загроз, аналізувати великі обсяги даних і прогнозувати атаки, що значно посилює оборонні можливості. Таким чином, штучний інтелект стає не лише потужним інструментом захисту, але й ефективною зброєю для нападників, що призводить до постійної боротьби між захистом і атакою в кіберпросторі.

Інструменти ШІ активно використовуються у нападі, як легітимними червоними командами так і кіберзлочинцями для здійснення більш складних і ефективних атак. Їх використання дозволяє значно підвищити рівень автоматизації та адаптації атак, що робить загрози більш численними та небезпечними. Усі типи учасників кіберзагроз – державні та недержавні, кваліфіковані та менш кваліфіковані – вже використовують ШІ різною мірою [2].

ШІ дає можливість створювати більш правдоподібні фішингові повідомлення та сайти, що імітують реальні. ШІ насамперед запропонує суб'єктам загрози підвищення можливостей у соціальній інженерії. Генеративний штучний інтелект використовується для забезпечення переконливої взаємодії з жертвами, включаючи створення документів-

приманок, без очевидного перекладу, орфографічних і граматичних помилок, за якими часто ідентифікують фішинг. Зловмисники можуть використовувати ШІ для створення та маніпулювання зображеннями або відео (так звані "deepfake"), щоб здійснювати психологічний тиск чи вводити ціль в оману. Завдяки вищезгаданим методам, зловмисники можуть формувати ботнети значних розмірів у соцмережах, що складатимуться із правдоподібних ботів-користувачів, такі ботнети є загрозливим засобом що може використовуватись у дезінформаційних кампаніях, фішингових кампаніях, тощо [3].

Застосування ШІ інструментів у процесі розробки ШПЗ може пришвидшувати їх розробку, скорочення терміну розробки призводить до полегшення їх адаптування до нових умов [1]. ШІ має потенціал для створення зловмисного програмного забезпечення, яке могло б уникнути виявлення поточними фільтрами безпеки, але лише якщо він навчений на якісних даних експлоїтів. Існує ймовірність того, що зловмисники, такі як різноманітні АРТ можуть мати необхідні сховища шкідливих програм, а також достатньо кваліфікованих фахівців, щоб ефективно навчати модель ШІ для цієї мети[2].

ШІ відіграє важливу роль у діяльності фахівців з кібербезпеки, автоматизуючи процеси виявлення та реагування на загрози. ШІ допомагає автоматизувати рутинні завдання, такі як моніторинг мережі та аналіз подій безпеки, що дозволяє фахівцям зосередитися на складніших аспектах роботи. Це підвищує ефективність роботи та знижує ризик людських помилок.

Використання алгоритмів машинного навчання дає спроможність виявляти аномалії у поведінці, завдяки здатності обробляти великі обсяги різноманітних даних, ШІ може ідентифікувати патерни, що відрізняються від норми. Такий моніторинг може здійснюватись у відношенні різних об'єктів спостереження.

Моніторинг на основі ШІ може виявляти нетипову, підозрілу поведінку користувача, враховуючи поведінкові фактори, такі як манера введення пароля або тип взаємодії із системою Це дозволяє створити більш надійні методи

аутифікації, що значно ускладнює проникнення зловмисників, навіть якщо їм вдалося отримати доступ до облікових даних.

ШІ може використовуватися для моніторингу мережевого трафіку, Алгоритми ШІ здатні відслідковувати зміни метрик трафіку мережі і виявляти відхилення від нормального функціонування. Будучи доповненням до встановлених «жорстких» правил систем IDS та IPS такий моніторинг дозволяє виявити нові, раніше невідомі атаки. ШІ де він допомагає автоматично ідентифікувати та блокувати різноманітні типи атак, такі як атаки "відмова в обслуговуванні" (DDoS), спроби злому через слабкі місця в протоколах або мережеві уразливості. Вони можуть автоматично ініціювати заходи для блокування загрози. Згадані методи знайшли застосування у різноманітних XDR рішеннях IDS та IPS системах [4].

Зокрема, через свої поведінкову природу аналізу, можливо виявити нові, невідомі типи шкідливих програм. За допомогою методів машинного навчання можна створити системи, що здатні виявити не тільки відомі, але й нові віруси, трояни чи шпигунські програми, навіть якщо вони не мають явних ознак шкідливого коду.

Штучний інтелект активно використовується як у кібернападах, так і в захисті, створюючи нові виклики для кібербезпеки. Він автоматизує як атаки, так і захист, підвищуючи ефективність обох процесів. Це також призводить до постійної боротьби між обороною і атаками в кіберпросторі. ШІ стає незамінним інструментом у сучасній кібербезпеці, однак він також стає і потужною зброєю для зловмисників. Розуміння способів використання ШІ для атак є важливим кроком до розробки більш ефективних методів протидії цим загрозам. Експерти аналізують вплив ШІ на кібербезпекові операції. Серед загальних висновків, ШІ розглядається більше як вдосконалення існуючих інструментів, ніж їхня заміна [1].

## Література

1. Національний координаційний центр кібербезпеки при РНБО України, «Річний аналітичний огляд (жовтень 2023 – вересень 2024)», URL: [https://www.rnbo.gov.ua/files/2024/NATIONAL\\_CYBER\\_SCC/20250109/Year%20in%20review\\_UKR\\_upd.pdf](https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf).
2. Національний центр кібербезпеки Великої Британії, «Вплив ШІ на кіберзагрози», URL: <https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat>.
3. Yang, Kai-Cheng та Filippo Menczer, «Anatomy of an AI-powered malicious social botnet.» (2023), URL: <https://arxiv.org/abs/2307.16336>.
4. «Securing Your Network: The Power of AI in Intrusion Detection Systems» (2024), URL: <https://hcrobo.com/securing-your-network-the-power-of-ai-in-intrusion-detection-systems/>

## ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ ТА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Дудій С. А.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

З розвитком цифрових технологій підприємства все більше стикаються з загрозами кібератак, що можуть завдати значних фінансових та репутаційних збитків. У зв'язку з цим застосування штучного інтелекту (ШІ) у забезпеченні кібербезпеки стає актуальним напрямком для мінімізації ризиків і покращення рівня захисту інформаційних систем.

Використання ШІ у сфері кібербезпеки підприємств дозволяє автоматизувати процеси виявлення загроз, аналіз аномальної активності й

реагування на потенційні атаки в режимі реального часу. Основні напрями застосування ШІ у кібербезпеці охоплюють [1, 2]:

- машинне навчання (МН) для аналізу поведінки користувачів і виявлення підозрілих дій;
- системи виявлення вторгнень (IDS), які використовують алгоритми ШІ для ідентифікації загроз;
- автоматизовані засоби аналізу шкідливого програмного забезпечення;
- використання чат-ботів та інтелектуальних асистентів для моніторингу інцидентів безпеки;
- інтеграцію з SIEM-системами для оперативного аналізу логів і подій безпеки.

Окрему увагу слід приділити використанню ШІ для забезпечення кібербезпеки об'єктів критичної інфраструктури, таких як підприємства зв'язку, атомні електростанції, фінансові установи та державні установи, де ШІ інтегрується в багаторівневі системи кіберзахисту, забезпечуючи прогнозування потенційних вразливостей шляхом аналізу великих обсягів історичних даних; розпізнавання складних атак на рівні мережевого трафіку та програмного забезпечення; автоматичне блокування підозрілої активності без втручання людини; використання алгоритмів глибокого навчання для адаптації до нових загроз у режимі реального часу [3].

Водночас впровадження ШІ поряд із багатьма перевагами спричиняє появу нових викликів і проблем, серед яких:

- потреба навчання моделей на якісних даних, що потребує значних ресурсів;
- ймовірність появи нових видів атак, орієнтованих саме на обхід систем ШІ;
- забезпечення захисту самих алгоритмів МН від маніпуляцій і атак [1, 2].

Таким чином, впровадження ШІ в системи забезпечення кібербезпеки підприємств і об'єктів критичної інфраструктури є ефективним підходом до протидії сучасним кіберзагрозам, який дозволяє значно покращити безпеку корпоративних систем і мереж, зменшуючи ризики несанкціонованого доступу та витоку даних, а також створює можливість швидкої адаптації до нових атак.

### Література

1. Claire dela Luna. AI and Cyber Security: Innovations & Challenges. September 16, 2024. *eSecurityPlanet*. URL: <https://www.esecurityplanet.com/trends/ai-and-cybersecurity-innovations-and-challenges/>
2. The Rise of Artificial Intelligence in Cybersecurity: The Benefits and Drawbacks. June 9, 2024. *Cyber Security News*. URL: <https://cybersecuritynews.com/rise-of-ai-in-cybersecurity/>
3. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич, І., & Литвинов, В. Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2023. 2(22), С. 156–167. <https://doi.org/10.28925/2663-4023.2023.22.156167>

## МЕТОДИ АНАЛІЗУ ПОВЕДІНКИ КОРИСТУВАЧІВ ДЛЯ ВИЯВЛЕННЯ ВНУТРІШНІХ ЗАГРОЗ

Донцов Є. А.

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасне інформаційне середовище характеризується стрімким зростанням як зовнішніх, так і внутрішніх загроз. Особливу увагу привертає внутрішній фактор: неналежна поведінка співробітників або зловмисні дії осіб,

які мають легітимний доступ до корпоративних ресурсів. За даними останніх досліджень, значна частина інцидентів інформаційної безпеки виникає саме через людський фактор, що обумовлює необхідність впровадження інноваційних методів моніторингу діяльності користувачів. Технології аналізу поведінки користувачів (User Behavior Analytics, UBA/UEBA) дозволяють не лише ідентифікувати загрози на основі сигнатур, але й аналізувати аномальні дії, що відхиляються від встановлених моделей поведінки, що суттєво підвищує ефективність запобіжних заходів.

Основним завданням UBA/UEBA-систем є побудова «базової лінії» нормальної поведінки для кожного користувача та ІТ-об'єкта в організації. Це досягається за рахунок збору даних із численних джерел, таких як журнали подій, мережевий трафік, активність у системах автентифікації, електронна пошта та навіть внутрішнє спілкування у месенджерах [1]. За допомогою алгоритмів машинного навчання система аналізує ці дані, встановлюючи типовий шаблон поведінки для кожного суб'єкта. При виникненні відхилень від встановленої норми система автоматично порівнює поточні дії з базовими моделями та визначає ступінь аномальності. У разі перевищення порогових значень система генерує сповіщення, що дозволяє фахівцям з безпеки оперативно реагувати на потенційну загрозу [1; 3]. Цей підхід дозволяє виявляти як випадкові, так і свідомі спроби порушення політик безпеки.

Для ефективного аналізу поведінки користувачів використовуються різноманітні алгоритмічні та статистичні методи, серед яких можна виділити:

- Алгоритми класифікації. Супервізовані методи, такі як логістична регресія, дерева рішень, методи випадкового лісу (Random Forest) та опорні вектори (SVM), застосовуються для класифікації дій користувачів як нормальних чи аномальних. Ці алгоритми навчаються на історичних даних, щоб визначити, які характеристики поведінки свідчать про потенційну загрозу [3].
- Методи кластеризації. Неспостережувані алгоритми, такі як К-середніх (K-means), DBSCAN або ієрархічна кластеризація, дозволяють

групувати схожі поведінкові патерни. Виявлення груп, що значно відхиляються від основних кластерів, може сигналізувати про підозрілу активність.

- Алгоритми виявлення аномалій. Метод Isolation Forest, Local Outlier Factor (LOF) та інші алгоритми аномалій дозволяють безпосередньо виявляти дані, що відхиляються від норми. Такі підходи ефективні для своєчасного виявлення нових типів загроз, у тому числі атак нульового дня [3].

- Глибинні нейронні мережі та рекурентні нейронні мережі (LSTM). Використання автоенкодерів або LSTM дозволяє аналізувати часові ряди даних і виявляти складні патерни, що розвиваються у часі. Це особливо корисно для прогнозування майбутніх аномалій на основі попередніх спостережень.

- Статистичний аналіз та тестування гіпотез. Методи статистичної обробки даних дозволяють оцінити відхилення від середніх показників, визначити розподіл поведінкових характеристик та встановити порогові значення для спрацювання систем сповіщення.

- Нормалізація та стандартизація даних. Перед застосуванням алгоритмів важливо привести дані до єдиного масштабу, що дозволяє підвищити точність моделей і зменшити вплив шуму.

Ці методи у комплексі дозволяють створити точну модель нормальної поведінки, а також виявляти навіть найтонші відхилення, які можуть бути індикаторами внутрішніх загроз [3].

Інтеграція UBA/UEBA-рішень із системами управління інформацією та подіями безпеки (SIEM) є ключовим елементом для досягнення комплексного захисту організації. SIEM-системи консолідують дані з різних джерел та забезпечують централізований аналіз подій, що значно підвищує ефективність виявлення загроз [2]. Поєднання UBA/UEBA з SIEM дозволяє отримати більш повну картину подій у мережі: дані про аномальну поведінку користувачів доповнюють традиційні сигнатурні методи виявлення загроз. Крім того, інтеграція сприяє автоматизації процесів реагування, що зменшує час між виявленням загрози та прийняттям відповідних заходів. Таким чином, організації можуть швидше локалізувати проблему, провести детальний аналіз

інциденту та впровадити коригувальні заходи, що сприяє безперервності бізнес-процесів [2].

Після детального розгляду методів аналізу поведінки користувачів та інтеграції UBA/UEBA-рішень із SIEM-системами, важливо звернути увагу на практичні аспекти впровадження цих технологій у реальному середовищі. Розуміння переваг та викликів використання UBA/UEBA дозволяє організаціям більш ефективно планувати та оптимізувати свої заходи з кібербезпеки, а також враховувати можливі труднощі при експлуатації даних систем.

Переваги:

- Проактивне виявлення загроз. Завдяки постійному моніторингу та аналізу поведінки користувачів, UBA/UEBA-системи здатні виявляти потенційні загрози ще до того, як вони призведуть до серйозних інцидентів.
- Зменшення хибнопозитивних спрацювань. Використання алгоритмів машинного навчання дозволяє точніше розрізняти аномальну активність від нормальної, що знижує кількість помилкових сповіщень та оптимізує роботу операційних команд.
- Комплексний підхід до безпеки. Інтеграція з SIEM та іншими системами дозволяє створити єдину платформу, де дані аналізуються з різних точок зору.

Виклики:

- Обсяг даних та ресурси для аналізу. Ефективна робота UBA/UEBA-систем вимагає обробки великого обсягу даних, що може створювати високі вимоги до обчислювальних потужностей і зберігання інформації.
- Постійне навчання та адаптація. Зміни у робочому середовищі організації вимагають постійного оновлення моделей поведінки, що може ускладнювати процес налаштування системи та потребувати регулярного втручання експертів.
- Інтеграція з існуючими системами. Впровадження UBA/UEBA у вже діючі SIEM та інші системи безпеки може бути складним через різницю в

форматах даних та вимогах до сумісності, що потребує додаткових зусиль з боку ІТ-відділів [1; 3]

Загалом, впровадження технологій аналізу поведінки користувачів дозволяє організаціям своєчасно виявляти внутрішні загрози та ефективно управляти ризиками, забезпечуючи стабільність роботи інформаційних систем. Комплексне використання алгоритмів класифікації, кластеризації, виявлення аномалій і глибинного аналізу сприяє точному визначенню відхилень від норми.

Інтеграція з SIEM-системами створює єдину платформу для аналізу даних, що допомагає швидко локалізувати загрози та оптимізувати процес реагування. Незважаючи на певні виклики, ці технології є ключовими для підвищення кіберстійкості організації та забезпечення безперервності бізнесу.

## Література

1. Muzhanova, T. M.; Lehominova, S. V.; Yakymenko, Y. M.; Mordas, I. V. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. *Кібербезпека: освіта, наука, техніка*. 2021. Т. 1, № 13, с. 50–62. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/281>
2. IBM CORPORATION. IBM QRadar SIEM. IBM Security: White Paper / IBM Corporation. URL: <https://www.ibm.com/downloads/cas/RLXJNX2G>
3. Sadowski, G., Litan, A., Bussa, T., & Phillips, T. (2018). Market Guide for User and Entity Behavior Analytics. Gartner Inc. URL: <https://www.studocu.com/es-mx/u/60541508?sid=01739915822>

# НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

**Гаврилець Д. Р.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасні кіберзагрози стають усе більш складними, що потребує впровадження нових підходів до управління ризиками кібербезпеки. Основними трендами у цій сфері є використання штучного інтелекту, автоматизації безпеки, концепції Zero Trust та підвищення обізнаності співробітників.

Застосування штучного інтелекту та машинного навчання дає змогу аналізувати загрози в режимі реального часу, прогнозувати потенційні атаки та автоматизувати процеси реагування [1]. Автоматизація та оркестрація безпеки (SOAR) значно знижують ризики, пов'язані з людським фактором.

Концепція Zero Trust передбачає перевірку кожного користувача та пристрою незалежно від їх місця розташування, що значно знижує ризики внутрішніх загроз [2].



*Рис.1 Модель Zero Trust*

Також важливим аспектом є підвищення рівня обізнаності співробітників. Навчальні програми та тренінги з кібербезпеки допомагають зменшити ризик атак соціальної інженерії.

Таблиця 1 підсумовує вразливості, які можуть бути використані кожним із вищезгаданих інструментів зворотного інжинірингу [3].

Таблиця 1

### Порівняння методів управління кіберризиками

Метод	Опис	Переваги
Штучний інтелект	Використання алгоритмів ML для аналізу загроз	Висока швидкість реагування
Zero Trust	Контроль доступу на основі перевірки кожного елемента	Зменшення внутрішніх ризиків [4]
Автоматизація	Автоматичне виявлення та реагування на загрози	Мінімізація людського фактора [5]

Отже, новітні технології управління кіберризиками є необхідною умовою для забезпечення інформаційної безпеки організацій. Впровадження сучасних методів дозволяє мінімізувати ризики та підвищити стійкість інформаційних систем до загроз.

### Література

1. ISO/IEC 27001:2022. Information Security Management Systems.
2. NIST Cybersecurity Framework 2.0.
3. ENISA Threat Landscape 2024.
4. "The Role of Artificial Intelligence in Cybersecurity", Journal of Information Security, 2023.
5. Сервіси безпеки IT і Web3 URL: <https://www.h-x.technology/>

# КІБЕРЗАГРОЗИ ДЛЯ ОРГАНІЗАЦІЙ У СУЧАСНОМУ КІБЕРПРОСТОРІ

Легомінова С.В., д.е.н., проф., Петренко Н.В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Проблемою кожної організації являється нездатність захистити себе від величезної кількості вразливостей і зловмисників. За результатами аналізу проведених опитувань постачальників рішень з кібербезпеки, а саме 1Password, Cisco, CrowdStrike, Flashpoint, NetScout, Pentera та Sophos визначено п'ять основних загроз кібербезпеці, на які варто звернути увагу: зламані облікові дані, атаки на інфраструктуру, організовані та просунуті зловмисники, програми-вимагачі та неконтрольовані пристрої [1].

В таблиці 1 представлено ключові загрози з кібербезпеки організаціям, які виявлено основними постачальниками рішень з кібербезпеки.

Таблиця 1

## Кіберзагрози у сучасному кіберпросторі

Постачальник рішень з кібербезпеки	Загрози з кібербезпеки			
	Проблема паролів		Некеровані пристрої	
<b>1Password</b>	61% співробітників використовують неправильні методи введення пароля; 64% керівників і вище визнають, що неправильно використовують паролі; 23% використовують ідентичні паролі або дотримуються схожої моделі; 13% зберігають доступ до інструментів або ресурсів компанії після того, як залишили організацію; 9% діляться обліковими даними для робочих інструментів з людьми за межами компанії.		Документує мізерний контроль програмного забезпечення та доступу до персональних пристроїв: 92% політик компанії вимагають, але 59% зобов'язують ІТ-схвалення програмного забезпечення. 34% працівників використовують несанкціоновані додатки чи програмне забезпечення. 17% працівників працюють лише на персональних чи публічних комп'ютерах.	
<b>Cisco</b>	<b>Фішинг</b> <b>Підміна облікових даних</b> <b>Оновлення</b>	<b>Організовані та просунуті зловмисники</b>	<b>Програми-вимагачі та крадіжки даних</b>	<b>Некеровані пристрої</b>

	<b>програмного забезпечення, спрямовано на крадіжку облікових даних</b>				
	54% – Фішинг 37% – підміна облікових даних	62% компаній відзначили зовнішніх акторів як найбільшу загрозу проти 31% - внутрішніх акторів	Проаналізовано, що 35% усіх атак у 2023 році були програмами-вимагачами.	Відзначає загальний доступ персональних пристроїв і некерованих хмарних небезпек: 43% співробітників використовують некеровані пристрої для доступу до корпоративних мереж. 20% часу співробітників витрачається на мережу компанії. 27% усіх атак спрямовані на майнінг криптовалют, як правило, на неконтрольованих хмарних системах.	
<b>CrowdStrike</b>	<b>Фішинг</b>	<b>Атаки на інфраструктуру</b>	<b>Організовані та просунуті зловмисники</b>	<b>Програми-вимагачі та крадіжки даних</b>	<b>Некеровані пристрої</b>
	76% Фішинг	Моніторинг атак хакерів і розподілених DDoS-атак, пов'язаних із ізраїльсько-палестинським конфліктом, зокрема проти аеропорту США.	Відстежено значне зростання організованої супротивної активності: +34 нові групи противника (+18% від названих груп, +35% активних). Зростання інтерактивних (під керівництвом експертів) кампаній проникнення на +60% за рік. Зловмисники почали доставляти зловмисне програмне забезпечення користувачам за допомогою законних і звичайних інструментів П-підтримки, таких як ConnectWise ScreenConnect.	Спостерігали за політично афілійованими атаками програм-вимагачів проти Ізраїлю.	Спостерігає найвищий вектор атаки у 2023 році та передбачає цілі 2024 року: Некеровані мережеві пристрої (граничний шлюз, брандмауер, віртуальна приватна мережа/VPN) залишаються найбільш спостережуваним початковим вектором доступу, який використовувався у 2023 році. Зловмисники будуть націлені на мережеві периферійні пристрої: мережеве сховище (NAS), резервне

					сховище, телефони, мережеве обладнання та активи, що вийшли з експлуатації.
<b>Flashpoint</b>	<b>Програми-вимагачі та крадіжки даних</b>				
	<p>Зібрані статистичні дані про виявлене програмне забезпечення-вимагач і витоки даних:        +84% зростання кількості атак програм-вимагачів у порівнянні з минулим роком.        +34,5% у всьому світі, +19,8% у США за витоки даних за 2023 рік.        +30% витоків даних і +23% програм-вимагачів за перші два місяці 2024 року.        60% усіх порушень походять із США.        19,3% усіх порушень даних сталося через уразливість MOVEit, CVE-2023-34362, включно з розкриттям даних сторонніх розробників.        &gt; 54% усіх порушень даних походять від атак програм-вимагачів у виробництві, охороні здоров'я, уряді, фінансах, роздрібній торгівлі та технологічних галузях.</p>				
<b>Pentera</b>	<b>Некеровані пристрої</b>				
	<p>Зосереджено на основних джерелах порушень, на які посилаються корпоративні клієнти:        60% віддалених пристроїв.        54% локальної інфраструктури.        50% хмарних цілей.</p>				
<b>Sophos</b>	<b>Фішинг</b>	<b>Організовані та просунуті зловмисники</b>	<b>Програми-вимагачі та крадіжки даних</b>	<b>Некеровані пристрої</b>	
	43%	<p>Спостережувані зміни в поведінці зловмисників у відповідь на покращений захист:        Прийняті вразливі або зловмисні драйвери, коли Windows заблокувала макроси.        Розгортання шкідливої реклами та отруєння SEO, щоб уникнути інструментів виявлення.        Використовував активну взаємодію з кількома електронними листами після ефективної перевірки фішингу.</p>	<p>Зосередили свій звіт на малому та середньому бізнесі (SMB):        70% атак програм-вимагачів спрямовані на SMB.        &gt; 90% атак, про які повідомляють клієнти, стосуються крадіжки даних або облікових даних.</p>	<p>Виявлено, що незахищені пристрої є основною точкою входу для SMB-атак.</p>	

Інструментами зламу облікових даних визначають скомпрометовані ідентифікаційні дані через фішинг, викрадачі інформації, клавіатурні шпигуни та погані паролі, які являються є точкою входу для більшості атак програм-вимагачів і витоку даних. Зловмисники націлені на отримання облікових даних, тому більшість шкідливих програм розробляється в програмному забезпеченні для крадіжки облікових даних.

Пріоритетами щодо забезпечення кібербезпеки організацій можна визначити: вирішення проблем за допомогою розширеної автоматизації AI або ML. Також вирішення проблематики полягає у фінансуванні, сповіщенні, вирішення проблеми з нестачею кадрів і невирішеними вразливостями.

Cisco виявляє необхідність збільшення витрат на кібербезпеку. Pentera визначає необхідний бюджет на кібербезпеку - 1,27 мільйона доларів на рік для середнього бюджету безпеки IT.

1Password виявив, що 32% опитаних професіоналів із безпеки минулого року, які змінили інструменти або постачальників безпеки на ті, які пропонують більш повні наскрізні рішення.

Велика кількість інструментів породжує потік сповіщень (інцидент із безпекою, вразливість до виправлення) і тягне команди в протилежних напрямках. Великі команди можуть досягти достатнього прогресу, щоб стати проактивними, але більшість команд залишаються неукомплектованими. Багато ініціатив у сфері кібербезпеки не досягають прогресу через недостатню кількість персоналу.

Відсутність кадрів призводить до низки проблем. Найбільш очевидні помилки призводять до створення заголовків, як-от проблеми з паролями для клієнтів Okta (2022), оскільки персонал має бути на зв'язку 24/7. Більшість помилок залишаються прихованими ризиками, які чекають, щоб їх використали, особливо у формі відкритих уразливостей.

Виявлені вразливості. Більшість команд безпеки найбільше хвилюються через атаки нульового дня, які вражають без попередження. Однак набагато більше уваги слід приділяти відомим і невирішеним уразливостям.

Майже кожній четвертій організації важко йти в ногу з виправленнями. Несподівано привид стороннього ризику стає більш виразним, коли стає ймовірним, що принаймні частина кожного ланцюжка поставок матиме виявлені вразливі місця.

Крім того, двоє з п'яти встановлюють пріоритет на основі офіційних рейтингів уразливостей, але Flashpoint зазначає, що понад 100000 вразливостей

не мають ідентифікаційного номера відстеження, включаючи відомих постачальників, таких як Apache, Google, Microsoft і Zoho. Зловмисники активно використовують сотні цих невідстежуваних уразливостей, і це навіть не включає спірні вразливості, такі як вплив інфраструктури ShadowRay AI .

Тести на проникнення можуть виявити як відкриті, так і нерозпізнані вразливості, але більшість тестів на проникнення не охоплюють всю організацію.

Тестування на часткове проникнення. Тестування на проникнення перевіряє існуючі елементи керування, виявляє помилки та розкриває активи, перш ніж зловмисник зможе їх використати.

Отже, проведення пентесту у рамках розслідування порушень відбувається після інциденту, що засновується на реальній проблемі неукomплектовання кваліфікованим персоналом та перевантаженням.

### **Література**

1. Kime C., Lafferty M. 2024 State of Cybersecurity: Reports of More Threats & Prioritization Issues. URL: <https://www.esecurityplanet.com/threats/state-of-cybersecurity/>

## СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

### ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

**Бабенко А.В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

В умовах цифрової трансформації та зростання кіберзагроз досвід побудови організаційних систем захисту стає ключовим для забезпечення стійкості бізнесу, державних інституцій та критичної інфраструктури.

Організаційне забезпечення захисту інформації є стратегічним комплексом заходів, спрямованих на формування системи управління інформаційною безпекою. Його основна мета полягає у забезпеченні конфіденційності, цілісності, доступності та спостережуваності критичних активів організації [1]. Цей процес ґрунтується на принципах законності, системності, безперервності та чіткого розподілу відповідальності, що дозволяє інтегрувати захисні механізми у всі бізнес-процеси.

Система організаційного захисту формується через створення структурованих політик інформаційної безпеки, які регламентують доступ до даних, правила їх обробки та санкції за порушення. Ключову роль відіграє організаційна структура, де спеціалізовані підрозділи або призначені особи координують впровадження стандартів (наприклад, ISO/IEC 27001) та відповідність вимогам національного законодавства, зокрема Закону України "Про захист інформації в інформаційно-комунікаційних системах" [2].

Процес побудови системи включає етапи: аналіз ризиків з ідентифікацією загроз, розробку нормативної бази, впровадження техніко-організаційних заходів, навчання персоналу та постійний моніторинг ефективності. Особливу

увагу приділяється мінімізації впливу людського фактора через регулярні тренінги, мотиваційні механізми та контроль за дотриманням процедур [3].

Сучасні виклики, такі як динамічний розвиток кіберзагроз, зростання обсягів даних і еволюція нормативних вимог, вимагають гнучкості системи. Ефективне управління неможливе без адаптації до нових умов, інвестицій у кіберкультуру співробітників та впровадження проактивних стратегій аудиту [4].

Таким чином, організаційний захист інформації є динамічною складовою бізнес-стратегії, що потребує системного підходу, міждисциплінарної взаємодії та постійного оновлення. Його успіх залежить від збалансованості технічних рішень, правової відповідності та формування свідомого середовища безпеки в організації.

### **Література**

1. Закон України "Про захист інформації в інформаційно-комунікаційних системах". URL: <https://zakon.rada.gov.ua/laws/show/80/94%D0%B2%D1%80>
2. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.
3. Гуржій А.М., Дорошенко Ю.І. "Основи інформаційної безпеки". Київ: Наукова думка, 2019.
4. Положення про технічний захист інформації в Україні, затверджене постановою Кабінету Міністрів України від 27 січня 1995 р. № 46. URL: <https://zakon.rada.gov.ua/laws/show/46-95-%D0%BF>

# МЕТОДИ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕГУЛЯТОРНИМ ВИМОГАМ

Іпатов І. А.

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

В сучасному світі інформація є одним із найцінніших ресурсів, і її захист стає ключовим фактором для забезпечення стабільності та безпеки організацій. Стрімкий розвиток цифрових технологій, хмарних платформ, мобільних додатків та інтернету речей створює нові можливості для бізнесу, але водночас відкриває двері для кіберзлочинців. Збільшення кількості кібератак, витоків даних та зломів інформаційних систем підштовхує компанії до впровадження ефективної системи менеджменту інформаційної безпеки (СМІБ).

Основна мета СМІБ – це захист конфіденційності, цілісності та доступності інформації. Однак, для досягнення цієї мети організації повинні дотримуватися міжнародних стандартів та нормативних актів, які регламентують вимоги до захисту даних [1].

Серед основних регуляторних вимог виділяють:

- **ISO/IEC 27001** – міжнародний стандарт, який визначає вимоги до створення, впровадження та підтримки системи управління інформаційною безпекою.
- **NIST 800-53** – стандарт Національного інституту стандартів і технологій США, який містить контрольні заходи для захисту інформаційних систем та даних.
- **GDPR (General Data Protection Regulation)** – Загальний регламент захисту даних Європейського Союзу, що встановлює вимоги до захисту персональних даних.

- **Закон України "Про захист інформації в інформаційно-комунікаційних системах"** – національний нормативний акт, що регламентує вимоги до захисту інформації на території України.

Невиконання цих вимог може призвести до серйозних фінансових штрафів, втрати репутації та витоку конфіденційних даних. Саме тому організації зобов'язані впроваджувати ефективні заходи контролю, проводити оцінку ризиків та забезпечувати безперервний моніторинг інформаційної безпеки.

Ключові виклики, з якими стикаються компанії під час забезпечення відповідності СМІБ [2]:

- Виявлення та управління кіберзагрозами.
- Забезпечення захисту персональних даних.
- Управління інцидентами інформаційної безпеки.
- Підтримка безперервності бізнес-процесів у разі кібератак.
- Підготовка персоналу та підвищення їх обізнаності у сфері кібербезпеки.

Таким чином, забезпечення відповідності СМІБ регуляторним вимогам є не просто формальністю, а необхідною умовою для захисту критичних даних та збереження довіри клієнтів і партнерів.

### **1. Оцінка ризиків інформаційної безпеки**

Оцінка ризиків є основою для побудови ефективної системи інформаційної безпеки. Вона дозволяє ідентифікувати потенційні загрози, оцінити їх вплив на організацію та розробити заходи з мінімізації ризиків [3].

Основні підходи:

- **Кількісний аналіз** – базується на математичних розрахунках ймовірності виникнення загроз та потенційних фінансових втрат. Наприклад, розрахунок середнього збитку за інцидент та частоти його виникнення.
- **Якісний аналіз** – передбачає експертну оцінку рівня загроз та наслідків для організації. Використовуються рейтингові шкали, наприклад, високий, середній, низький рівень ризику.

- **Комбінований підхід** – поєднує кількісні та якісні методи для отримання більш точних результатів та побудови детального профілю ризиків.

## **2. Політики та процедури безпеки**

Розробка та впровадження політик є основою для забезпечення відповідності стандартам. Основні напрямки:

- **Управління доступом** – контроль ідентифікації та автентифікації користувачів, налаштування прав доступу до конфіденційної інформації.

- **Аудит інформаційної безпеки** – регулярна перевірка дотримання політик безпеки та виявлення вразливостей.

- **Реагування на інциденти** – створення планів реагування на кібератаки та мінімізація їх наслідків.

- **Управління активами та криптографічний захист даних** – класифікація інформаційних активів та захист конфіденційних даних за допомогою шифрування.

## **3. Використання міжнародних стандартів**

Виконання вимог міжнародних стандартів дозволяє забезпечити високий рівень безпеки та уникнути штрафів за недотримання регуляторних норм:

- **ISO/IEC 27001** – стандарт для створення системи управління інформаційною безпекою.

- **NIST 800-53** – набір контролів для захисту інформаційних систем.

- **GDPR** – Загальний регламент захисту даних Європейського Союзу.

## **4. Технологічні засоби забезпечення безпеки**

Використання сучасних технологічних інструментів допомагає виявляти та блокувати загрози в режимі реального часу:

- **Системи управління доступом (IAM)** – контроль автентифікації та авторизації користувачів.

- **Шифрування даних** – захист конфіденційних даних під час зберігання та передачі.

- **Системи моніторингу та аналізу подій (SIEM)** – виявлення аномальної активності та реагування на інциденти.

- **Антивірусні програми та фаєрволи** – захист від зловмисного програмного забезпечення та мережевих атак.

### 5. Аудит та моніторинг відповідності

Постійний контроль за дотриманням політик та процедур безпеки дозволяє вчасно виявляти порушення та реагувати на них [4]:

- **Внутрішній аудит** – регулярна перевірка відповідності стандартам та нормативам.

- **Зовнішній аудит** – оцінка незалежними експертами для підтвердження відповідності вимогам.

- **Моніторинг інцидентів** – аналіз журналів подій та виявлення аномалій у режимі реального часу.

Таблиця 1

#### Порівняльний аналіз політик та процедур

Метод забезпечення	Опис	Переваги	Недоліки
Оцінка ризиків	Аналіз загроз та наслідків	Виявлення слабких місць	Висока трудомісткість
Політики безпеки	Регламентування процесів	Систематизація захисту	Потребує регулярного оновлення
Використання стандартів	Дотримання ISO, NIST, GDPR	Підвищення рівня довіри	Висока вартість впровадження
Аудит та моніторинг	Постійний контроль відповідності	Виявлення порушень	Вимагає ресурсів

Забезпечення відповідності СМІБ регуляторним вимогам є важливим процесом, який потребує комплексного підходу. Поєднання аналізу ризиків, впровадження політик безпеки, дотримання міжнародних стандартів, використання технологічних рішень та постійного аудиту дозволяє ефективно захищати інформаційні ресурси організації.

### Література

1. ISO/IEC 27001:2022. Information Security Management Systems – Requirements.

2. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations.

3. Закон України "Про захист інформації в інформаційно-комунікаційних системах".

4. GDPR (General Data Protection Regulation).

## ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

**Петренко А. О.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасних умовах цифровізації та глобальної інтеграції бізнесу кіберзагрози стають дедалі серйознішими. Підприємства стикаються з широким спектром загроз, зокрема фішинговими атаками, зламами корпоративних систем, витоками даних та DDoS-атаками. Для зменшення впливу цих ризиків необхідне комплексне забезпечення кіберстійкості – здатності організації протистояти кібератакам, оперативно реагувати на інциденти та швидко відновлювати роботу після порушень безпеки.

### ***1. Створення ефективних структур управління кібербезпекою.***

Ключову роль у забезпеченні кіберстійкості відіграють спеціалізовані команди та відділи інформаційної безпеки. Ефективна структура управління включає [2].:

- ***Кібербезпекові центри (SOC – Security Operations Center)***, які займаються постійним моніторингом та аналізом загроз.

- ***Групи реагування на інциденти (CSIRT – Computer Security Incident Response Team)***, які відповідають за швидке виявлення та нейтралізацію атак.

- **Офіс управління ризиками (Risk Management Office)**, що аналізує потенційні загрози та розробляє заходи для їх мінімізації.

## **2. Організація команд реагування на кіберінциденти**

Створення команди реагування на інциденти є важливим компонентом кіберстійкості. Успішна команда CSIRT має:

- Чітко визначені ролі та обов'язки всередині організації.
- Доступ до сучасних інструментів для аналізу загроз (SIEM-системи, IDS/IPS тощо).
- Регламентовані процеси реагування на кіберінциденти, включаючи сценарії ліквідації наслідків атак [3].

## **3. Розробка внутрішніх політик та процедур безпеки**

Впровадження внутрішніх політик є основою забезпечення кіберстійкості. До них входять:

- Правила доступу до інформаційних ресурсів, що регулюють права користувачів та розмежування рівнів доступу.
- Політики управління паролями, які передбачають використання двофакторної автентифікації та регулярну зміну паролів.
- Регламенти оновлення програмного забезпечення, що зменшують ризик використання вразливостей у застарілих системах.
- Навчання співробітників з основ інформаційної безпеки та протидії соціальній інженерії [3].

## **4. Використання сучасних технологій у кіберзахисті**

Ключові технології, що підвищують кіберстійкість:

- Штучний інтелект та машинне навчання для виявлення аномальної активності та аналізу загроз.
- Технології блокчейн для забезпечення надійного захисту даних.
- Системи управління інформаційною безпекою (SIEM) для централізованого моніторингу кіберінцидентів.

- Автоматизовані платформи реагування (SOAR – Security Orchestration, Automation and Response) для швидкої ліквідації наслідків атак [3].

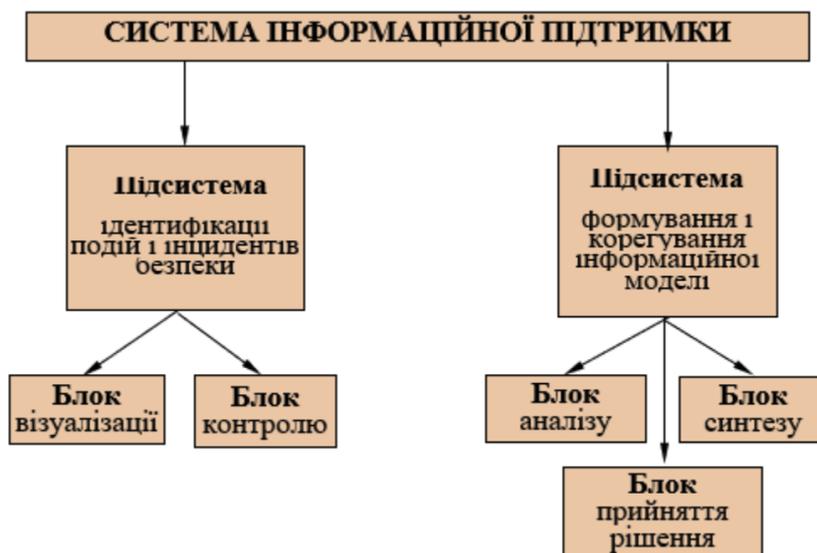


Рис.1 Структурна схема системи інформаційної підтримки

Результати дослідження показали, що кіберстійкість підприємства залежить не тільки від впровадження сучасних технологій, а й від організаційної складової. Побудова ефективної системи управління безпекою, організація груп швидкого реагування та розробка політик інформаційної безпеки є ключовими факторами захисту від загроз [4].

Перспективи подальших досліджень включають:

- Аналіз впровадження штучного інтелекту у системи моніторингу кіберзагроз.
- Дослідження впливу кібергігієни співробітників на загальний рівень безпеки підприємства.
- Опрацювання методів кіберзахисту для хмарних платформ та корпоративних мереж.

## Література

1. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних

системах. Постанова від 29 березня 2006 р. N 373 Верховна Рада України : Законодавство. – URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text>

2. Роль керівника у забезпеченні кіберзахисту своєї установи. Інтерв'ю з головою Держспецзв'язку Юрієм Щоголем / Реформа державного управління– Режим доступу: <https://par.in.ua/en/information/publications/90>

3. Alferidah, D.K. and Jhanjhi, N.Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.4, April 2020.

4. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса. 2015. Вип. 3. С. 220-237.

## **МЕТОДИ ІНТЕГРАЦІЇ CSIRT ТА SOC У РАМКАХ КОРПОРАТИВНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ**

**Книш Л. А.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Інтеграція Центру реагування на інциденти комп'ютерної безпеки (CSIRT) та Центру операцій безпеки (SOC) є ключовим елементом корпоративної стратегії кібербезпеки. SOC відповідає за постійний моніторинг та захист бізнес-сервісів, ІТ-систем та інфраструктури, виявлення вразливостей, кібер-атак, порушень політик та швидке реагування на інциденти. Ефективність SOC залежить від здатності швидко аналізувати події безпеки та координувати управління інцидентами до їх вирішення. Одним із основних завдань SOC є

зменшення часу виявлення загроз (MTTD) і часу на реагування (MTTR), що безпосередньо впливає на рівень безпеки організації [1].

CSIRT, у свою чергу, спеціалізується на реагуванні на кіберінциденти, розслідуванні та розробці рекомендацій для запобігання майбутнім атакам. Основною метою CSIRT є управління кризовими ситуаціями, створення планів реагування та аналіз типових атак, що дозволяє організаціям ефективніше протидіяти новим загрозам. Ця команда зазвичай складається з експертів із кібербезпеки, аналітиків загроз та спеціалістів із цифрової криміналістики, що дозволяє їй швидко визначати вектори атак та їхні наслідки. Завдяки інтеграції CSIRT та SOC забезпечується безперервний цикл моніторингу, виявлення та реагування на інциденти, що підвищує загальну стійкість організації до кіберзагроз [2].

Для успішної інтеграції необхідно розробити чіткі процеси взаємодії між командами, забезпечити обмін інформацією та спільне використання інструментів моніторингу та аналізу. Одним із ключових аспектів є автоматизація обробки подій безпеки, що дозволяє значно зменшити навантаження на аналітиків та скоротити час виявлення загроз. Сучасні системи управління інформаційною безпекою (SIEM) та технології розширеного виявлення та реагування (XDR) можуть забезпечити ефективний зв'язок між SOC та CSIRT, покращуючи швидкість обробки інцидентів. Важливо також проводити регулярні тренінги та симуляції для підвищення готовності персоналу до реальних кіберінцидентів. Розробка та впровадження спільних політик безпеки, а також використання стандартизованих методологій, сприяють ефективній координації дій між CSIRT та SOC [3].

Враховуючи зростаючу залежність сучасного суспільства від ІТ-систем та інфраструктури, інтеграція CSIRT та SOC стає невід'ємною частиною корпоративної стратегії кібербезпеки, забезпечуючи проактивний підхід до захисту інформаційних ресурсів та мінімізації потенційних ризиків. Застосування методів штучного інтелекту та машинного навчання у процесах SOC дозволяє виявляти аномальну активність, що може свідчити про складні

багатовекторні атаки. Розвиток SOC та CSIRT у напрямку розподіленого захисту (Cybersecurity Mesh) дозволяє забезпечити безпеку навіть у гібридних середовищах, які включають хмарні сервіси та локальні інфраструктури. У результаті, інтеграція цих двох підрозділів формує надійну систему кіберзахисту, яка здатна адаптуватися до змін у загрозах та оперативно реагувати на нові виклики [4].

### Література

1. Центр безпеки (Security Operation Center, SOC) на варті кібербезпеки. URL: <https://eska.global/blog/centr-bezpeki-security-operation-center-soc-na-varti-kiberbezpeki/>
2. CSIRT Державно науково-дослідного інституту технологій кібербезпеки та захисту інформації. URL: <https://csirt.csi.cip.gov.ua/>
3. НКЦК проводить дводенні навчання «Діяльність операційного центру (SOC) та синіх команд» - Рада національної безпеки і оборони України. URL: <https://www.rnbo.gov.ua/ua/Diialnist/5127.html?>
4. Як SOC допомагає реалізувати Cybersecurity Mesh - Octava Defence. URL: <https://octava.ua/yak-soc-dopomagaye-realizuvaty-cybersecurity-mesh/>

# ЛЮДСЬКИЙ ФАКТОР У СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА ISO/IEC 27001

Лоза О. Д.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Інформаційна безпека є критично важливим аспектом функціонування сучасних організацій. Одним із найефективніших інструментів для забезпечення безпеки даних є стандарт ISO/IEC 27001, який встановлює вимоги до системи управління інформаційною безпекою (СУІБ). Однак, навіть найсучасніші технології та політики безпеки можуть бути неефективними, якщо людський фактор не врахований належним чином.

Люди є ключовою ланкою в будь-якій системі безпеки: вони приймають рішення, обробляють дані, взаємодіють із системами та часто є першими, хто стикається з потенційними загрозами. Саме тому управління людським фактором та підвищення обізнаності персоналу має вирішальне значення для ефективного впровадження ISO/IEC 27001 [1].

Людський фактор може бути як найсильнішою, так і найслабшою ланкою у захисті інформаційних активів. Основні проблеми, пов'язані з людською поведінкою, включають:

- Низький рівень обізнаності про кіберзагрози – співробітники можуть не знати, як правильно поводитися у випадку атак або витоку даних.
- Недотримання політик безпеки – навіть при наявності чітких правил багато працівників нехтують ними через незручність або недостатній контроль.
- Соціальна інженерія – зловмисники використовують психологічні методи маніпуляції для отримання конфіденційної інформації [2].
- Недостатній контроль доступу – співробітники можуть несвідомо або навмисно передавати доступ до важливих систем стороннім особам.

Соціальна інженерія – це один із найбільш небезпечних методів атаки, який використовує довіру та психологічні слабкості людини. Найпоширеніші види атак:

- Фішингові атаки – електронні листи або повідомлення, які імітують офіційні запити та змушують жертву надати конфіденційні дані.
- Смішинг (SMS-фішинг) – атаки через SMS-повідомлення, які змушують користувачів перейти за шкідливими посиланнями.
- Вішинг (голосовий фішинг) – шахраї телефонують жертві, видаючи себе за представників банку, IT-відділу або державних установ.
- Tailgating – фізичний доступ до захищених зон через використання довіри співробітників [3].

Недостатній контроль доступу є ще однією загрозою, пов'язаною з людським фактором. Основні проблеми:

- Використання слабких паролів або їх повторне використання.
- Передача облікових даних між співробітниками.
- Недостатній контроль над правами доступу після звільнення співробітників [4].

Щоб мінімізувати ці ризики, ISO/IEC 27001 вимагає впровадження строгих політик управління доступами, зокрема принципу "найменшого необхідного доступу".

Організації, що впроваджують ISO/IEC 27001, повинні:

- Проводити регулярні тренінги з інформаційної безпеки.
- Використовувати симуляції фішингових атак для перевірки готовності персоналу.
- Розробити чіткі політики щодо безпечної поведінки в мережі [5].
- Оцінювати рівень обізнаності співробітників та коригувати навчальні програми.

Культура безпеки – це не просто дотримання правил, а спосіб мислення, що має бути інтегрованим у щоденну роботу кожного співробітника. Основні принципи:

- Лідерство керівництва – топ менеджмент має демонструвати важливість інформаційної безпеки.
- Заохочення відповідальної поведінки – винагороджувати працівників за активну участь у програмах безпеки.
- Прозора комунікація – створення механізму для швидкого повідомлення про потенційні загрози [5].

### Література

1. ISO/IEC 27001:2022. Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги. Женева: Міжнародна організація зі стандартизації, 2022. 40 с. URL:<https://www.iso.org/standard/27001>
2. Witkowski D., Benczik S., Jarrin P., Walker E. Cybersecurity – the Human Factor. National Institute of Standards and Technology (NIST), 2017. 5-6 с. URL:[https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017\\_Witkowski\\_Benczik\\_Jarrin\\_Walker\\_Materials\\_Final.pdf](https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf)
3. Національний інститут стандартів і технологій США (NIST). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. Вашингтон: Міністерство торгівлі США, 2020. 20-30 с. URL:<https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
4. AIG. Human Cyber Risk – The First Line of Defence. Лондон: AIG, 2023. 38 с. URL:<https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-human-factor.pdf>
5. NQA. ISO/IEC 27001:2022 Implementation Guide. Лондон: NQA, 2022. 56 с. URL:<https://www.nqa.com/getmedia/ae12c945-4dbb-4b73-a4e3-996261a540af/NQA-ISO-27001-Implementation-Guide.pdf>

# МЕТОДИЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСІВ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ

**Якименко Ю. М., к.в.н., доц.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному бізнес-середовищі процеси управління інцидентами інформаційної безпеки та безперервністю бізнесу стають невід'ємною частиною стратегії забезпечення стійкості підприємства. Особливо в умовах швидкої цифровізації та глобалізації, де ризики від неочікуваних подій, таких як кіберінциденти, природні катастрофи, технічні збої та інші кризові ситуації, можуть мати катастрофічні наслідки для бізнесу.

Згідно з дослідженнями [1;2], підприємства, які не враховують цих аспектів, значно більше ризикують зупинити свою діяльність через неготовність до кризових ситуацій. Наприклад, впровадження чітко прописаних інцидентних процедур і планів відновлення бізнесу допомогло знизити час простою у компаніях до 30%, що суттєво збільшило їх стійкість підтверджують отримані результати досліджень Тимченко і авторами відповідно до вимог [3]. Таким чином, важливість належної організації управління цими процесами стає очевидною. Тому основною метою подальших досліджень є розробка комплексних методичних підходів до забезпечення безперервності бізнесу в умовах постійних змін і нових загроз, в тому числі від сучасних інцидентів інформаційної безпеки. В такому разі завданнями в подальших дослідженнях є:

- Визначення основних процесів управління інцидентами та безперервністю бізнесу (планування, моніторинг, оцінка ризиків, управління інцидентами, планування відновлення).
- Оцінка існуючих підходів і стратегій щодо їх ефективності в умовах різних підприємств.

- Розробка детальних рекомендацій з інтеграції цих процесів у корпоративне управління підприємством.

Для виконання цих задач повинна бути створена система забезпечення процесів управління інцидентами інформаційної безпеки та безперервністю бізнесу (СЗПУІБтаББ) підприємства. Функціонально система повинна включати у вигляді взаємопов'язаних між собою підсистем, які теж можуть використовуватись як автономні систем для виконання інших функціональних задач (рис.1):

- Систему попередження та моніторингу для своєчасного виявлення потенційних загроз.
- Систему управління інцидентами, що включає процедури реагування, комунікації та відновлення безперервності бізнесу підприємства після інцидентів.
- Систему оцінки та аналізу ефективності для виявлення слабких місць і постійного вдосконалення стратегії діяльності підприємства.



Рис.1. Функціональна схема системи забезпечення процесів управління інцидентами інформаційної безпеки та безперервністю бізнесу підприємства.

Структурно важливо, щоб у процесах управління інцидентами інформаційної безпеки брали участь усі рівні організації їх виконання: від топ-менеджменту до технічних фахівців. Попередній аналіз функціонування цих

систем передбачає розподіл ролей і відповідальностей у межах підприємства для більш ефективного управління інцидентами інформаційної безпеки та безперервністю бізнесу.

Методика забезпечення самих управлінських процесів в СЗПУІБтаББ повинна включати декілька етапів:

1. Оцінка ризиків – для визначення потенційних інцидентів інформаційної безпеки, які можуть порушити безперервність бізнесу.

2. Планування – для створення планів по кожному з визначених ризиків, включаючи сценарії відновлення та підтримку основних функцій.

3. Впровадження процедур реагування – для налаштування систем моніторингу та звітності, а також навчання персоналу.

4. Тестування та вдосконалення – для проведення регулярних тренувань і тестів з метою перевірки ефективності процедур.

Місце і роль керівництва в управлінських процесах підприємства полягає в стратегічному управлінні, забезпеченні ресурсами та створенні організаційних заходів, орієнтованих на безперервність бізнесу.

На основі отриманих результатів дослідження можна зробити висновки:

- Методичні заходи щодо управління інцидентами та безперервністю бізнесу є критично важливими для підтримки стабільності організації в умовах змін.

- Вдосконалення існуючих методик має забезпечити зниження ризиків і покращення швидкості реагування на кризові ситуації і виявлення сучасних інцидентів інформаційної безпеки.

- Рекомендується впроваджувати інтегровані системи управління, що дозволяють не лише реагувати на інциденти, а ще і сприяють постійному покращенню процесів, спрямованих на забезпечення безперервності бізнесу підприємства.

### **Література**

1. Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В.. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. - Київ:

Радіотехніка.. Вип. 2021– 20 с. URL:  
[https://duikt.edu.ua/uploads/l\\_1066\\_72351971.pdf](https://duikt.edu.ua/uploads/l_1066_72351971.pdf).

2. Лекція 1 Поняття кризи та класифікація кризових явищ. 134с. URL:  
<https://web.kpi.kharkov.ua/kedcv/wp-content/uploads/sites/187/2018/05/Opornij-konspekt-lektsij.pdf>.

3. Ушатов В., Сєверінов О. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. URL:  
<https://openarchive.nure.ua/server/api/core/bitstreams/c2575d95-c877-47e6-aef8-2c19e286d900/content>.

## **ПІДГОТОВКА ДО РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПЛАНУВАННЯ, НАВЧАННЯ ТА ТЕСТУВАННЯ**

**Артеменко Н. Ю.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

З огляду на ескалацію загроз у цифровому середовищі, організації змушені вдосконалювати механізми реагування на інциденти інформаційної безпеки, оскільки неефективна протидія загрозам може призвести до значних фінансових втрат, порушення бізнес-процесів і компрометації критично важливих активів. Формування ефективної системи реагування є не лише тактичною, а й стратегічною необхідністю, що вимагає комплексного підходу, заснованого на міжнародних стандартах, передовій практиці та системному аналізі середовища загроз.

Одним із ключових елементів цього підходу є розроблення нормативно-регламентної бази реагування, що забезпечує уніфіковані процедури дій у разі виявлення інцидентів. Відповідно до рекомендацій NIST SP 800-61r2 [1],

ефективна система реагування повинна включати алгоритми ідентифікації, аналізу, локалізації, усунення наслідків та відновлення інформаційних ресурсів. Чітка регламентація кожного з етапів дає змогу мінімізувати часові витрати на прийняття критичних рішень та підвищити загальну ефективність реагування.

Важливою складовою забезпечення інформаційної безпеки є функціонування команди реагування на інциденти (CSIRT), формування якої передбачає чіткий розподіл ролей та зон відповідальності, а також забезпечення персоналу необхідними ресурсами для проведення оперативних заходів з ліквідації загроз. Згідно з професійним стандартом «Фахівець з реагування на інциденти кібербезпеки», ефективність таких команд безпосередньо залежить від рівня їхньої технічної експертизи, налагодженості внутрішньої взаємодії та доступу до засобів моніторингу, аналізу та протидії атакам.

Додатково, адаптивність системи реагування забезпечується інтеграцією методів оцінки та управління інформаційними ризиками, що дозволяє проводити превентивне моделювання сценаріїв атак і коригувати стратегію реагування відповідно до специфіки загроз. Як зазначено в [2], впровадження стандартів аудиту кібербезпеки є важливим інструментом для підвищення прозорості процесів оцінки ризиків та своєчасного виявлення критичних вразливостей, що створюють потенційні вектори атак.

Системний підхід до організації реагування на інциденти дозволяє не лише мінімізувати наслідки порушень інформаційної безпеки, а й підвищити рівень кіберстійкості організації загалом, що є ключовим чинником у забезпеченні довготривалої безпеки інформаційних активів у динамічному середовищі загроз.

Додатково рекомендується проводити регулярні симуляційні вправи, що моделюють реальні інциденти, з метою відпрацювання навичок та покращення координації дій між різними підрозділами. Ефективне забезпечення інформаційної безпеки вимагає інтеграції технічних заходів із людським фактором (табл. 1) [3].

**Ключові організаційні заходи**

<b>Заходи</b>	<b>Пояснення</b>
Перевірка персоналу (Screening)	Перед прийомом на роботу проводиться ретельна перевірка кандидатів. Перевірка досвіду, кримінального минулого.
Умови працевлаштування та угоди про конфіденційність	Працівники повинні бути ознайомлені з вимогами інформаційної безпеки ще до вступу в посаду. Це включає чітке визначення обов'язків у трудових договорах і підписання конфіденційних угод (NDA).
Навчання та підвищення обізнаності	Вимоги регулярного проведення тренінгів та навчальних заходів, які допомагають співробітникам розуміти політики безпеки, їхні ролі у захисті інформації.
Дисциплінарні процедури	Визначаються чіткі правила та процедури, які описують наслідки порушення політик безпеки.
Заходи при зміні статусу	Стандарт передбачає, що при звільненні або зміні посад у працівника мають бути негайно припинені доступи до критичних систем, а також здійснено повернення корпоративних активів і інформації.
Політика віддаленої роботи	Для співробітників, які працюють віддалено, повинні бути розроблені спеціальні заходи
Процедури повідомлення про інциденти	Працівники мають бути чітко проінформовані про те, як і куди повідомляти про будь-які інциденти чи підозрілу активність.

Регулярні аудити систем безпеки, в свою чергу, дозволяють виявити слабкі місця та оцінити готовність організації до потенційних інцидентів, а використання сучасних автоматизованих систем моніторингу та виявлення загроз забезпечують оперативне реагування та скорочують час усунення інцидентів [4].

Таким чином, організаційні заходи, що передбачені стандартом, охоплюють розробку внутрішньої документації, формування спеціалізованої команди, систематичну оцінку ризиків, регулярне навчання персоналу та впровадження ефективних механізмів контролю та моніторингу. Це забезпечує всебічний захист інформаційних активів та сприяє підвищенню загальної кібербезпеки організації.

**Література**

1. (SP) 800-61r2. Керівні настанови щодо управління інцидентами, пов'язаними з комп'ютерною безпекою. Чинний від 2012-03-01. Вид. офіц.

Гейтесбург, штат Меріленд : Нац. ін-т стандартів і технологій США, 2012. 90 с.  
URL: <https://doi.org/10.6028/NIST.SP.800-61r2>

2. Курій Є. О. Методологія підвищення захищеності об'єктів критичної інфраструктури за рахунок перехресного впровадження стандартів аудиту з кібербезпеки : дис. д-ра філософії в галузі техн. наук : 125. Львів, 2024. 287 с.  
URL: <https://lpnu.ua/sites/default/files/2024/radaphd/27652/disertaciya-kurii-eo.pdf>

3. INFORMATION SECURITY CONTROLS. *ISO/IEC 27001:2022*. 2022. P. 28–36. URL: <https://doi.org/10.2307/j.ctv30qq13d.8>

4. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

## **ФОРМУВАННЯ КОНТЕКСТУ ОЦІНКИ РИЗИКІВ У СИСТЕМАХ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Жестков Д. І.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Стрімкий розвиток інформаційних технологій супроводжується експоненційним зростанням кіберзагроз, що зумовлює необхідність комплексного та системного підходу до управління інформаційною безпекою. Для організацій різних секторів економіки забезпечення кіберстійкості стає пріоритетним завданням, оскільки несанкціоновані дії зловмисників можуть спричинити значні фінансові, репутаційні та операційні втрати. За прогнозами Cybersecurity Ventures, сукупні глобальні збитки від кіберзлочинності у 2023 році мали перевищити \$8 трлн [1]. Водночас, згідно зі звітом ФБР, опублікованим у квітні 2024 року, фактичні втрати світової економіки внаслідок

кіберзлочинних дій за підсумками 2023 року сягнули \$12,5 млрд (рис. 1) [2]. Така розбіжність у прогнозованих та фактичних показниках свідчить про зростаючу складність та динамічність середовища загроз, що ускладнює традиційні підходи до оцінки ризиків та запобігання атакам.

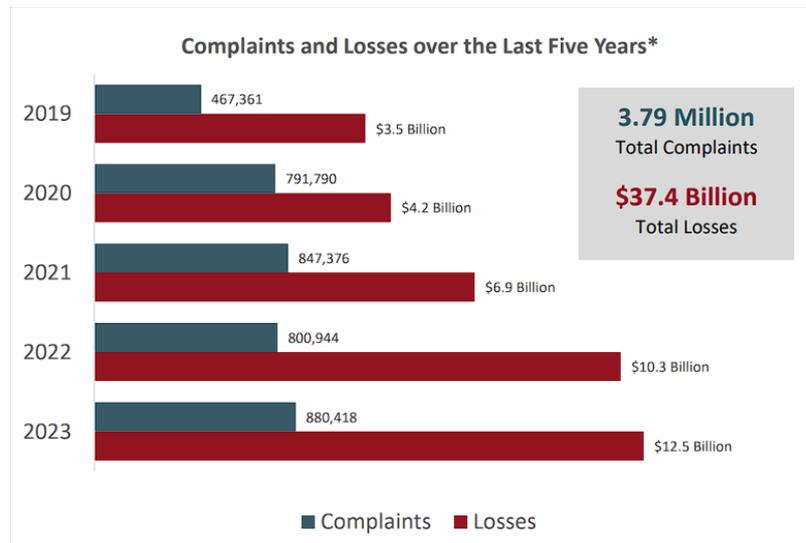


Рис. 1 Статистика збитків у рік за даними ФБР

За таких умов критичним стає впровадження систем менеджменту інформаційної безпеки, що забезпечують структуровану методологію оцінки, контролю та мінімізації кіберризиків. Ефективне функціонування таких систем передбачає застосування адаптивних моделей ризик-менеджменту, заснованих на міжнародних стандартах (ISO/IEC 27001, NIST CSF) та інтеграцію механізмів проактивного моніторингу загроз.

Підготовка до оцінки ризиків є початковим етапом у процесі їх аналізу, який визначає ключові параметри та забезпечує методологічну основу для подальшої оцінки. Основним завданням цього етапу є встановлення контексту оцінювання ризиків, що передбачає врахування організаційних, нормативно-правових та методологічних аспектів управління ризиками. Формування цього контексту ґрунтується на результатах попередніх етапів управління ризиками, зокрема процесу ідентифікації та формування ризиків, що визначає ключові політики, вимоги до оцінювання, методологічні підходи, а також критерії вибору релевантних факторів ризику.

Ефективна підготовка до оцінки ризиків передбачає уніфікацію процедур аналізу шляхом визначення рівня деталізації, ступеня формальності, охоплення оцінки, а також механізмів забезпечення узгодженості та повторюваності результатів у межах організації. Використання стратегічного підходу до управління ризиками дозволяє формалізувати процес підготовки та отримати необхідні дані для подальшого аналізу.

Згідно з міжнародними стандартами управління ризиками, ключовими завданнями етапу підготовки є [3]:

- формулювання мети оцінки, що визначає очікувані результати та критерії прийняття рішень;
- визначення обсягу оцінки, який охоплює межі аналізу, залучені ресурси та рівень деталізації оцінювання;
- ідентифікація припущень та обмежень, які впливають на методологічні підходи та валідність отриманих результатів;
- аналіз джерел інформації, що будуть використані як вхідні дані для оцінювання ризиків, включно з історичними даними, експертними оцінками та аналітичними звітами;
- визначення моделі ризику та аналітичних підходів, що передбачає вибір методів ідентифікації, оцінки та аналізу ризиків, зокрема кількісного та якісного моделювання загроз.

Системний підхід до підготовки оцінки ризиків забезпечує обґрунтованість і точність подальших рішень у сфері кібербезпеки, підвищує ефективність реагування на загрози та сприяє розробленню заходів зниження ризиків відповідно до поточного середовища загроз.

## Література

1. 2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics. URL: <https://cybersecurityventures.com/cybersecurity-almanac-2023/>
2. Federal Bureau of Investigation. Internet Crime Report 2023. *Internet Crime Complaint Center (IC3)*. URL: [https://www.ic3.gov/annualreport/reports/2023\\_ic3report.pdf](https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf)

3. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. *U.S. Department of Commerce, National Institute of Standards and Technology*. URL: <https://doi.org/10.6028/NIST.SP.800-30r1>

## **РОЛЬ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНИХ СЕРЕДОВИЩАХ**

**Пехова Л. О.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Політика інформаційної безпеки (ПІБ) є ключовим елементом забезпечення захисту інформаційних ресурсів у корпоративних середовищах. Вона визначає основні принципи, процедури та заходи, спрямовані на захист конфіденційності, цілісності та доступності інформації в організації. Однак, ефективна політика ІБ – це не лише дотримання стандартів і регламентів, а й розуміння специфіки кожного бізнесу та його загроз. Саме тому компанії повинні адаптувати свої стратегії безпеки до реальних викликів та потреб [1]. Крім того, важливо враховувати, що корпоративна політика безпеки не є статичним документом – вона повинна постійно переглядатися та вдосконалюватися відповідно до змін у середовищі загроз.

Основними завданнями ПІБ у корпоративному середовищі є:

1. Визначення стратегічних напрямів захисту інформаційних активів компанії.
2. Формування культури інформаційної безпеки серед співробітників.
3. Регламентація доступу до інформаційних ресурсів на основі принципів мінімальних привілеїв та Zero Trust.
4. Реалізація механізмів реагування на інциденти безпеки та планів аварійного відновлення.

5. Впровадження сучасних методів шифрування даних для захисту інформації як у стані збереження, так і під час передачі.

6. Впровадження механізмів моніторингу та контролю дотримання політики ІБ [2].

Одним із ключових аспектів ефективності ПІБ є її інтеграція у загальні бізнес-процеси. Безпека не повинна розглядатися як окремий компонент, що обмежує діяльність співробітників. Навпаки, добре структурована політика ІБ допомагає підвищити ефективність роботи, зменшуючи ризики простою систем та втрати даних через атаки або технічні збої. Успішна інтеграція політики безпеки в корпоративну культуру сприяє формуванню проактивного підходу до захисту інформації.

Наразі існують основні виклики, що впливають на ефективність політики ІБ:

- Різноманітність інформаційних систем, що використовуються в корпоративному середовищі.
- Вплив людського фактора та необхідність постійного навчання персоналу.
- Баланс між безпекою та продуктивністю: жорсткі заходи можуть обмежувати роботу співробітників, тому політика має бути гнучкою.
- Висока вартість впровадження сучасних рішень інформаційної безпеки та необхідність оцінки економічної доцільності таких заходів.
- Динамічний розвиток загроз, що вимагає регулярного оновлення політики безпеки [1].

Компанії впроваджують різні підходи для забезпечення ефективності політики ІБ. Одним із ключових напрямів є автоматизація управління доступом та моніторинг дотримання політики за допомогою SIEM-систем та технологій управління ідентифікацією та доступом (IAM) [1]. Разом із цим важливо підтримувати баланс між автоматизованими рішеннями та людським фактором, оскільки безпека значною мірою залежить від відповідальності та свідомості співробітників. Регулярне тестування систем захисту, проведення навчальних

тренінгів та впровадження механізмів зворотного зв'язку дозволяють покращити загальний рівень інформаційної безпеки.

Окрім технічних аспектів, важливу роль у впровадженні ефективної політики ІБ відіграє нормативно-правове регулювання. Компанії повинні враховувати вимоги міжнародних стандартів, таких як ISO/IEC 27001, а також законодавчі акти у сфері кібербезпеки. Важливим є ідентифікація критичних активів організації та оцінка ризиків їх втрати або компрометації. В цьому контексті важливу роль відіграє концепція управління ризиками, яка дозволяє визначити пріоритети безпекових заходів на основі можливого впливу загроз.

Ефективна політика інформаційної безпеки є невід'ємною складовою корпоративної стратегії управління ризиками. Її впровадження дозволяє організаціям підвищити рівень захисту інформаційних активів, забезпечити відповідність нормативним вимогам та зменшити ймовірність реалізації кіберзагроз. Водночас, політика ІБ повинна бути живим документом, що адаптується до змін у технологічному середовищі та внутрішніх процесах компанії [2]. Важливо пам'ятати, що ефективність політики інформаційної безпеки визначається не лише технічними заходами, а й рівнем усвідомленості персоналу щодо потенційних загроз та методів їх мінімізації.

### **Література**

1. ISO/IEC 27001:2022. Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги.
2. Ністор О.М. Управління інформаційною безпекою підприємства: навчальний посібник. – К.: НАУ, 2020. – 256 с.

## ZERO TRUST ЯК СТРАТЕГІЯ КІБЕРЗАХИСТУ: ПРИНЦИПИ, ВПРОВАДЖЕННЯ ТА ПЕРСПЕКТИВИ

Кондратюк Д. О.

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Ми живемо у світі, де технології розвиваються стрімкими темпами, і традиційні підходи до кібербезпеки більше не можуть гарантувати надійний захист. Зі зростанням кількості віддалених користувачів, хмарних сервісів та мобільних пристроїв компанії стикаються з новими викликами у сфері кібербезпеки. Саме тому стратегія **Zero Trust** набуває все більшої популярності. Цей підхід базується на принципі «**Нікому не довіряй, усе перевіряй**», що означає повну перевірку кожного користувача, пристрою та запиту перед наданням доступу до ресурсів.

Ще у 2020 році дослідницька компанія **Gartner** прогнозувала, що понад 60% організацій перейдуть на модель **Zero Trust** до 2023 року [1]. Такий підхід значно знижує ризик внутрішніх і зовнішніх атак, оскільки доступ надається не на основі довіри до корпоративної мережі, а на основі суворої ідентифікації та авторизації кожної операції.

Zero Trust включає кілька ключових принципів:

1. Перевірка кожного доступу – кожен запит до системи має бути автентифікований та авторизований.
2. Мінімальні привілеї – користувачі отримують доступ лише до тих ресурсів, які їм необхідні для роботи.
3. Сегментація мережі – поділ мережі на окремі зони, щоб обмежити можливості зловмисників у разі атаки.
4. Моніторинг та аналіз загроз – постійний контроль активності користувачів та автоматизоване виявлення аномалій.

5. Автоматизація реагування – впровадження механізмів машинного навчання для швидкого виявлення та усунення загроз.

Одним із основних викликів у впровадженні Zero Trust є його складність та потреба у комплексному підході до управління доступом. Проте компанії, які впровадили цей підхід, значно знижують ризики витоку даних та фінансових втрат через кібератаки. Наприклад, корпорації Google та Microsoft уже реалізували Zero Trust у своїх мережах, що значно підвищило їхню кіберстійкість [2].

Таким чином, стратегія Zero Trust стає необхідністю для сучасних організацій. Вона дозволяє підвищити рівень кібербезпеки, знизити ризики внутрішніх загроз та мінімізувати вплив атак. Впровадження цієї моделі потребує ретельного планування та технологічної модернізації, проте її переваги значно переважають потенційні труднощі. На мою думку, Zero Trust є одним із найперспективніших напрямів у сфері кіберзахисту, який забезпечить надійний захист даних у цифрову епоху.

## Література

1. Gartner Research: "Zero Trust Security Model Adoption Trends" (2020). URL: <https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust>
2. Gonçalves G., O'Malley K., Beyer, B., Saltonstall M. BeyondCorp and the long tail of Zero Trust // login. 2023. 52423. URL: <https://www.usenix.org/publications/loginonline/beyondcorp-and-long-tail-zero-trust>.

## **СЕКЦІЯ 4. ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ**

### **ВПРОВАДЖЕННЯ ZERO TRUST ЯК КЛЮЧОВОГО ПІДХОДУ ДО БЕЗПЕКИ**

**Слободська Л. О.**

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

У сучасному цифровому середовищі, де межі між внутрішніми та зовнішніми ресурсами організацій стають дедалі розмитішими, традиційні методи забезпечення безпеки втрачають свою ефективність. Підхід Zero Trust (нульової довіри) виник як відповідь на ці виклики, пропонуючи нову парадигму захисту мереж та операційних систем.

Zero Trust базується на принципі, що жоден користувач чи пристрій не повинні автоматично довірятися, незалежно від їхнього розташування — всередині чи поза межами корпоративної мережі. Кожен запит на доступ повинен бути автентифікований, авторизований та підданий перевірці перед наданням доступу до ресурсів. Цей підхід передбачає постійний моніторинг та перевірку всіх користувачів і пристроїв, незалежно від того, намагаються вони отримати доступ до ресурсів у межах периметра мережі чи з віддалених місць.

[1]

Впровадження Zero Trust не є одноразовою дією, а скоріше поступовим процесом, який вимагає ретельного планування та оцінки поточної інфраструктури безпеки. Першим кроком є оцінка наявної системи безпеки та визначення чутливих даних, активів та сервісів. Більшість організацій уже мають основні компоненти для впровадження політики нульової довіри. Йдеться не про необхідність починати з нуля, а про те, щоб отримати загальний огляд поточної ситуації та оцінити, де є прогалини. [2]

Наступним етапом є стратегічне планування, яке повинно враховувати довгострокові бізнес-цілі та забезпечувати безпеку, яка відповідає цим цілям. Політика безпеки не повинна визначати, як працює організація. Необхідно розглянути оцінку ризиків, бізнес-вимоги, аналіз поточних інструментів та їх використання. Залежно від розміру та сфери діяльності організації, а також від рівня зрілості наявних налаштувань безпеки, ця частина роботи може зайняти від кількох тижнів до кількох місяців.

Впровадження Zero Trust вимагає використання сучасних засобів мережевої та операційної безпеки. Одним із ключових аспектів є суворе управління ідентифікацією та доступом. Це включає багатофакторну аутентифікацію (MFA), яка забезпечує додатковий рівень захисту, вимагаючи від користувачів підтвердження своєї особи за допомогою декількох методів. Наприклад, налаштування MFA та умовного доступу для захисту облікових записів є важливим кроком у забезпеченні безпеки. [3]

Крім того, важливо забезпечити безпеку при зберіганні та транспортуванні даних. Це можна досягти шляхом шифрування внутрішніх каналів зв'язку, обмеження доступу за політиками та мікросегментації мережі. Використання телеметрії для виявлення атак й аномалій, автоматичне блокування та позначення підозрілих дій також сприяє підвищенню рівня безпеки.

Інтеграція систем кіберзахисту в корпоративну інфраструктуру є критично важливою для успішного впровадження Zero Trust. Це включає впровадження рішень, які забезпечують контроль пристроїв і доступ на основі ролей і політик, захищають від зовнішніх та внутрішніх загроз і звільняють ІТ-персонал від марудної роботи. Наприклад, рішення Aruba ClearPass забезпечують контроль пристроїв і доступ на основі ролей і політик, захищають від зовнішніх та внутрішніх загроз.

Важливо також забезпечити безпеку в хмарних середовищах та при використанні SaaS-додатків. Інтеграція з Zero Trust дозволяє автоматизувати доступ і реагувати на нові загрози, забезпечуючи надійний підхід до безпеки.

Наприклад, Cisco Secure Firewall забезпечує відмінну видимість зашифрованого трафіку та підтримує масштабованість завдяки можливостям кластера, що підвищує продуктивність у гібридних мережах. Завдяки інтеграції з Zero Trust, Cisco Secure Firewall допомагає реалізувати надійний підхід до безпеки, автоматизуючи доступ і реагуючи на нові загрози. [4]

В умовах зростаючих кіберзагроз та еволюції робочих середовищ, впровадження моделі Zero Trust стає критично важливим для забезпечення надійної безпеки організацій. Цей підхід, заснований на принципі "ніколи не довіряй, завжди перевіряй", дозволяє мінімізувати ризики, пов'язані як із зовнішніми атаками, так і з внутрішніми загрозами. Завдяки суворому контролю доступу та постійному моніторингу, Zero Trust забезпечує підвищену видимість та контроль над мережевою активністю, що є ключовим для своєчасного виявлення та запобігання інцидентам безпеки. Хоча впровадження цієї моделі може вимагати значних зусиль та ресурсів, її переваги у вигляді посиленої безпеки та адаптивності до сучасних викликів роблять Zero Trust незамінним елементом стратегії кіберзахисту будь-якої організації.

## Література

1. Впровадження безпеки на підприємствах з Zero Trust Security. URL: <https://sib.com.ua/sib-1-130-2024/zero-trust.html>.
2. Як впровадити Zero Trust модель. SoftwareOne blog. *SoftwareOne*. URL: <https://www.softwareone.com/uk-ua/blog/articles/2024/04/05/how-to-implement-a-zero-trust-model>.
3. Комплексні рішення Security на базі моделі Zero Trust. *Cloud*. URL: <https://cloud.smart-it.com/security/>.
4. Актуальні тренди в кібербезпеці: погляд Cisco. *Integrity Vision*. URL: <https://integrity.com.ua/aktualni-trendy-v-kiberbezpeczi-poglyad-cisco/>.

# АНАЛІЗ ТЕМПІВ ЗРОСТАННЯ ФІШИНГОВИХ АТАК: НОВІ МЕТОДИ ОЦІНКИ РИЗИКІВ

**Святська Н. А., Запорожченко М. М., Примаченко Д. В.**

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

За останні роки кількість фішингових атак значно зросла: згідно з повідомленнями, 57% організацій зазнають фішингових атак щодня або щотижня. Стрімке зростання частоти атак пов'язане зі зростаючою витонченістю фішингових тактик, включаючи створення електронних листів за допомогою штучного інтелекту та багатовекторні стратегії атак. Дані Антифішингової робочої групи (APWG) показали, що тільки в третьому кварталі 2023 року було зареєстровано 493,2 мільйона фішингових атак, що на 173% більше, ніж у другому кварталі того ж року. Таке експоненціальне зростання підкреслює еволюцію ландшафту загроз і необхідність постійного моніторингу та адаптивних заходів безпеки.

Фінансовий сектор залишається найбільш вразливою галуззю: 23% фішингових атак спрямовані на фінансові установи. На платформи соціальних мереж і SaaS-провайдерів припадає по 22,3%, що ілюструє, як кіберзлочинці використовують популярні цифрові платформи для здійснення масштабних атак. Оманливі посилання залишаються найпоширенішим методом фішингу, на який припадає 36% фішингових загроз, проаналізованих у базі даних з 13 мільярдів електронних листів. Зловмисники часто видають себе за великі бренди, такі як Microsoft, Google та Amazon, причому 51,7% шкідливих листів маскуються під офіційні повідомлення цих компаній [1].

Одним з основних чинників зростання кількості фішингових атак є інтеграція штучного інтелекту в методології атак. Фішингові атаки зі штучним інтелектом використовують обробку природної мови (NLP) та машинне навчання (ML) для створення високореалістичних повідомлень, які імітують

людську поведінку. Такий підхід підвищує ефективність фішингових атак, оскільки звичайні заходи безпеки не в змозі виявити тонкі варіації мови та структури, які може створювати ШІ. За даними Zscaler ThreatLabs, зростання кількості фішингових листів, створених штучним інтелектом, значно знизило ефективність традиційних систем виявлення, заснованих на правилах.

Поширення програм-вимагачів через фішингові канали ще більше посилює ризик. Приблизно 35% атак з використанням програм-вимагачів відбуваються через фішингові електронні листи, що підкреслює критично важливу роль, яку відіграє безпека електронної пошти в запобіганні більш широким кіберзагрозам. Паралельно з цим, поява смішингу (SMS-фішинг) та вішингу (голосового фішингу) розширила сферу застосування фішингових атак. Звіти свідчать про 30% зростання кількості вішингових атак за минулий рік, при цьому організації зазнають щорічних збитків в середньому на \$14 млн через шахрайські голосові атаки [2].

Фішингові сайти створюються з безпрецедентною швидкістю: кожні 20 секунд у світі з'являється новий фішинговий сайт. Сполучені Штати повідомляють, що 36% всіх витоків даних пов'язані з фішингом, що підкреслює його роль як основного вектора атаки. Незважаючи на розвиток методів автентифікації електронної пошти, таких як SPF, DKIM і DMARC, 89% шкідливих електронних листів обходять ці заходи безпеки, що свідчить про потребу в більш досконалих моделях виявлення.

Оцінка фішингових ризиків еволюціонувала завдяки інтеграції предиктивної аналітики на основі штучного інтелекту та машинного навчання. Традиційні моделі ризику покладалися на статичну евристику, але сучасні підходи використовують динамічний поведінковий аналіз для виявлення аномалій у режимі реального часу. Ці моделі оцінюють безліч параметрів, включаючи репутацію відправника, структуру контенту, достовірність посилань і моделі взаємодії з одержувачем. Удосконалені системи виявлення фішингу використовують алгоритми глибокого навчання для аналізу великих

масивів даних, підвищуючи точність ідентифікації загроз і водночас зменшуючи кількість хибних спрацьовувань.

Одним з нових методів оцінки ризиків фішингу є використання байєсівських мереж, які моделюють імовірнісні зв'язки між різними факторами ризику. Аналізуючи історичні дані та постійно оновлюючи розподіли ймовірностей, байєсівські моделі можуть забезпечити більш адаптивну та точну систему оцінки ризиків. Крім того, алгоритми кластеризації, такі як K-середнє та ієрархічна кластеризація, застосовуються для виявлення закономірностей у фішингових атаках, що дозволяє класифікувати характеристики електронної пошти з високим рівнем ризику.

Поведінкова біометрія пропонує ще один рівень оцінки фішингових ризиків, аналізуючи патерни взаємодії користувачів. Динаміка натискання клавіш, патерни руху миші та час відгуку оцінюються для виявлення відхилень від нормальної поведінки користувача. Цей підхід виявився особливо ефективним у боротьбі з фішинговими атаками типу «спис», коли зловмисники видають себе за відомі контакти, щоб маніпулювати жертвами і змусити їх розголошувати конфіденційну інформацію. Організації, які впроваджують поведінковий біометричний аналіз, повідомили про зменшення на 60% кількості витоків даних, пов'язаних з фішингом [3].

Системи оцінки ризиків у режимі реального часу тепер включають автоматизовані канали розвідки загроз для покращення виявлення фішингу. Ці системи агрегують дані з різних джерел, включаючи моніторинг темного Інтернету, бази даних фішингових атак і звіти про дослідження в галузі кібербезпеки. Постійно оновлюючи параметри ризику на основі даних про нові загрози, організації можуть проактивно виявляти і нейтралізувати фішингові кампанії ще до їх ескалації.

Виявлення аномалій на основі графіків - ще один перспективний метод оцінки фішингових ризиків. Відображаючи зв'язки між відправниками, одержувачами та доменами електронної пошти, графові моделі можуть виявляти незвичайні патерни, що вказують на спроби фішингу. Такий підхід

підвищує точність виявлення, особливо для атак на ділову електронну пошту (BEC), які часто пов'язані з ледь помітними відхиленнями від легітимної поведінки електронної пошти.

На зростання кількості фішингових атак також вплинуло збільшення використання хмарних сервісів. Кіберзлочинці використовують вразливості в хмарних механізмах автентифікації для запуску масштабних фішингових кампаній. Cloudflare повідомляє, що 35,6% фішингових атак пов'язані з переходом за шкідливими посиланнями, вбудованими в документи, що зберігаються в хмарі, що ускладнює їх виявлення за допомогою звичайних методів фільтрації електронної пошти [4].

Оцінка фішингових ризиків ще більше покращилася завдяки змагальним методам машинного навчання, які тренують моделі ШІ, використовуючи зразки оманливих фішингових атак, щоб покращити можливості виявлення. Піддаючи моделі виявлення змагальним прикладам, дослідники підвищили стійкість фішингових фільтрів, керованих ШІ, до складних стратегій атак. Цей метод виявився особливо ефективним у боротьбі зі згенерованими штучним інтелектом фішинговими листами, які намагаються обійти наявні механізми виявлення.

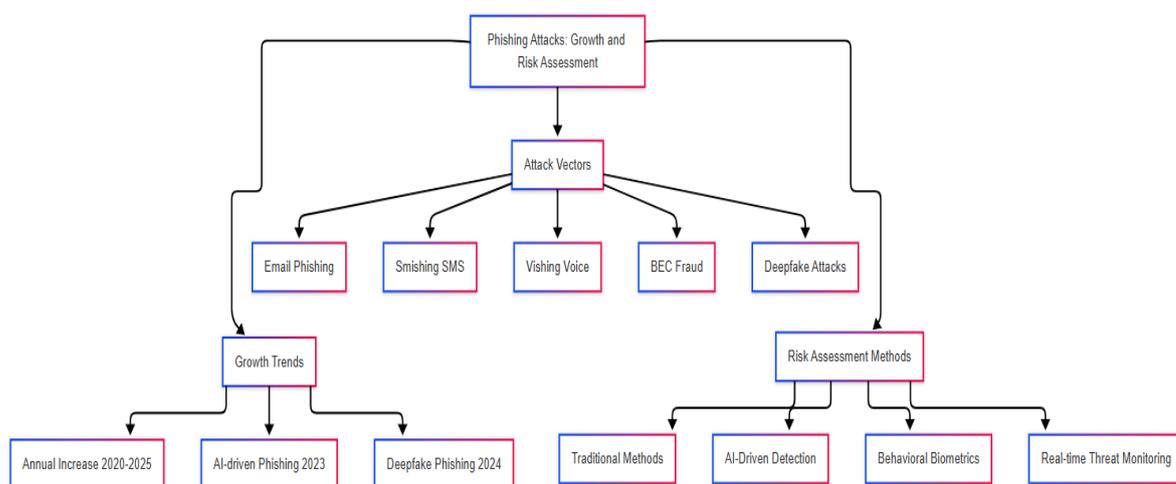


Рис. 1. Зростання фішингових атак та методи оцінки ризиків

Ключовим викликом в оцінці фішингових ризиків є баланс між мінімізацією хибних спрацьовувань і забезпеченням високого рівня виявлення. Хоча моделі на основі штучного інтелекту підвищують точність, надто агресивна фільтрація може призвести до того, що легітимні електронні листи будуть позначені як спроба фішингу, що порушить бізнес-операції. Для вирішення цієї проблеми організаціям необхідно вдосконалити свої алгоритми виявлення фішингу, включивши в них контекстний аналіз і оцінку репутації домену.

Ще одним важливим компонентом оцінки фішингових ризиків є використання технологій обману. Для ідентифікації зловмисників і відстеження їхньої інфраструктури використовуються токени - фальшиві облікові дані, вбудовані в фішингові поштові пастки. Такий проактивний підхід дозволяє командам безпеки отримати уявлення про методології фішингу та завчасно заблокувати шкідливі домени до того, як вони будуть використані у масштабних атаках.

Верифікація електронної пошти на основі блокчейну була запропонована як довгострокове рішення для боротьби з фішингом. Використовуючи децентралізовану перевірку ідентичності, блокчейн може забезпечити незмінний запис автентичності електронної пошти, зменшуючи ризик підміни доменів та атак під чужими іменами. Хоча ця технологія все ще перебуває на ранніх стадіях розвитку, пілотні впровадження показали багатообіцяючі результати в підвищенні стійкості до фішингу.

Оскільки фішингові атаки продовжують розвиватися, методології оцінки ризиків повинні відповідно адаптуватися. Інтеграція аналітики на основі штучного інтелекту, поведінкової біометрії та розвідки загроз у реальному часі підвищує точність виявлення та швидкість реагування. Використовуючи ці передові методи, організації можуть зменшити зростаючий ризик фішингових атак і зміцнити загальну систему кібербезпеки.

## Література

1. Brezeanu G., Archip A., Artene C.-G. Phish fighter: self updating machine learning shield against phishing kits based on HTML code analysis. *IEEE access*. 2025. P. 1. URL: <https://doi.org/10.1109/access.2025.3525998>
2. Liesnaia Y., Malakhov S. The analysis of development, typical objectives and mechanisms of phishing attacks. *Computer science and cybersecurity*. 2023. No. 1. P. 6–27. URL: <https://doi.org/10.26565/2519-2310-2023-1-01>
3. A comprehensive review of phishing attacks techniques, types and solutions / A. S. Mustafa et al. *Journal of hacking techniques, digital crime prevention and computer virology*. 2024. Vol. 1, no. 1. P. 15–24. URL: <https://doi.org/10.46610/johtdcpcv.2024.v01i01.002>
4. Phishing attacks: a recent comprehensive study and a new anatomy / Z. Alkhalil et al. *Frontiers in computer science*. 2021. Vol. 3. URL: <https://doi.org/10.3389/fcomp.2021.563060>

## AI-ПРОТИДІЯ ФІШИНГОВИМ АТАКАМ: РОЗПІЗНАВАННЯ ЗАГРОЗ У РЕАЛЬНОМУ ЧАСІ

**Святська Н. А., Тищенко В. С., Примаченко Д. В.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Алгоритми машинного навчання слугують основою для виявлення фішингу на основі штучного інтелекту, використовуючи великі масиви даних для виявлення шаблонів і аномалій, що вказують на фішингові атаки. Традиційні методи, засновані на правилах, часто не здатні виявити нові тактики фішингу, що робить ШІ більш адаптивним рішенням. Моделі керованого навчання, такі як дерева рішень, випадкові ліси та машини опорних векторів (SVM), класифікують електронні листи та URL-адреси на основі заздалегідь

визначених ознак, підвищуючи точність виявлення фішингу. Методи глибокого навчання, включаючи згорткові нейронні мережі (CNN) і рекурентні нейронні мережі (RNN), ще більше покращують виявлення, виявляючи складні патерни в текстових і візуальних даних [1].

Методи обробки природної мови (NLP) аналізують текстовий контент для виявлення спроб фішингу, розрізняючи підозрілі мовні патерни, сигнали терміновості та аномальні запити. Попередньо навчені моделі, такі як BERT (Bidirectional Encoder Representations from Transformers), аналізують електронну пошту та контекст повідомлень, виявляючи шахрайські повідомлення з високою точністю. Аналіз настроїв, підгалузь NLP, виявляє емоційно забарвлену мову, поширену у фішингових повідомленнях, наприклад, терміновість або погрози, тим самим допомагаючи класифікувати в реальному часі.

Можливості виявлення загроз у режимі реального часу дозволяють негайно реагувати на спроби фішингу ще до того, як вони потраплять до кінцевих користувачів. Системи штучного інтелекту постійно відстежують вхідні електронні листи, веб-сайти та мережевий трафік, миттєво блокуючи підозрілі дії. Наприклад, фільтри Google на основі машинного навчання щодня сканують мільярди електронних листів, виявляючи фішингові листи за вмістом, метаданими та аналізом поведінки відправника. Аналогічно, Microsoft Office 365 інтегрує методи автентифікації доменів на основі штучного інтелекту, такі як SPF і DKIM, для виявлення підроблених електронних листів.

Аналіз зображень і URL-адрес ще більше покращує виявлення фішингу, оцінюючи вбудовані посилання та графічний вміст. Системи на основі штучного інтелекту сканують URL-адреси за відомими базами даних фішингу, виявляючи оманливі візуальні елементи, що імітують легальні бренди. Моделі глибокого навчання аналізують структуру веб-сайтів і макет сторінок, виявляючи невідповідності, що вказують на фішингові сайти. Наприклад, Vade Secure використовує штучний інтелект для порівняння URL-адрес і вмісту веб-

сайтів з базами даних про загрози, блокуючи шкідливі домени в режимі реального часу [2].

Поведінковий аналіз є невід'ємною частиною виявлення фішингу, оскільки ШІ відстежує взаємодію користувачів і відхилення від звичайних шаблонів активності. Незвичайні спроби входу в систему, нерегулярна поведінка електронної пошти та нетипові запити на транзакції позначаються як потенційні спроби фішингу. Платформа безпеки Cisco на основі штучного інтелекту відстежує поведінку електронної пошти та мережі, попереджаючи користувачів про аномалії. Автоматизована поведінкова біометрія, включаючи динаміку натискання клавіш і аналіз рухів миші, забезпечує додаткові рівні безпеки, виявляючи відхилення від стандартних шаблонів взаємодії користувача.

Гібридні підходи ШІ поєднують кілька методів виявлення, інтегруючи фільтри на основі правил з моделями машинного навчання для підвищення точності. Методи ансамблевого навчання, такі як boosting і bagging, покращують показники виявлення, об'єднуючи результати з декількох класифікаторів. Дослідження показали, що гібридні моделі перевершують одноалгоритмічні підходи до виявлення фішингу, зменшуючи кількість помилкових спрацьовувань, зберігаючи при цьому високі бали відгуку [3].

Системи виявлення фішингу зі штучним інтелектом працюють на основі багаторівневої архітектури, що включає збір даних, вилучення ознак, навчання моделей і модулі класифікації в реальному часі. На етапі збору даних збираються електронні листи, URL-адреси та мережеві журнали, які потім обробляються за відповідними ознаками, такими як вік домену, структура URL-адреси та метадані електронного листа. Моделі штучного інтелекту аналізують отримані дані, щоб класифікувати спроби фішингу, запускаючи автоматичні реакції, такі як блокування доступу, відправлення листів у карантин або сповіщення адміністраторів.



Рис. 1 Архітектура системи виявлення фішингу зі штучним інтелектом

Виявлення фішингу в режимі реального часу ґрунтується на потоковій аналітиці, що забезпечує безперервний моніторинг і миттєву класифікацію. Моделі глибокого навчання аналізують заголовки електронних листів, вміст і метадані вкладень у режимі реального часу, швидко розрізняючи легітимні та шахрайські повідомлення. QRadar від IBM використовує аналіз мережі на основі штучного інтелекту для виявлення аномалій, що вказують на спроби фішингу, інтегруючись із системами управління інформацією та подіями безпеки (SIEM) для покращення розвідки загроз.

Механізми адаптивного навчання дозволяють системам штучного інтелекту розвиватися разом з новими методами фішингу. Моделі виявлення фішингу постійно навчаються на нових даних розвідки загроз, удосконалюючи свою здатність виявляти фішингові кампанії «нульового дня». Платформи розвідки загроз на основі штучного інтелекту агрегують дані з досліджень кібербезпеки, моніторингу темного інтернету та звітів користувачів, динамічно оновлюючи параметри виявлення фішингу [4].

Виявлення фішингу за допомогою штучного інтелекту продемонструвало вищу точність порівняно з традиційними методами. Емпіричні дослідження показують, що моделі машинного навчання досягають понад 95% точності в класифікації фішингу, а методи глибокого навчання перевершують традиційні евристичні фільтри. Незважаючи на свою ефективність, системи, керовані штучним інтелектом, стикаються з проблемами, в тому числі з атаками, коли кіберзлочинці маніпулюють моделями штучного інтелекту, щоб уникнути виявлення. Методи навчання в умовах суперництва підвищують стійкість, піддаючи AI-системи оманливим зразкам фішингу, підвищуючи надійність проти загроз, що еволюціонують.

Виявлення фішингу з використанням ШІ застосовується в різних сферах, включаючи корпоративну безпеку, фінансові послуги та мобільні додатки. У корпоративному середовищі інтегровані з AI рішення для захисту електронної пошти захищають організації від фішингових атак, запобігаючи несанкціонованому доступу до даних. Фінансові установи використовують AI для моніторингу шахрайських транзакцій і фішингових атак на клієнтів. Мобільні системи виявлення фішингу на основі штучного інтелекту захищають користувачів від смс-фішингу (SMS-фішингу) та загроз, що походять від шкідливих додатків.

Моделі виявлення фішингу на основі штучного інтелекту отримують вигоду від масштабних навчальних наборів даних, що дає змогу чудово узагальнювати різноманітні тактики фішингу. Загальнодоступні набори даних, такі як PhishTank і Kaggle Phishing Websites Dataset, сприяють навчанню моделей, покращуючи ефективність класифікації фішингу. Однак дисбаланс наборів даних створює проблеми, оскільки легітимних листів часто більше, ніж зразків фішингу. Надмірна вибірка, синтетична генерація даних і методи виявлення аномалій зменшують упередженість набору даних, підвищуючи ефективність моделі.

Інтеграція виявлення фішингу на основі ШІ з більш широкими системами кібербезпеки посилює загальний рівень безпеки. Системи зі штучним

інтелектом доповнюють традиційні заходи безпеки, такі як багатофакторна автентифікація (MFA) і захист кінцевих точок, щоб забезпечити комплексний захист від фішингових загроз. Автоматизовані тренінги з підвищення обізнаності про фішинг використовують ШІ для імітації фішингових атак, навчаючи користувачів розпізнавати шахрайські повідомлення і знижуючи вразливість до тактик соціальної інженерії.

Роль штучного інтелекту у виявленні фішингу виходить за межі захисту електронної пошти, охоплюючи аналіз загроз на веб-сайтах і в соціальних мережах. Розширення для браузерів на основі штучного інтелекту аналізують веб-сторінки в режимі реального часу, запобігаючи доступу користувачів до шкідливих сайтів. Інструменти моніторингу соціальних мереж використовують ШІ для виявлення фішингових кампаній, що поширюються через соціальні платформи, блокування шкідливих посилань і шахрайської реклами.

Майбутні досягнення в галузі виявлення фішингу на основі штучного інтелекту зосереджені на покращенні інтерпретованості моделі, зменшенні кількості хибних спрацьовувань та покращенні масштабованості виявлення фішингу. Методи пояснюваного штучного інтелекту (Explainable AI, XAI) мають на меті забезпечити прозору класифікацію фішингових атак, підвищуючи довіру до рішень для безпеки на основі штучного інтелекту. Масштабовані архітектури ШІ забезпечують ефективне виявлення фішингу у великих корпоративних середовищах, зменшуючи загрози в масштабі.

Системи виявлення фішингу на основі штучного інтелекту представляють собою трансформаційний підхід до протидії фішинговим загрозам, інтегруючи машинне навчання, глибоке навчання та аналітику в реальному часі для комплексного захисту. Постійно розвиваючись і адаптуючись до нових векторів атак, ШІ підвищує стійкість кібербезпеки, знижуючи ризики, які несуть витончені фішингові кампанії.

## Література

1. AI-driven threat intelligence for real-time cybersecurity: frameworks, tools, and future directions . Kelvin Ovabor et al. *Open access research journal of science and technology*. 2024. Vol. 12, no. 2. P. 040–048.  
URL: <https://doi.org/10.53022/oarjst.2024.12.2.0135>
2. Automated AI system for online phishing detection and mitigation / D. Raj et al. *2024 international conference on electrical electronics and computing technologies (ICEECT)*, Greater Noida, India, 29–31 August 2024. 2024. P. 1–6.  
URL: <https://doi.org/10.1109/iceect61758.2024.10739139>
3. Ramkumar G. Elevated learning based secured phishing website identification methodology using artificial intelligence assistance. *2024 5th international conference on electronics and sustainable communication systems (ICESC)*, Coimbatore, India, 7–9 August 2024. 2024. P. 1543–1551.  
URL: <https://doi.org/10.1109/icesc60852.2024.10689980>
4. Sarika Nitin Zaware. AI-Based phishing detection and automated response: a multi-channel security framework for modern communication platforms. *Panamerican mathematical journal*. 2024. Vol. 35, no. 1s. P. 250–263.  
URL: <https://doi.org/10.52783/pmj.v35.i1s.2312>

## АВТОМАТИЗАЦІЯ ПРОЦЕСІВ МОНІТОРИНГУ ТА РЕАГУВАННЯ: СУЧАСНІ ІНСТРУМЕНТИ ТА ПРАКТИКИ

**Романов О. А.**

Державний університет інформаційно-комунікаційних технологій  
м Київ, Україна

У цифровому середовищі підприємства стикаються з постійно зростаючими кіберзагрозами, які стають дедалі складнішими й витонченішими. Ручне управління безпекою вже не є ефективним, оскільки обсяг подій та

потенційних атак зростає експоненційно. Автоматизація процесів моніторингу та реагування дозволяє значно зменшити навантаження на фахівців з кібербезпеки, підвищити швидкість реагування на інциденти та знизити ризики для критичних систем компанії.

У цій статті буде розглянуто ключові виклики, пов'язані з моніторингом та реагуванням, сучасні інструменти автоматизації, а також організаційні аспекти їхнього впровадження для підвищення кіберстійкості підприємства.

У сучасному цифровому середовищі підприємства стикаються з низкою викликів у сфері моніторингу та реагування на кіберзагрози. Один із головних викликів — постійне зростання обсягу даних та подій безпеки. Сучасні організації використовують численні системи та сервіси, кожен із яких генерує значну кількість логів та сповіщень. Це ускладнює своєчасне виявлення реальних загроз серед великого обсягу інформації.

Обмеженість людських ресурсів у командах безпеки є ще одним суттєвим викликом. Навіть із наявністю кваліфікованих фахівців, обробка великої кількості подій безпеки вручну стає непосильним завданням. Це може призвести до затримок у реагуванні на інциденти та підвищення ризику успішних атак.

Крім того, кіберзлочинці постійно вдосконалюють свої методи, використовуючи нові техніки та інструменти для обходу традиційних засобів захисту. Це вимагає від підприємств постійного оновлення своїх стратегій безпеки та впровадження сучасних рішень для ефективного моніторингу та реагування на загрози.

Відсутність інтеграції між різними системами безпеки також створює додаткові труднощі. Різні інструменти можуть працювати ізольовано один від одного, що ускладнює отримання цілісної картини стану безпеки та уповільнює процес реагування на інциденти.

Для подолання цих викликів підприємствам необхідно впроваджувати сучасні інструменти автоматизації моніторингу та реагування, а також

розробляти ефективні стратегії управління кібербезпекою, враховуючи як технічні, так і організаційні аспекти.

У сучасному кібербезпековому ландшафті підприємства стикаються з численними загрозами, що вимагають ефективних рішень для моніторингу та реагування. Впровадження таких інструментів, як SIEM, SOAR та EDR/XDR, дозволяє автоматизувати процеси безпеки та підвищити загальну стійкість організації до кіберзагроз.

- SIEM-системи забезпечують централізований збір, зберігання та аналіз логів з різних джерел в IT-інфраструктурі. Вони дозволяють виявляти аномалії та потенційні загрози шляхом кореляції подій, що сприяє своєчасному реагуванню на інциденти. [1]

- SOAR-рішення орієнтовані на автоматизацію та оркестрацію процесів безпеки. Вони інтегрують різні інструменти та платформи, дозволяючи автоматично реагувати на інциденти за заздалегідь визначеними сценаріями. Це знижує навантаження на команди безпеки та підвищує ефективність реагування. [2]

- EDR-системи фокусуються на моніторингу та аналізі активності на кінцевих точках, таких як робочі станції та сервери, для виявлення та реагування на загрози. XDR розширює цей підхід, об'єднуючи дані з різних джерел, включаючи мережеві та хмарні сервіси, забезпечуючи більш глибоке розуміння та контекст для виявлення загроз. [3]

Впровадження автоматизованих рішень вимагає ретельного планування та організаційних змін. Перш за все, необхідно створити ефективну структуру команди реагування на інциденти, яка може включати Центр операцій безпеки (SOC) або Команду реагування на комп'ютерні інциденти (CSIRT). Чітке визначення ролей та відповідальностей забезпечить оперативність та ефективність реагування.

Розробка внутрішніх політик та процедур безпеки є критично важливою. Вони повинні визначати порядок дій у разі інцидентів, правила доступу до інформаційних ресурсів та інші аспекти, пов'язані з безпекою. Відповідність

міжнародним стандартам, таким як ISO 27001 та IEC 62443, сприяє підвищенню рівня кібербезпеки та довіри з боку партнерів і клієнтів. [4]

Інтеграція автоматизованих систем з існуючими процесами вимагає навчання персоналу та адаптації робочих процедур. Важливо забезпечити безперервний моніторинг та вдосконалення впроваджених рішень, враховуючи змінюваний характер кіберзагроз.

Таким чином, поєднання сучасних інструментів автоматизації з належною організаційною структурою та політиками безпеки дозволяє підприємствам ефективно протидіяти кіберзагрозам та забезпечувати стійкість своїх інформаційних систем.

Впровадження автоматизованих рішень у процеси моніторингу та реагування на кіберзагрози приносить підприємствам низку значних переваг. Однією з ключових є прискорення виявлення та реагування на загрози. Завдяки автоматизації можна забезпечити майже миттєву реакцію на події безпеки, зводячи до мінімуму можливий збиток.

Автоматизація також сприяє оптимізації роботи команди безпеки. Завдання, які раніше потребували значних людських ресурсів, виконуються набагато ефективніше за допомогою автоматизованих систем. Це дозволяє фахівцям зосередитися на більш складних та критичних аспектах безпеки, підвищуючи загальну ефективність команди.

Крім того, автоматизовані системи забезпечують раннє виявлення загроз. Зупинення кіберзагроз ще до того, як станеться порушення безпеки, є важливим способом суттєво зменшити вплив інциденту. Завдяки сучасним інструментам виявлення загроз і реагування на них, а також спеціалізованій команді, центри безпеки збільшують шанси виявлення загроз на ранній стадії, коли їх буде легше усунути.

Автоматизація також допомагає забезпечити відповідність нормативним вимогам. У багатьох країнах і регіонах приймаються суворі закони про конфіденційність, які вимагають від організацій вжиття надійних заходів із захисту даних і запровадження деталізованого процесу реагування на інциденти

з безпекою. Програма виявлення загроз і реагування на них допомагає організаціям виконувати вимоги цих законів. [5]

Загалом, впровадження автоматизованих рішень підвищує загальну кіберстійкість компанії, зменшуючи ризики та забезпечуючи більш надійний захист інформаційних ресурсів.

Автоматизація процесів моніторингу та реагування є невід'ємною частиною сучасної стратегії забезпечення кіберстійкості підприємства. Використання сучасних інструментів, таких як SOAR-рішення та технології штучного інтелекту, дозволяє підвищити ефективність кіберзахисту та зменшити час реагування на інциденти. Однак, для досягнення повної кіберстійкості необхідно також приділяти увагу організаційним аспектам, таким як розробка внутрішніх політик і процедур безпеки, управління кіберризиками та організація команд реагування на інциденти.

## Література

1. Pham T. SIEM vs XDR vs SOAR vs SOC vs EDR vs MDR | Blumira. SIEM + Endpoint Visibility + XDR For SMB | Blumira. URL: <https://www.blumira.com/blog/siem-soc-soar-xdr-defined>.

2. What is SOAR vs. SIEM vs. XDR?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-soar-vs-siem-vs-xdr>.

3. Understanding the Difference Between EDR, SIEM, SOAR, and XDR. SentinelOne. URL: <https://www.sentinelone.com/cybersecurity-101/xdr/understanding-the-difference-between-edr-siem-soar-and-xdr/> (date of access: 13.02.2025).

4. Як технології змінюють сферу кібербезпеки - UAGeneral. Домашня сторінка - UAGeneral. URL: <https://uageneral.net/blog/it/iak-tekhnologii-zminiuiut-sferu-kiberbezpeki/>.

5. Що таке виявлення загроз і реагування на них? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons.

URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-threat-detection-response-tdr>.

## РОЗВІДКА НА ОСНОВІ ВІДКРИТИХ ДЖЕРЕЛ СУСПІЛЬСТВО ТА КІБЕРГІГІЄНА

**Майсузенко Р. В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Згідно визначенню корпорації Microsoft: “Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи й мережу від кібератак”.

Кібербезпека охоплює завелику площину соціальних, державних та національних інтересів, аби спростувати це поняття. Кібербезпека це про запобігання та протидію, розвідку та роботу з людьми, кібератаки та психологічні операції. Наприклад, в контексті Етичного Хакінгу ми завжди ділимо цю галузь на дві команди, тобто, Red Team ( команда нападу ) та Blue Team ( команда захисту ), проте на практиці таке розподілення відноситься не тільки до напрямку Етичного Хакінгу, але й інших, більш важливих напрямів кібербезпеки, наприклад, OSINT, який також є поняттям тільки загальноописуваного характеру галузі пошуку інформації з відкритих джерел, я поділив його на вузькоспеціалізовані категорії:

- SOCMINT - розвідка соціальних мереж.
- GEOINT - збір та аналіз географічної інформації з відкритих джерел.
- HUMINT - збір інформації через міжособистісні взаємодії.

Об'єктивно, вище перелічені елементи мають багато точок перетину, проте є кардинально різними стосовно цілей, використання підходів та принципів роботи.

Наприклад, в залежності від поставленої цілі, розвідка соціальних мереж може включати в себе аналіз профілів користувачів, публікацій та коментарів, фотографій та відео, зв'язків між користувачами та геолокаційних даних [1].

В свою ж чергу GEOINT – є розвідкою на основі просторових даних, яка використовує географічну інформацію для аналізу та розуміння різних явищ і подій, наприклад: супутникові знімки, аерофотозйомка ( знімки з літаків, або дронів ), картографічні дані, геолокаційні дані, дані про погоду та клімат.

HUMINT - збір розвідувальної інформації шляхом міжособистісного спілкування. Інформація отримується безпосередньо від людей. Наприклад, міжособистісне спілкування, допити, вербування. Включає в себе елементи соціальної інженерії, може поєднувати в собі технічні завдання, наприклад, встановлення геолокації, або отримання несанкціонованого доступу до соціальних мереж шляхом використання ПЗ, використання прихованих мікрофонів або відокамер.

Сьогодні завдяки OSINT, його напрямкам та поєднанню цих спеціалізацій, ми маємо можливість знаходити та ідентифікувати самих військових країни агресора та їхнє розташування, наслідком чого не рідко є їхнє знищення нашими Збройними Силами, завдяки цьому ми можемо ідентифікувати осіб, які сприяли, або сприяють викраденню дітей з території України на територію країни агресора, проводити контрдиверсійні заходи і т.д.

Підсумовуючи вище описане, я можу зробити висновок, що нам необхідно бути більш далекоглядними та виходити за рамки загальноприйнятих норм в галузі кібербезпеки, оскільки шахрайство та кіберзагрози не завжди можливо передбачити. Дійсно, можна використовувати певні заходи безпеки, наприклад впроваджуючи їх у культуру користування телефонами, комп'ютерами планшетами, або взагалом інтернетом, проте через стрімкий розвиток технологій, нові вразливості або тенденції, які постійно змінюються,

передбачити кіберзагрозу, або шахрайство для людини може бути важко, або неможливо.

Не менш важливою складовою у сфері кібербезпеки є поширення правдивої та об'єктивної інформації на національному рівні.

"Я думаю, що роль кібербезпеки трохи перебільшена. Про неї багато говорять, але по факту назвати якісь реальні кейси кіберзагроз мало хто може.", - розповів міністр цифрової трансформації Федоров 2019 р.

Об'єктивно, сьогодні, коли в Україні кожного дня стається багато випадків шахрайства, коли сім'ям загиблих військових дзвонять по телефону, або пишуть в месенджери, та пропонують забрати тіло за декілька тисяч доларів – це шахрайство, коли надсилають посилання в месенджери, а люди масово по ним переходять, це і є кіберзагроза, оскільки внаслідок цих дій, від їхнього імені може здійснюватися вплив на контакти цих людей, і вони під приводом довіри можуть ділитися інформацією, переводити гроші, переходити на посилання, завантажувати шкідливе ПЗ і т.д [2].

Про те, що кіберзагроз мало, немає, чи вони не актуальні, я вважаю, про таке говорити недопустимо міністру, тим паче, за 6 пройдених років, після цього коментаря, принцип комунікації з людьми не змінився, проте, тренди кіберзагроз змінилися, шахрайство набуло нових методів, про які суспільство зобов'язане знати і могти їм протидіяти.

10 січня 2025 року Опендатабот – українська компанія, що надає доступ до державних даних з основних публічних реєстрів для громадян та бізнесу, опублікував аналітику по шахрайствам в Україні. А саме про майже 65 тисяч кримінальних проваджень (178 справ на день) за статтю 190 "Шахрайство", які було відкрито за 2024 рік. Це на 21% менше ніж у 2023 році, проте майже втричі більше ніж до війни. Звичайно не всі ці справи про телефонне шахрайство, але саме це направлення здобуло неабияке поширення.

Суспільство має знати як відбувається шахрайство не на власному прикладі, а через правильні державні ініціативи, освітніх проектів самих по собі мало, людей потрібно ще зацікавити. Необхідне залучення людей до

самоосвітнього процесу, вчити завдяки правильним та грамотно вибудованим методам та стратегії комунікації з суспільством у найбільш впливових засобах зв'язку та у побутових сферах життєдіяльності.

Кібербезпека без активних заходів поширення інформації, тобто інформаційних кампаній, не зможе привернути увагу всіх громадян України, необхідно поширювати свій вплив не тільки через телевізор, але й через соціальні мережі, залучаючи до цього партнерів своїх компаній, або організацій.

Кібергігієна, що є сукупністю практик та звичок, які допомагають підтримувати безпеку цифрових пристроїв, інформації в інтернеті та людей. Кібергігієна є спільним завданням держави та кожного громадянина, оскільки саме від дотримання самої ж кібергігієни залежить буде наш цифровий простір безпечним чи ні. Отже, окрім державних ініціатив та роботи державних служб, або урядовців, кожна людина повинна відповідально відноситись до дотримання правил кібергігієни, формувати правильні звички, застерігати інших людей, допомагати їм та поширювати інформацію про правила кібергігієни. Безумовно, дотримання правил кібергігієни може бути незручним, комусь не подобатись, проте завтра, від цього може залежати чиясь фінансове становище, або життя.

10 січня 2025 року Опендатабот – українська компанія, що надає доступ до державних даних з основних публічних реєстрів для громадян та бізнесу, опублікував аналітику по шахрайствам в Україні. А саме про майже 65 тисяч кримінальних проваджень (178 справ на день) за статтю 190 “Шахрайство”, які було відкрито за 2024 рік, це побило 12 річний рекорд. Це на 21% менше ніж у 2023 році, проте майже втричі більше ніж до війни. Звичайно не всі ці справи про телефонне шахрайство, але саме це направлення здобуло неабияке поширення.

## Література

1. Інтерв'ю міністра цифрової трансформації Михайла Федорова [https://lb.ua/tech/2019/11/29/443542\\_rol\\_kiberbezopasnosti\\_nemnogo.html](https://lb.ua/tech/2019/11/29/443542_rol_kiberbezopasnosti_nemnogo.html)

2. Оpendatabot: кількість справ про шахрайство побила 12 річний рекорд <https://opendatabot.ua/analytics/fraud-2024-4>

## **ВИКОРИСТАННЯ SIEM-СИСТЕМ НА БАЗІ ELASTIC STACK ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ТА УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ**

**Никитенко Є. Я.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасних умовах, коли кіберзагрози стають все більш складними та динамічними, ефективне управління інформаційною безпекою потребує використання інноваційних інструментів. SIEM-системи (Security Information and Event Management) на базі Elastic Stack пропонують гнучкість, масштабованість та потужні аналітичні можливості для моніторингу, виявлення та реагування на кіберінциденти.

Ключові аспекти впровадження SIEM на базі Elastic Stack, зокрема:

1. Моніторинг та аналіз подій безпеки: Використання Elasticsearch для збору та аналізу великих обсягів даних із різних джерел, що дозволяє оперативно виявляти аномалії та потенційні загрози [1].

2. Автоматизація реагування: Інтеграція з інструментами оркестрації (наприклад, SOAR) для автоматизації процесів реагування на інциденти, що зменшує час відповіді та знижує ризики для бізнесу.

3. Масштабованість та гнучкість: Переваги Elastic Stack у роботі з великими обсягами даних та можливість адаптації до потреб конкретного підприємства [2].

4. Зменшення ризиків: Використання SIEM для проактивного управління ризиками шляхом аналізу шаблонів атак, вразливостей та індикаторів компрометації (IoC).

5. Інтеграція з іншими системами безпеки: Можливість інтеграції Elastic Stack з іншими засобами кібербезпеки для створення єдиної платформи управління інформаційною безпекою [3].

SIEM-системи на базі Elastic Stack є потужним інструментом для забезпечення кіберстійкості підприємств, дозволяючи ефективно управляти ризиками, забезпечувати безперервність бізнесу та протидіяти сучасним кіберзагрозам. Впровадження таких рішень сприяє формуванню культури кібербезпеки та підвищує загальний рівень захищеності критичної інфраструктури.

### **Література**

1. Overview of SIEM technology. URL: <https://www.coursera.org/learn/detection-and-response/supplement/aqoqn/overview-of-siem-technology>
2. Elastic Stack. URL: <https://discuss.elastic.co/c/elastic-stack/81>
3. ELK, SIEM. URL: <https://habr.com/ru/articles/515576/>

## **МЕТОДИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ В КІБЕРБЕЗПЕЦІ. ІНТЕГРАЦІЯ ЦИХ МЕТОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ**

**Рубан Ю. Р.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

На сьогоднішній день організації змушені впроваджувати найсучасніші технології для запобігання кібератакам і швидкого реагування на них. У даній доповіді розглядаються підходи до забезпечення високого рівня захисту мереж

і інформаційних систем, що ґрунтуються на постійному моніторингу мережевої активності та своєчасному виявленні відхилень, які можуть свідчити про спроби несанкціонованого доступу.

На першому етапі забезпечення безпеки важливу роль відіграють системи виявлення та запобігання вторгненням. Такі програми, як Snort та Suricata, є класичними прикладами IDS/IPS-рішень, що, використовуючи технологію глибокого аналізу пакетів (Deep Packet Inspection), ретельно аналізують мережевий трафік. Завдяки цьому вони здатні виявити навіть найменші відхилення від звичної роботи мережі, що дозволяє експертам оперативно реагувати на потенційні загрози.

Для більш комплексного аналізу та кореляції інформації, що надходить з різних джерел, активно застосовуються SIEM-системи. Наприклад, Splunk, IBM QRadar та AlienVault USM допомагають централізовано збирати логи з серверів, мережевого обладнання та кінцевих пристроїв. Завдяки цим системам можна не лише виявити ізольовані інциденти, але й побудувати єдину картину кібербезпеки підприємства, що дозволяє ідентифікувати складні атаки, коли низка незначних подій в сукупності свідчать про серйозну загрозу. Згідно з вимогами законодавства України щодо кіберзахисту об'єктів критичної інфраструктури, впровадження систем моніторингу безпеки та журналювання подій є обов'язковим елементом системи захисту.

У контексті операційної безпеки важливою складовою є моніторинг стану операційних систем та серверів. Програми, як-от CrowdStrike Falcon або Carbon Black, дозволяють відстежувати активність кінцевих пристроїв, аналізувати підозрілу поведінку користувачів та швидко виявляти зловмисні дії, навіть якщо атака має внутрішнє походження. Крім того, інтегровані системи автоматизованого сканування вразливостей, зокрема Nessus та OpenVAS, регулярно перевіряють мережеву інфраструктуру на наявність слабких місць.

Перевагою сучасних систем є алгоритми машинного навчання, що інтегровані в SIEM-системи. Вони дозволяють класифікувати події за допомогою нейронних мереж або алгоритмів Random Forest, що забезпечує

більш точне розпізнавання аномалій. Це допомагає знизити кількість помилкових сповіщень і спрямувати увагу фахівців на реальні загрози.

Реагування на інциденти розпочинається з швидкого виявлення підозрілої активності завдяки інтегрованим системам сповіщення. Негайно після визначення загрози відповідні служби проводять аналіз отриманих даних, використовуючи як автоматизовані методи, так і експертну оцінку. Швидка ізоляція уражених сегментів мережі — наприклад, шляхом блокування конкретних IP-адрес або відключення підозрілих вузлів — дозволяє зменшити розповсюдження загрози [1].

Для остаточного усунення наслідків інциденту проводиться оновлення мережесих політик і впровадження патчів безпеки, що дозволяє закріпити результати реагування та запобігти повторенню подібних ситуацій. Для кращого розуміння цього процесу рекомендую ознайомитися із схемою (рис.1) яка демонструє етапи реагування на кіберінциденти. Додаткову інформацію про стандартизований підхід до реагування можна знайти у NIST Special Publication 800-61 Revision 2 – "Computer Security Incident Handling Guide".



Рис.1. Блок-схема реагування на інциденти

Об'єднання зазначених рішень дозволяє створити єдину систему безпеки, в якій програмне забезпечення для моніторингу мережі, аналізу логів та роботи кінцевих пристроїв взаємодіє задля забезпечення максимального захисту.

Таким чином, застосування цих інструментів від Snort та Suricata для аналізу мережевого трафіку до Splunk і IBM QRadar для збирання та кореляції даних, а також CrowdStrike Falcon для моніторингу кінцевих точок, забезпечує комплексний захист підприємства. Ці заходи сприяють формуванню

стабільного та надійного середовища, де інформаційна безпека виступає одним із ключових чинників успішного функціонування організації.

Крім технічних рішень, невід'ємною складовою ефективної системи безпеки є навчання персоналу (рис.2). Регулярні тренінги з кібербезпеки допомагають співробітникам розпізнавати фішингові атаки, методи соціальної інженерії та інші загрози, що пов'язані з людським фактором. Проведення симуляцій кібератак, внутрішніх аудитів і розробка чітких політик безпеки сприяють формуванню культури, в якій кожен розуміє свою роль у захисті корпоративних даних. Практичні кейси демонструють, що інвестиції в навчання персоналу значно знижують ризик помилок. Закон України "Про основні засади забезпечення кібербезпеки України" визначає необхідність підготовки кадрів у сфері кібербезпеки та проведення відповідних навчань персоналу [2].

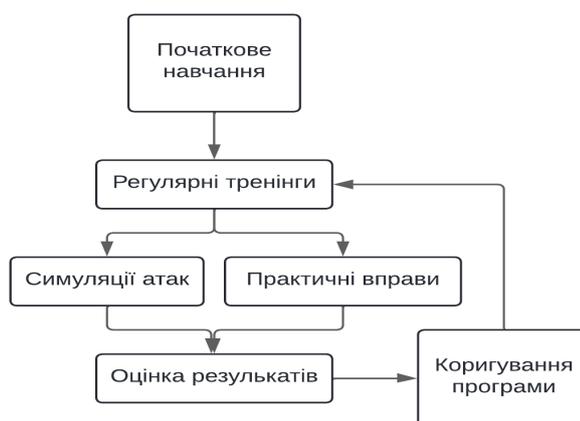


Рис. 2. Блок-схема навчання персоналу

Завдяки постійному вдосконаленню технологій та інтеграції новітніх програмних рішень, організації здатні ефективно протидіяти кібератакам, знижуючи як і фінансові, так і репутаційні ризики. Усі впроваджені заходи та системи відповідають вимогам Закону України "Про основні засади забезпечення кібербезпеки України" та створюють комплексну систему захисту інформації. Сучасна система безпеки – це не просто набір окремих засобів, а інтегрований комплекс, що дозволяє швидко реагувати на зміни в кіберсередовищі та гарантувати надійний захист інформаційних ресурсів.

## Література

1. NIST Special Publication 800-61 Revision 2 – "Computer Security Incident Handling Guide". URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
2. Закон України "Про основні засади забезпечення кібербезпеки". URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

## НЕЙРОМЕРЕЖЕВА ТЕХНОЛОГІЯ ЗАХИСТУ КАНАЛІВ УПРАВЛІННЯ В ГРУПІ БПЛА

**Савченко В. А., д.т.н., проф.**

Державний університет інформаційно-комунікаційних технологій,  
м. Київ, Україна

**Горбачова Я. С., Новікова І. В.**

Національний університет оборони України, м. Київ, Україна

Починаючи з 2022 року безпілотні літальні апарати (БПЛА) стали ключовим інструментом ведення бойових дій. Дрони перетворилися з іграшок на машини для виконання різноманітних бойових завдань, виконуючи їх як поодинці, так і узгоджено у складі груп [1].



*Рис. 1 Виконання завдань групою БПЛА*

Керуюча система БПЛА, окрім управління роботом, повинна забезпечувати узгодженість його дій з іншими членами групи. Така система управління повинна оптимізувати індивідуальну поведінку окремого робота, узгоджуючи її з поведінкою інших членів групи навіть в умовах відсутності зв'язку БПЛА з наземним пунктом управління.

Метою даного дослідження є розробка моделі управління групою автономних об'єктів, яка б забезпечувала можливість розпізнавання ситуацій на основі багатосарової нейронної архітектури, здатної навчатися на основі генетичних алгоритмів.

Система управління роботом будується на основі 2-шарової неповнозв'язної нейронної мережі прямого розповсюдження (рис. 2). Нейронна мережа має 16 входів та 4 виходи. Входи розбиті на 2 рівні групи  $S$  та  $V$ . Зв'язки у першому прихованому шарі обмежені з метою досягнення незалежної попередньої обробки вхідної інформації в групах входів  $S$  та  $V$ , та скорочення числа параметрів нейронної мережі, які навчаються [2].

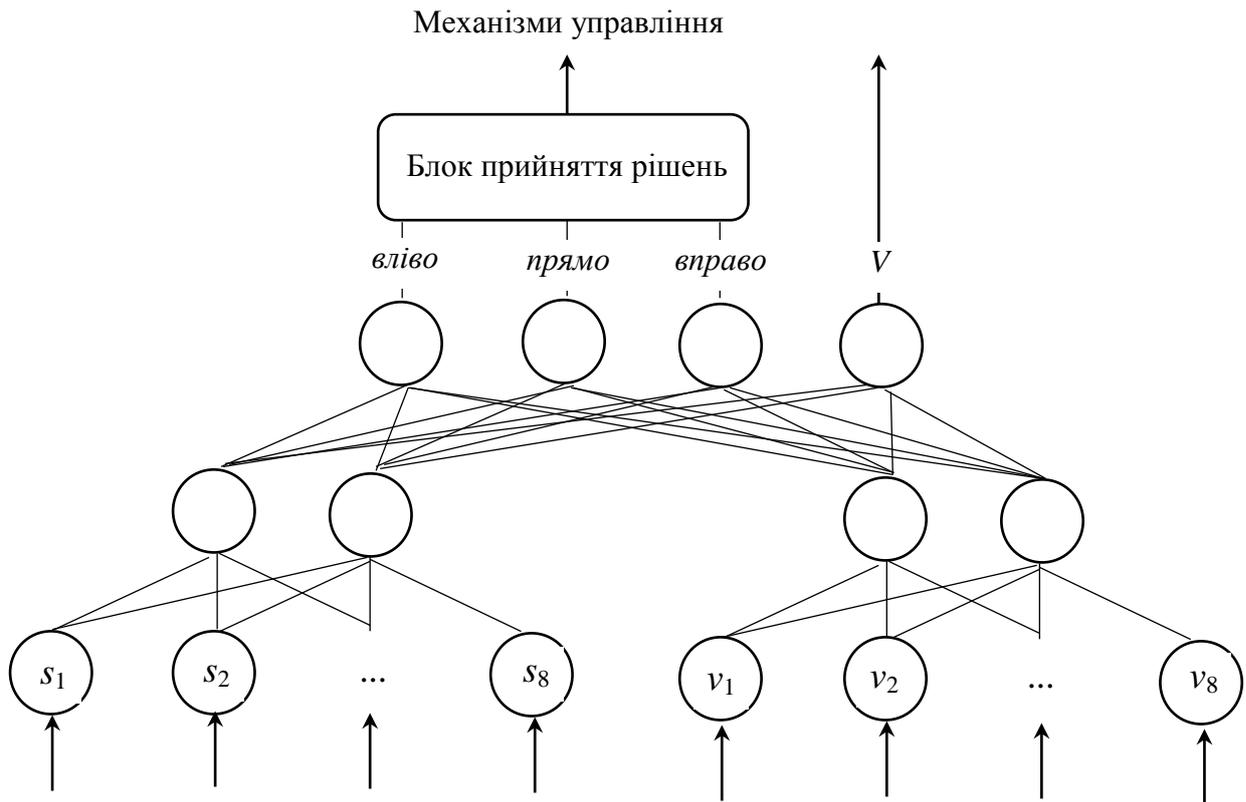


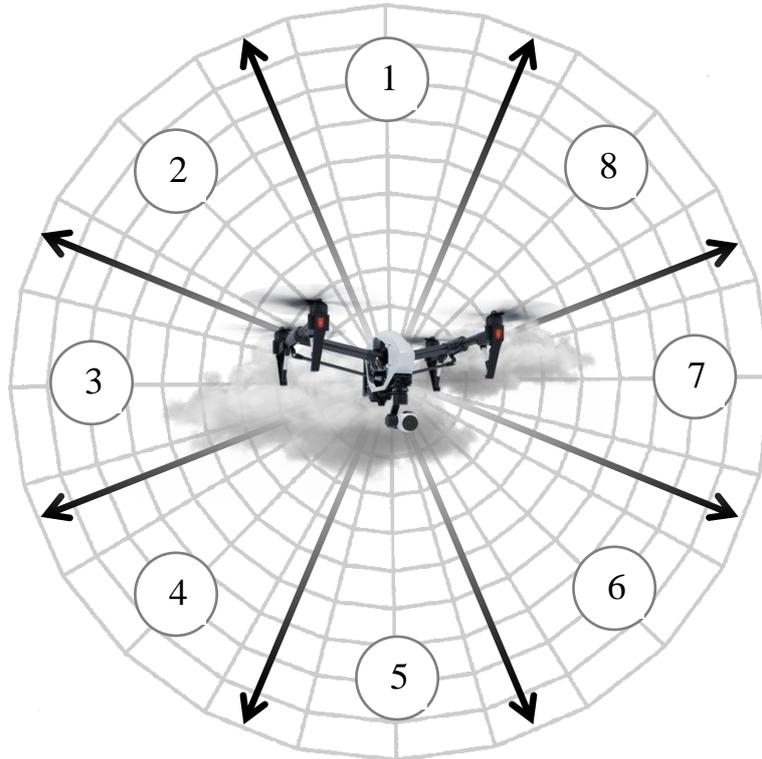
Рис. 2 Нейронна мережа системи управління БПЛА

Входи  $S_1-S_8$  приймають інформацію про розташування цілей. Інформація надходить до нейроконтролера як від сенсорів самого робота, так і від інших роботів каналом зв'язку. Входи  $V_1-V_8$  працюють як спрямовані приймачі комунікаційної інформації від інших роботів. Згідно зі схемою (рис. 3) простір навколо робота ділиться на 8 секторів, кожен з яких є входом нейромережі.

Величини, що подаються на вхід, визначаються формулами:  $S_i = \sum_j \frac{1}{r_{ij}^\alpha}$ ;

$V_i = \sum_j \frac{1}{(v_{ij} r_{ij})^\alpha}$ , де  $i$  – номер входу (сектора);  $r_{ij}$  – відстань до  $j$ -ї цілі чи до

робота, який надіслав комунікаційний сигнал з  $i$ -го сектора;  $\alpha \in [0;4]$  – параметр навчання (пріоритет близьких об'єктів над віддаленими);  $v_{ij}$  – інтенсивність прийнятого сигналу.



*Рис. 3 Сектори управління БПЛА*

Три виходи нейромережі визначають дії щодо переміщення робота: на кожному кроці блок управління випадковим чином обирає одну з 3-х дій з ймовірністю, яка пропорційна величинам на відповідних виходах нейромережі. Четвертий вихід визначає інтенсивність сигналу робота, який випромінюється для комунікації. Ця інтенсивність визначається у результаті навчання генетичним алгоритмом. Нейромережа робота сама обирає зміст повідомлення та правила реагування на повідомлення від інших роботів. Також, у такій нейромережі відсутній вихід, який ініціює дію щодо позначення цілі. Вважається, що дана дія виконується автоматично, у випадку, коли координати робота співпали з координатами цілі.

Навчання нейронних мереж індивідуумів здійснюється стандартним генетичним алгоритмом. Кожна особа у популяції генетичного алгоритму відповідає окремому роботу та складає  $L$  ваг керуючої нейронної мережі та параметра  $\alpha$ . Кожен параметр кодується  $b$  бітами, а загальна довжина

хромосоми складає  $B$  біт. Задаються також ймовірності кросовера ( $P_{ко}$ ) та комутації ( $P_{ком.}$ ).

Застосування нейронної мережі з генетичним алгоритмом самонавчання дозволяє роботам навчатися один у одного та “запам’ятовувати” закономірності виявлення цілей, що забезпечує автономність роботи всієї групи. За результатами експерименту такий підхід підвищує загальну ефективність системи на 20–30 % у порівнянні з роботою групи роботів за випадковою схемою пошуку і забезпечує можливість роботи групи навіть у випадку втрати каналу зв’язку з наземним пунктом управління.

### Література

1. Перша у світі війна дронів іде в Україні: як безпілотники змінили бойові дії у 2022-2024 роках. [https://antikor.com.ua/articles/685703-pervaja\\_v\\_mire\\_vojna\\_dronov\\_idet\\_v\\_ukraine\\_kak\\_bespilotniki\\_izmenili\\_boevye\\_d\\_ejstvija\\_v\\_2022-2024\\_godah](https://antikor.com.ua/articles/685703-pervaja_v_mire_vojna_dronov_idet_v_ukraine_kak_bespilotniki_izmenili_boevye_d_ejstvija_v_2022-2024_godah)

2. Савченко, В.А., Мацько, О.Й., Пшоннік В.О. (2019). Нейромережева технологія управління багатомашинним роботизованим комплексом пошуку нелегальних випромінювачів. Сучасний захист інформації, 3(39), 15–22. <https://doi.org/10.31673/2409-7292.2019.031522>

## СИСТЕМА ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

**Устименко В. О.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасному цифровому світі питання захисту інформації від несанкціонованого доступу є однією з найактуальніших проблем для організацій і окремих користувачів. Несанкціонований доступ до даних може

призвести до серйозних наслідків, таких як витік конфіденційної інформації, фінансові збитки або порушення функціонування критичних інфраструктур (сс. 1-3). Тому створення надійної системи захисту є необхідною умовою для забезпечення безпеки в умовах зростаючих кіберзагроз.

### 1. Моделі аутентифікації

Аутентифікація є першим рівнем захисту від несанкціонованого доступу. Це процес перевірки ідентичності користувача перед наданням доступу до інформаційних ресурсів. Існують кілька основних моделей аутентифікації:

- **Парольна аутентифікація** — найпоширеніший метод, що вимагає введення правильного пароля. Однак через можливість його вгадування або викрадення цей метод є вразливим.
- **Біометрична аутентифікація** — використовує унікальні фізіологічні або поведінкові характеристики користувача, такі як відбитки пальців, сканування обличчя, голосова аутентифікація.
- **Багатофакторна аутентифікація (MFA)** — поєднує кілька методів аутентифікації для підвищення безпеки (наприклад, комбінація пароля і одноразового коду з телефону) (сс. 5-8) (сс. 4-6).

В Таблиці 1 наведені переваги та недоліки основних моделей аутентифікації.

Таблиця 1

#### Моделі аутентифікації

Тип аутентифікації	Опис	Переваги	Недоліки
Парольна	Використовує пароль	Простота, швидкість	Вразливість до крадіжки
Біометрична	Використовує фізичні або поведінкові характеристики	Високий рівень точності	Висока вартість, проблеми з точністю
Багатофакторна	Комбінація кількох методів	Покращена безпека	Необхідність додаткових пристроїв

## 2. Контроль доступу

Контроль доступу визначає, хто може отримати доступ до конкретних ресурсів і які операції може виконати. Існують кілька моделей контролю доступу:

- **Модель доступу на основі ролей (RBAC):** доступ до ресурсів надається на основі ролі користувача (наприклад, адміністратор, користувач, гість).
- **Модель доступу на основі атрибутів (ABAC):** доступ визначається не тільки роллю, а й іншими атрибутами (наприклад, місцезнаходженням користувача, часом доби).
- **Модель найменших привілеїв:** кожному користувачу надаються лише ті права доступу, які необхідні для виконання його завдань (с. 4-6).

## 3. Моніторинг та виявлення вторгнень

Для забезпечення ефективної системи захисту важливо не лише запобігати несанкціонованому доступу, а й виявляти атаки в реальному часі. Для цього використовуються системи виявлення та запобігання вторгненням (IDS/IPS). Такі системи моніторять мережевий трафік, шукають аномалії і видають попередження або автоматично блокують шкідливу активність (с. 7).

У Таблиці 2 показана архітектура системи виявлення вторгнень.

- Система виявлення вторгнень (IDS) — забезпечує моніторинг трафіку і повідомляє про потенційні загрози.
- Система запобігання вторгненням (IPS) — не лише виявляє загрози, а й активно блокує їх.

Таблиця 2

### Архітектура системи виявлення вторгнень

Система	Функція	Приклад використання
IDS	Моніторинг і виявлення атак	Аналіз мережевого трафіку
IPS	Блокування вторгнень	Запобігання DDoS-атакам

#### 4. Криптографія та шифрування

Криптографія є важливою частиною систем захисту від несанкціонованого доступу, оскільки вона забезпечує конфіденційність і цілісність даних. Шифрування даних, як під час їх зберігання, так і під час передачі, є основним механізмом захисту від перехоплення і несанкціонованого доступу.

- **Асиметричне шифрування (RSA, ECC)** — використовується для безпечної передачі даних між користувачами або серверами.
- **Симетричне шифрування (AES)** — використовується для шифрування великих обсягів даних.

У Таблиці 3 показані приклади використання алгоритмів шифрування (сс. 8-10).

Таблиця 3

#### Алгоритми шифрування

Тип шифрування	Опис	Приклад використання
Асиметричне	Використовує пару ключів	TLS/SSL для захисту веб-з'єднань
Симетричне	Використовує один ключ	Шифрування файлів (AES)

#### 5. Захист від внутрішніх загроз

Не менш важливою є боротьба з внутрішніми загрозами. Працівники, які мають високий рівень доступу до системи, можуть стати джерелом небезпеки через несанкціоноване використання своїх привілеїв або випадкові помилки. Для цього застосовуються методи моніторингу активності користувачів і аудит дій.

- **Аудит доступу** — фіксація всіх дій користувачів і адміністраторів для виявлення підозрілих або несанкціонованих дій.
- **Сегментація мережі** — обмеження доступу до різних частин мережі на основі ролей користувачів (сс. 12-14).

Враховуючи постійно зростаючі загрози в області кібербезпеки, система захисту від несанкціонованого доступу повинна включати багат шарові механізми аутентифікації, контролю доступу, моніторингу, криптографії та захисту від внутрішніх загроз. Лише інтеграція цих технологій у єдину архітектуру може гарантувати ефективний захист від сучасних кіберзагроз.

### **Література**

1. Іванов О. О. Основи кібербезпеки: теорія та практика. Київ: Академвидав. 2021.
2. Кузьменко І. В. Захист інформаційних систем. Теорія та практика побудови безпечних мереж. Харків: Техніка. 2020.
3. Петренко С. І. Методи захисту інформації та криптографія. Львів: Видавництво Львівської політехніки. 2019.
4. Чорновол Л. М. Технології захисту від внутрішніх загроз в інформаційних системах. Одеса: Наука і техніка. 2022.
5. Srinivasan A. Cybersecurity Essentials: The Need for Multi-layer Protection. Springer. 2020

## **МЕТОДИКА РОЗРОБКИ І ВПРОВАДЖЕННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ В СИСТЕМУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ**

**Заведя К. А.**

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

Враховуючи інтенсивність розвитку сучасних інформаційних технологій та інформаційно-комунікаційних систем (ІКС), які забезпечують передавання, оброблення та зберігання даних, актуальність захисту інформаційних ресурсів

набуває все більш важливого значення. Одним із ключових аспектів забезпечення кіберстійкості організації є впровадження надійних механізмів автентифікації, які мінімізують ризики несанкціонованого доступу до критично важливих даних. Багатофакторна автентифікація (MFA) є ефективним методом підвищення рівня захисту, оскільки вимагає від користувача підтвердження особи за допомогою кількох незалежних факторів. У цій роботі розглядається методика розробки та впровадження MFA в систему управління інформаційною безпекою організації, що дозволяє знизити ризики кіберзагроз та забезпечити безперервність бізнес-процесів.

Методика розробки та впровадження багатофакторної автентифікації складається з кількох ключових етапів, кожен з яких має критичне значення для забезпечення ефективності та безпеки процесу автентифікації. Першочергово проводиться аналіз потреб та ризиків, що передбачає ідентифікацію основних загроз, які можуть впливати на інформаційну безпеку організації. Визначення критичних інформаційних систем, доступ до яких повинен бути максимально захищеним, допомагає сформулювати стратегію впровадження MFA та обґрунтувати вибір відповідних механізмів захисту.

Наступним кроком є вибір факторів автентифікації. В основі MFA лежить використання трьох основних типів факторів: щось, що знає користувач (наприклад, пароль або PIN-код), щось, що має користувач (токен, смарт-карта або мобільний пристрій) і щось, що є користувачем (біометричні дані, такі як відбиток пальця або розпізнавання обличчя). Оптимальне поєднання цих факторів визначається на основі рівня ризику та вимог до безпеки конкретної організації.

Інтеграція MFA в існуючі системи є одним із найважливіших етапів впровадження. Для цього необхідно забезпечити сумісність нового механізму автентифікації з чинними інформаційними системами та корпоративними платформами, такими як Active Directory, SSO-системи та інші засоби управління доступом. Важливо також забезпечити централізоване управління

обліковими записами та гнучке налаштування політик автентифікації відповідно до ролей та рівнів доступу в організації.

Після інтеграції слід провести тестування та оцінку ефективності впровадженної системи автентифікації. Тестування може відбуватися у форматі пілотного запуску для обмеженої групи користувачів, що дозволяє виявити можливі проблеми, оцінити рівень зручності користування та ефективність обраної методики. Важливим аспектом цього етапу є аналіз відгуків користувачів та виявлення потенційних недоліків системи з подальшим їх усуненням.

Остаточний етап – це розгортання системи на рівні всієї організації та навчання персоналу. Навчання є критичним для успішного впровадження MFA, оскільки недостатня обізнаність працівників щодо нових процедур може призвести до зниження ефективності заходів безпеки. Запровадження комплексної програми навчання, яка включає інструкції щодо використання MFA, ознайомлення з потенційними загрозами та методами їх уникнення, сприяє загальному підвищенню рівня кібербезпеки організації.

Впровадження багатофакторної автентифікації є важливим етапом у підвищенні рівня кіберстійкості організації та зменшенні ризику компрометації інформаційних систем. Методичний підхід до реалізації MFA, що включає аналіз ризиків, вибір оптимальних факторів автентифікації, інтеграцію, тестування та навчання персоналу, забезпечує ефективний захист від несанкціонованого доступу та сприяє безперервності бізнес-процесів. Таким чином, MFA є необхідним елементом сучасної системи управління інформаційною безпекою, який дозволяє організаціям ефективно протидіяти кіберзагрозам і забезпечувати стабільність своєї діяльності.

## Література

1. Що таке багатофакторна автентифікація (MFA)? URL: <https://cloud.smart-it.com/news-post/what-is-mfa/>

2. Що таке MFA — багатофакторна аутентифікація? URL: <https://datami.ee/ua/blog/shho-take-mfa-bagatofaktorna-autentifikatsiya/>
3. Впровадження систем багатофакторної аутентифікації. URL: <https://techexpert.ua/implementation-of-mfa-systems/>
4. Zero Trust Architecture: новий стандарт у кібербезпеці. URL: <https://vamark.ua/blog/zero-trust-architecture-novyj-standart-u-kiberbezpeczi/>
5. Що таке двохфакторна автентифікація? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa>

## **ТЕХНОЛОГІЇ ШИФРУВАННЯ ТА АНОНІМІЗАЦІЇ ДЛЯ ЗАХИСТУ КОРИСТУВАЧІВ В ІНТЕРНЕТІ**

**Капустенко Д. І.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному світі, де інтернет став невід'ємною частиною життя, захист персональних даних та конфіденційності користувачів набуває все більшого значення. Технології шифрування та анонімізації є ключовими інструментами для забезпечення безпеки в мережі. У даній тезі розглядаються основні методи шифрування та анонімізації, їх переваги та недоліки, а також перспективи розвитку цих технологій у контексті захисту користувачів в Інтернеті.

Інтернет став основним джерелом інформації та комунікації для мільярдів людей по всьому світу. Однак, зі зростанням кількості користувачів зростають і загрози, пов'язані з конфіденційністю та безпекою даних. Зловмисники все частіше використовують різноманітні методи для отримання несанкціонованого

доступу до персональної інформації користувачів. У цьому контексті технології шифрування та анонімізації стають невід'ємними елементами захисту даних у мережі.

Шифрування є одним із найефективніших способів захисту інформації. Воно дозволяє перетворити дані у формат, який може бути прочитаний лише за наявності відповідного ключа. Основні методи шифрування включають:

1. **Симетричне шифрування** – використовує один ключ для шифрування та дешифрування даних. Прикладом такого методу є алгоритм AES (Advanced Encryption Standard), який широко використовується для захисту даних у фінансових операціях та державних установах. Симетричне шифрування є швидким і ефективним, але вимагає надійного механізму обміну ключами між сторонами, що може бути уразливим місцем у системі безпеки.

2. **Асиметричне шифрування** – використовує пару ключів: відкритий для шифрування та закритий для дешифрування. Найвідоміший приклад – алгоритм RSA, який забезпечує високий рівень безпеки за рахунок використання складних математичних операцій. Асиметричне шифрування є більш безпечним для обміну ключами, але вимагає більше обчислювальних ресурсів, що робить його менш ефективним для шифрування великих обсягів даних.

3. **Гібридне шифрування** – поєднує переваги симетричного та асиметричного шифрування. У цьому методі асиметричне шифрування використовується для обміну ключами, а симетричне – для шифрування самих даних. Цей підхід дозволяє забезпечити високу швидкість та безпеку передачі даних.

Анонімізація даних дозволяє приховати особисту інформацію користувачів, зберігаючи при цьому можливість її використання для аналізу. Основні методи анонімізації включають:

1. **Маскування даних** – заміна частини інформації на символ або інший знак. Наприклад, заміна цифр у номері кредитної картки на зірочки. Цей метод є простим у реалізації, але може бути недостатньо ефективним для

повного захисту даних, оскільки зловмисники можуть використовувати додаткові джерела інформації для деанонізації.

2. **Генералізація** – заміна точних значень на більш загальні. Наприклад, заміна конкретного віку на діапазон віку. Цей метод дозволяє зберігати корисність даних для аналізу, але може призводити до втрати деталізації, що може бути критичним для деяких типів досліджень.

3. **Псевдонімізація** – заміна особистих даних на псевдоніми, які не мають прямого зв'язку з реальною особою. Цей метод часто використовується в медичних дослідженнях, де важливо зберігати конфіденційність пацієнтів, але при цьому забезпечувати можливість аналізу даних.

Технології шифрування та анонізації мають свої переваги та недоліки, які важливо враховувати при їх використанні.

#### **Шифрування:**

- **Переваги:** Високий рівень захисту даних, можливість використання в реальному часі, широке застосування у фінансовій та державній сферах.

- **Недоліки:** Вимагає значних обчислювальних ресурсів, складність управління ключами, можливість зламу при недостатній довжині ключа.

#### **Анонізація:**

- **Переваги:** Зберігає корисність даних для аналізу, проста у використанні, дозволяє захищати особисту інформацію без втрати функціональності.

- **Недоліки:** Можливість деанонізації при наявності додаткових даних, втрата деталізації при генералізації, обмежена ефективність у випадках, коли потрібно зберегти точність даних.

З розвитком квантових обчислень традиційні методи шифрування можуть стати менш ефективними. Тому вже зараз ведуться дослідження у сфері квантового шифрування, яке може забезпечити новий рівень захисту даних. Крім того, розвиваються технології диференційної конфіденційності, які дозволяють аналізувати дані без ризику розкриття особистої інформації.

Також важливим напрямком є інтеграція технологій шифрування та анонізації зі штучним інтелектом та машинним навчанням. Це дозволить автоматизувати процеси захисту даних та підвищити ефективність виявлення та запобігання кіберзагроз.

Технології шифрування та анонізації є важливими інструментами для забезпечення безпеки та конфіденційності користувачів в Інтернеті. Незважаючи на деякі недоліки, вони продовжують розвиватися, що дозволяє ефективно протистояти новим загрозам у кіберпросторі. Майбутнє цих технологій пов'язане з інтеграцією нових підходів, таких як квантове шифрування та диференційна конфіденційність, що дозволить забезпечити ще вищий рівень захисту даних.

### Література

1. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. №481-р Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України. URL: <http://zakon.rada.gov.ua/laws/show/96/2016>
2. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice*. 7th Edition. Pearson Education.
3. Narayanan, A., & Shmatikov, V. (2010). *Robust De-anonymization of Large Sparse Datasets*. Proceedings of the IEEE Symposium on Security and Privacy.

# ВИКОРИСТАННЯ XDR ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Орленко М. Є.

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Сучасні кіберзагрози вимагають комплексного підходу до інформаційної безпеки. Традиційні інструменти, такі як антивіруси або системи виявлення вторгнень (IDS/IPS), часто не здатні забезпечити належний рівень безпеки. Extended Detection and Response (XDR) є еволюційним кроком у розвитку технологій кіберзахисту, що інтегрує різні джерела даних та автоматизує процес виявлення й реагування на загрози, а тому є одним із найефективніших рішень, що забезпечує проактивний захист корпоративних мереж.

XDR – це об'єднана платформа інцидентів із безпекою, яка використовує штучний інтелект (ШІ) та автоматизацію. Вона надає організаціям цілісний і ефективний спосіб захисту від складних кібератак і реагування на них. На відміну від спеціалізованих систем, як-от рішення з протидії загрозам у кінцевих точках (EDR), платформи XDR пропонують ширше охоплення для захисту від складніших типів кібератак. Вони об'єднують можливості виявлення, розслідування та реагування в ширшій області, до якої входять, зокрема, кінцеві точки організації, гібридні ідентичності, хмарні програми й завантаженості, електронна пошти та сховища даних. Вони також стимулюють ефективність заходів безпеки (SecOps) завдяки кращій видимості ланцюжків кібератак, автоматизації та аналітики на основі ШІ, а також широкому аналізу кіберзагроз.

XDR використовує штучний інтелект і розширену аналітику, щоб контролювати численні області в технологічному середовищі організації, виявляти оповіщення та співвідносити їх з інцидентами, а також визначати пріоритетність інцидентів, які становлять найвищий ризик. Маючи змогу

бачити кожен кібератаку в ширшому контексті, команди безпеки можуть чіткіше й швидше визначати небезпеку та вибрати найкращий спосіб реагування. Роботу системи можна поділити на наступні кроки:

1. Збір та нормалізація даних - система автоматично збирає телеметричні дані з кількох джерел. Він очищує, упорядковує та стандартизує ці дані, щоб забезпечити доступність узгоджених і високоякісних даних для аналізу.

2. Аналіз та співвідношення даних - система за допомогою машинного навчання та інших можливостей штучного інтелекту автоматично аналізує дані та співвідносить оповіщення з інцидентами. Вона може аналізувати точки даних і виявляти кібератаки й зловмисну поведінку в реальному часі.

3. Полегшення керування інцидентами - система визначає пріоритети серйозності нових інцидентів і надає більше контексту, допомагаючи фахівцям із безпеки швидше сортувати кіберзагрози, виявляти серед них найважливіші та реагувати на них.

4. Допомога у запобіганні майбутнім інцидентам - шляхом аналізу численних даних про кіберзагрози деякі системи XDR надають докладні відомості про кіберзагрози, що стосуються конкретного середовища організації, зокрема про методи кібератак і рекомендовані заходи для протидії ним [1].

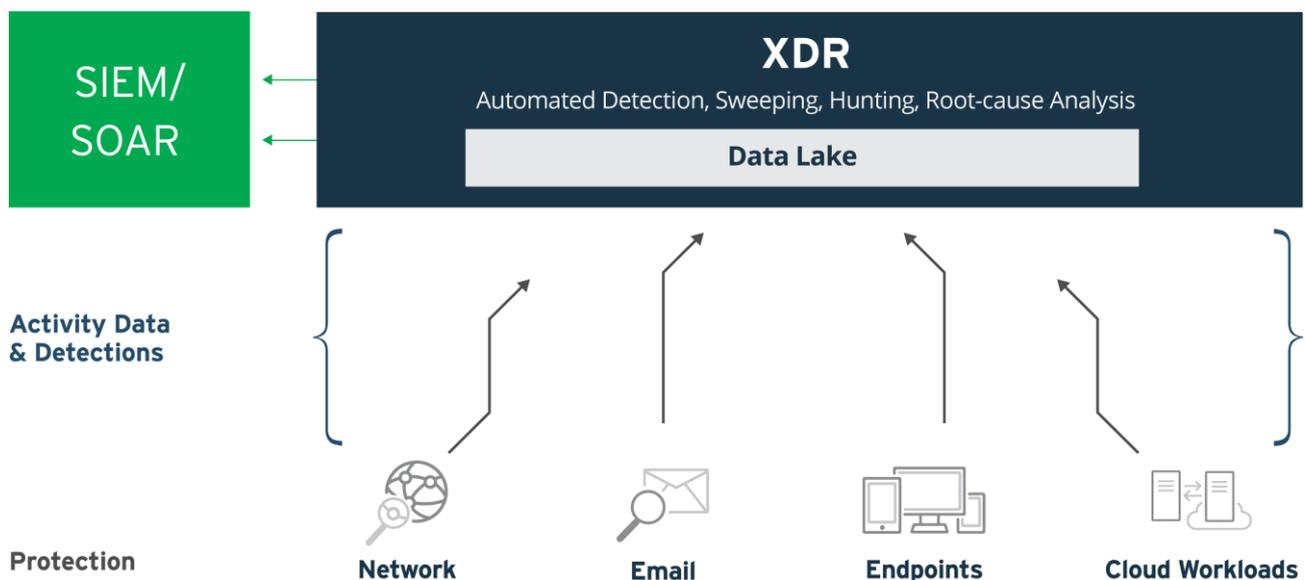


Рис.1 Рівні захисту XDR

Як і будь яка система XDR має свої переваги та недоліки на які слід зважати при прийнятті рішення впровадження в себе такого рішення. До переваг можна віднести:

- Централізоване управління - об'єднання всіх джерел безпеки в єдину систему дозволяє аналітикам отримувати повну картину кіберзагроз у режимі реального часу.
- Автоматизація процесів - XDR мінімізує людський фактор за допомогою штучного інтелекту та машинного навчання, що значно зменшує навантаження на спеціалістів з безпеки.
- Швидке виявлення загроз - аналіз подій з різних джерел дозволяє оперативно ідентифікувати навіть складні атаки, що можуть залишатися непомітними для традиційних рішень.
- Зменшення часу реагування - XDR дозволяє автоматично вживати заходи реагування, такі як припинення підозрілої активності, блокування трафіку чи ізоляція зараженого пристрою, що знижує ймовірність успішної атаки.
- Економічна ефективність - об'єднання всіх компонентів безпеки в одному рішенні дозволяє зменшити витрати на окремі засоби захисту та їхню інтеграцію[2].

У якості недоліків слід зазначити:

- Висока вартість впровадження - інтеграція XDR потребує значних фінансових витрат, особливо для малих і середніх підприємств.
- Складність налаштування та підтримки - XDR вимагає кваліфікованих спеціалістів для налаштування, обслуговування та аналізу загроз.
- Можливість хибнопозитивних спрацювань - через складність аналізу даних XDR може генерувати велику кількість хибних сповіщень, що може перевантажити аналітиків безпеки.

- Залежність від постачальника - деякі XDR-рішення обмежені екосистемою одного виробника, що може створювати проблеми з інтеграцією інших інструментів безпеки.

XDR є перспективною технологією, яка дозволяє суттєво підвищити рівень інформаційної безпеки. Завдяки інтеграції даних із різних джерел, автоматизації процесів та глибокій аналітиці XDR забезпечує ефективний кіберзахист для сучасних організацій. Однак, високі витрати, складність впровадження та можливість хибнопозитивних спрацювань є факторами, які слід враховувати при впровадженні цієї технології. Подальший розвиток XDR сприятиме вдосконаленню методів виявлення та протидії загрозам у кіберпросторі.

### **Література**

1. Що таке розширене виявлення й реагування (XDR)? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-xdr>.
2. Announcing The Forrester Wave: Extended Detection And Response Platforms, Q2 2024. URL: <https://www.forrester.com/blogs/announcing-the-forrester-wave-extended-detection-and-response-platforms-q2-2024/>.

# **ОСНОВИ ВИКОРИСТАННЯ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ У ФІНАНСОВИХ УСТАНОВАХ, КРИПТОГРАФІЧНІ ПРОТОКОЛИ У ЗАХИСТІ БАНКІВСЬКИХ ОПЕРАЦІЙ. РИЗИКИ ВИКОРИСТАННЯ ПУБЛІЧНИХ МЕРЕЖ WI-FI ДЛЯ БАНКІВСЬКИХ ОПЕРАЦІЙ.**

**Рябцун В. П.**

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

Враховуючи інтенсивність розвитку сучасних інформаційних технологій та інформаційно-комунікаційних систем (ІКС), які забезпечують передавання, оброблення та зберігання даних, актуальність захисту інформаційних ресурсів набуває все більш важливого значення. У фінансовому секторі, де здійснюються банківські операції та обробка конфіденційних даних клієнтів, забезпечення кібербезпеки є критично важливим аспектом. Одним із ключових механізмів захисту є використання багатофакторної автентифікації (MFA), яка мінімізує ризик несанкціонованого доступу до банківських систем. Додатково, криптографічні протоколи забезпечують надійність проведення фінансових транзакцій, а використання публічних Wi-Fi мереж несе значні ризики безпеки, що потребує особливої уваги [1].

Багатофакторна автентифікація (MFA) є одним із ключових методів захисту доступу до фінансових систем, що забезпечує високий рівень безпеки для банківських операцій. Вона базується на принципі використання кількох незалежних факторів автентифікації, що значно ускладнює можливість несанкціонованого доступу. У фінансових установах застосовуються три основні категорії автентифікаційних факторів: знання (паролі, PIN-коди), володіння (токени, смарт-карти, мобільні додатки) та біометрія (відбитки пальців, розпізнавання обличчя). Одним із найпоширеніших рішень у банківській сфері є двофакторна автентифікація (2FA), що поєднує пароль із тимчасовим кодом із мобільного додатка або SMS. Проте для підвищення

безпеки все частіше використовуються апаратні токени та криптографічні ключі, які значно зменшують ризик компрометації. Успішне впровадження MFA дозволяє банкам мінімізувати ймовірність шахрайства, зламів облікових записів і крадіжки фінансових даних клієнтів [2].

Захист банківських операцій ґрунтується на використанні криптографічних методів, які забезпечують конфіденційність, цілісність і автентичність даних під час їхнього передавання та зберігання. Сучасні фінансові установи застосовують різноманітні криптографічні протоколи, такі як TLS (Transport Layer Security) для захисту веб-транзакцій, HSM (Hardware Security Module) для зберігання криптографічних ключів і PKI (Public Key Infrastructure) для забезпечення електронного підпису та цифрової ідентифікації клієнтів. Один із найважливіших механізмів безпеки — використання алгоритмів шифрування, таких як AES-256 та RSA, які дозволяють забезпечити надійний захист даних під час операцій. Крім того, банки активно використовують одноразові паролі (OTP), захищені криптографічними алгоритмами HMAC (Hash-based Message Authentication Code), що значно ускладнює можливість їхнього перехоплення або підробки. Також важливу роль відіграють криптографічні механізми токенізації та хешування, які зменшують ризик витоку конфіденційної інформації, зокрема даних платіжних карток.

Підключення до публічних мереж Wi-Fi під час виконання банківських операцій є серйозним ризиком для користувачів, оскільки відкриті мережі часто є незахищеними або можуть контролюватися зловмисниками. Основні загрози включають атаки типу "людина посередині" (MITM), підроблені точки доступу та перехоплення трафіку. Зловмисники можуть створювати фальшиві Wi-Fi мережі, які імітують легітимні точки доступу, змушуючи користувачів несвідомо передавати свої облікові дані та фінансову інформацію. Крім того, через відсутність шифрування в деяких публічних мережах користувачі можуть стати жертвами сніффінгу (перехоплення трафіку), що дозволяє зловмисникам отримати доступ до паролів, номерів карток та іншої конфіденційної інформації. Для мінімізації цих ризиків рекомендується використовувати VPN-

сервіси, відключати автоматичне підключення до відкритих Wi-Fi-мереж і застосовувати багатофакторну автентифікацію. Також важливо перевіряти наявність захищеного з'єднання (HTTPS) під час входу в банківські системи та уникати введення особистих даних через публічні мережі без додаткового шифрування [3].

Ці заходи є важливими складовими забезпечення кібербезпеки у фінансовій сфері, сприяючи захисту клієнтів і збереженню їхніх активів у сучасному цифровому середовищі.

### **Література**

1. Потенційні небезпеки використання публічних Wi-Fi мереж. URL: <https://clearvpn.com/blog/ua/nebezpeky-vykorystannia-pubichnykh-wifi-merezh>
2. Багатофакторна автентифікація. URL: <https://iitd.ua/bagatofaktorna-avtentifikacziya>
3. Безпечне підключення до інтернету через публічні Wi-Fi мережі. URL: <https://loda.gov.ua/news/119025>

## **ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ІТ-ІНФРАСТРУКТУРИ**

**Журбенко А. О.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасні інформаційні системи все більше залежать від стабільності та доступності ІТ-інфраструктури. Безперервність роботи організацій значною мірою визначається ефективністю заходів із забезпечення кібербезпеки та стійкості до збоїв. Одним із ключових рішень для гарантування безперервності функціонування є використання хмарних технологій [1].

Хмарні обчислення дозволяють забезпечити гнучкість, масштабованість та відмовостійкість ІТ-інфраструктури завдяки використанню розподілених ресурсів, автоматичного балансування навантаження та механізмів резервного копіювання. До основних типів хмарних послуг можна віднести:

SaaS (Software as a Service) — це модель надання програмного забезпечення як послуги через інтернет. Користувачі отримують доступ до програм, що працюють на серверах постачальника послуг, без необхідності їх встановлення чи обслуговування. До SaaS належать можемо віднести такі сервіси як Google Workspace та Microsoft 365. Ця модель дозволяє знизити витрати на придбання та підтримку програмного забезпечення, а також швидко адаптуватися до змін у бізнес-процесах.

PaaS (Platform as a Service) — це модель, яка надає платформи для розробки, тестування та розгортання програмних продуктів. Компанії можуть використовувати інструменти розробки та управління програмами без необхідності підтримки серверної інфраструктури. Прикладами PaaS є Microsoft Azure, Google App Engine. Ця модель дозволяє скоротити час виходу нових продуктів на ринок, підвищити ефективність розробки та знизити витрати на ІТ-інфраструктуру.

IaaS (Infrastructure as a Service) — це модель, яка надає в оренду віртуальні сервери, сховища даних та мережеві ресурси через інтернет. Клієнти можуть налаштовувати та керувати обчислювальними ресурсами відповідно до власних потреб. Прикладами таких сервісів можуть бути Amazon Web Services (AWS), Google Cloud. Модель IaaS дозволяє підприємствам масштабувати свої ресурси в залежності від поточних потреб, мінімізуючи капітальні витрати. [1]

Основні переваги хмарних технологій для забезпечення безперервності ІТ-інфраструктури:

1. Гнучкість та масштабованість – можливість адаптації ресурсів під змінні навантаження:

Хмарні технології дають змогу легко масштабувати ресурси залежно від потреб бізнесу. Якщо вашому бізнесу потрібно більше потужності або сховища,

ви можете швидко адаптуватися, не витрачаючи місяці на закупівлю та налаштування нового обладнання. Це особливо корисно для стартапів, які можуть раптово зіткнутися зі зростанням попиту на свої продукти або послуги.

2. Автоматизоване резервне копіювання – збереження критичних даних у віддалених дата-центрах:

Постачальники хмарних послуг беруть на себе відповідальність за оновлення програмного забезпечення та забезпечення безпеки даних, що звільняє компанії від необхідності постійно слідкувати за оновленнями та боротьбою із загрозами безпеці. Вони впроваджують сучасні методи шифрування, багаторівневі системи автентифікації та постійний моніторинг безпеки, щоб захистити вашу інформацію.

Крім того, хмарні постачальники зазвичай мають високі стандарти безпеки, що відповідають міжнародним нормативам і сертифікаціям. Вони активно моніторять загрози безпеці та реагують на них, забезпечуючи захист ваших даних від кібератак.

3. Швидке відновлення після збоїв – зменшення часу простою завдяки вбудованим механізмам відновлення:

Ще одним важливим аспектом є резервне копіювання даних. Хмарні постачальники зазвичай надають регулярне резервне копіювання даних, що дає змогу відновити інформацію в разі аварій або надзвичайних ситуацій. Це забезпечує надійність і безперервність бізнес-процесів, навіть у разі непередбачених подій.

Таким чином, хмарні технології не тільки надають бізнесам доступ до передових ресурсів і застосунків, а й гарантують безпеку та надійність ваших даних, а також звільняють вас від турбот з обслуговування та оновлення ІТ-інфраструктури.

4. Розподілена архітектура – зниження ризику повної втрати доступу до сервісів через географічно розподілені сервери.

Однією з ключових переваг хмарних рішень є можливість спільного доступу до інформації в режимі реального часу. Співробітники можуть

одночасно працювати над спільними документами, проектами або файлами, незалежно від їхнього фізичного розташування. Це особливо важливо в умовах глобалізації бізнесу, коли команди можуть бути розподілені по різних країнах або навіть континентах. Хмарні сервіси дозволяють працівникам редагувати документи, обмінюватися ідеями і вносити зміни без необхідності пересилати файли через електронну пошту або зберігати їх локально.

Це значно скорочує час на прийняття рішень і вирішення завдань. Процеси, які раніше вимагали днів або навіть тижнів через затримки у комунікаціях або фізичному доступі до файлів, тепер можуть бути виконані за кілька годин. Завдяки інтеграції хмарних платформ з інструментами для відеоконференцій, миттєвих повідомлень та відстеження прогресу проектів, співробітники можуть підтримувати тісну комунікацію та вирішувати робочі питання в реальному часі.

#### 5. Економічна ефективність – зменшення витрат на власну інфраструктуру та її обслуговування:

Однією з основних переваг хмарних технологій є зниження витрат на інфраструктуру. Компанії більше не зобов'язані купувати і підтримувати власне обладнання та сервери. Замість цього, вони можуть орендувати ресурси у постачальників хмарних послуг, що надають готову інфраструктуру на абонентській основі. Це дає змогу заощадити кошти, які раніше були б спрямовані на капітальні витрати.

Причини зниження витрат включають в себе:

- Нульові витрати на початкове обладнання: Без необхідності купувати дороге обладнання, компанії можуть зосередити свій капітал на стратегічних пріоритетах і розвитку.
- Ефективне використання ресурсів: Хмарні постачальники забезпечують високий рівень використання серверів і сховища, що усуває необхідність у надлишкових ресурсах і знижує витрати.

- Управління операційними витратами: Турботу про фізичну безпеку, оновлення та резервне копіювання беруть на себе постачальники хмарних послуг, що знижує операційні витрати та зменшує ризики.

- Платіть тільки за використання: Модель оплати "за використанням" дає змогу компаніям платити тільки за ті ресурси, які вони реально використовують. Це справедливо як для невеликих підприємств, так і для великих корпорацій.

Однак, використання хмарних технологій також пов'язане з певними ризиками, зокрема загрозами кібербезпеці, що вимагає впровадження додаткових заходів захисту, таких як шифрування даних, багатofакторна автентифікація та контроль доступу.

Таким чином, інтеграція хмарних технологій у процеси забезпечення безперервності IT-інфраструктури є ефективним рішенням для сучасних організацій, що дозволяє забезпечити стабільність, безпеку та оперативне відновлення бізнес-процесів.

### **Література**

1. Хмарні технології як фактор підвищення ефективності діяльності компанії

URL:<https://heraldes.khmnu.edu.ua/index.php/heraldes/article/download/528/551/1860?>

# **ВИКОРИСТАННЯ SPLUNK ДЛЯ ОПТИМІЗАЦІЇ ПРОЦЕСІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРАТАКИ У СТРУКТУРАХ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ**

**Фомін І. О.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Оптимізація процесів виявлення та реагування на кібератаки у структурах малих та середніх підприємств обумовлена стрімким зростанням кіберзагроз та зростаючими потребами до аналізу, обробки та реагування. Використання Splunk дозволить подолати розрив в захищеності процесів враховуючи обмежені ресурси для організації безпеки корпоративного рівня. Це дозволить звільнити додаткові ресурси, котрі є надзвичайно важливим для малих та середніх підприємств. Звільнення ресурсів означатиме ефективніше використання людських та фінансових ресурсів, а також наявної технічної інфраструктури.

За останніми даними Світового банку, малі та середні підприємства залишаються опорою глобальної економіки – вони становлять приблизно 90% усіх бізнесів і забезпечують понад 55% робочих місць, що підкреслює їхню вирішальну роль у зайнятості. Проте, внаслідок швидкого впровадження цифрових технологій у відповідь на виклики пандемії COVID-19, численні підприємства стають дедалі більш вразливими до кіберзагроз, що вимагає посиленої уваги до питань кібербезпеки. [1].

Виявлення кібератак та реагування на них є наріжним каменем стратегій кібербезпеки підприємств і вимагають постійного вдосконалення, щоб протистояти зростаючій складності та адаптивності сучасних загроз [2]. Оскільки кіберзлочинці використовують передові інструменти, зокрема моделі штучного інтелекту, організаціям необхідно впроваджувати захисні засоби, які відповідають сучасним стандартам ефективності, зосереджуючись на

оперативності, точності та можливості масштабування. [3]. Тому важливо мати розширений аналіз цих процесів, збагачений висновками останніх досліджень і галузевими тенденціями [4]. Основними ключовими процесами, що можуть підпадати під оптимізацію є:

1. Інцидентний відгук: Оцінка ефективності автоматизованих процесів обробки інцидентів для оперативного визначення їх серйозності і пріоритетності, а також розробка механізмів призначення відповідальних осіб для реагування на конкретні типи інцидентів.

2. Моніторинг та аналіз загроз: Аналіз ефективності процесів обробки інцидентів автоматизованими системами для швидкого визначення їх серйозності та пріоритетів з можливістю визначення та призначення відповідальних осіб для реагування на конкретний тип інциденту.

3. Навчальні програми: Оцінка результативності програм підготовки та тренувань персоналу з питань реагування на кіберзагрози з метою підвищення їх компетенцій та оперативності у дії.

4. Співпраця та комунікації: Аналіз і вдосконалення існуючих комунікаційних протоколів і процедур для забезпечення ефективної взаємодії між командами під час реагування на інциденти.

Перегляд ефективності ключових процесів дозволяє не лише своєчасно виявляти та реагувати на кібератаки, а й визначити, які саме напрямки потребують оптимізації для досягнення максимальної ефективності за наявних ресурсів. Водночас постійне вдосконалення даних процесів, що базується на аналізі отриманої інформації та результатів заходів безпеки, є критично важливим – від встановлення політики інформаційної безпеки, яка задає цілі та основні принципи, до розробки детальних процедур, що регламентують впровадження цих принципів [5].

Наприклад, для підвищення якості збору та аналізу даних про загрози можна використовувати Splunk Enterprise – програмне забезпечення, яке дозволяє здійснювати пошук, аналіз та візуалізацію інформації, зібраної із різних компонентів ІТ-інфраструктури чи бізнесу. Splunk приймає дані з веб-

сайтів, додатків, датчиків, пристроїв та інших джерел, індексує їх і розбиває на окремі події для подальшого аналізу. Це забезпечує оперативне виявлення аномалій та дозволяє оптимізувати процеси безпеки, швидко реагуючи на нові виклики та зменшуючи ризики кіберзагроз [6].

Splunk Enterprise Security спрощує реагування на інциденти завдяки інтеграції можливостей Security Orchestration, Automation and Response. Для малих і середніх підприємств з обмеженим штатом автоматизація зменшує ручну роботу і прискорює локалізацію інцидентів. Наприклад:

1. Автоматизовані плейлисти: Splunk SOAR (тепер частина Unified Security Operations Splunk) дозволяє заздалегідь визначені робочі процеси для карантину фішингових електронних листів, ізоляції скомпрометованих пристроїв або блокування шкідливих IP-адрес за лічені секунди, мінімізуючи час очікування [7; 8].

2. Розстановка пріоритетів: Кореляційний пошук в Splunk ES аналізує дані з брандмауерів, кінцевих точок і хмарних систем, щоб ранжувати інциденти за ступенем серйозності, гарантуючи, що команди в першу чергу реагують на критичні загрози.

3. Інтеграція зі сторонніми інструментами: Splunk ES інтегрується з такими інструментами, як LDAP/SAML для управління ідентифікацією та брандмауери для усунення загроз в режимі реального часу, створюючи цілісну екосистему захисту [8].

Для малого та середнього бізнесу Splunk долає розрив між обмеженими ресурсами та безпекою корпоративного рівня. Автоматизуючи робочі процеси, покращуючи прозорість та спрощуючи дотримання нормативних вимог, Splunk дозволяє швидше виявляти загрози, рішуче реагувати на них та адаптуватися до все більш ворожого кібер-ландшафту. Його відповідність таким стандартам, як MITRE ATT&CK і NIST, забезпечує довгострокову стійкість, що робить його наріжним каменем сучасних стратегій кібербезпеки для малого та середнього бізнесу.

## Література

1. World Bank Group: Small and Medium Enterprises Finance. URL: <https://www.worldbank.org/en/topic/smefinance>
2. Emerging Threats: Cybersecurity Forecast 2025. URL: <https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025/>
3. Key cyber security trends to watch in 2025. URL: <https://new.abb.com/news/detail/123029/key-cyber-security-trends-to-watch-in-2025>
4. Cybersecurity for small businesses. URL: <https://shorturl.at/wCELT>
5. Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises. URL: <https://dialnet.unirioja.es/descarga/articulo/9031740>
6. Splunk Enterprise Overview. URL: <https://docs.splunk.com/Documentation/Splunk/9.4.0/Overview/AboutSplunkEnterprise>
7. Splunk ES Implementation Checklist. URL: <https://sp6.io/blog/es-implementation-checklist-for-splunk/>
8. Understanding Splunk ES and Its Role in Cybersecurity. URL: <https://securityboulevard.com/2023/03/understanding-splunk-es-and-its-role-in-cybersecurity/>

## ВИКЛИКИ ТА РІШЕННЯ ХМАРНОЇ БЕЗПЕКИ

**Завгородня Є. Я.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Зростання популярності хмарних обчислень спричинило необхідність забезпечення належного рівня безпеки даних, що зберігаються та обробляються в хмарному середовищі. З огляду на появу нових загроз і розширення

масштабів кіберзлочинності критично важливою для захисту інформації, яка зберігається й обробляється у хмарі є надійна система забезпечення кібербезпеки.

Важливою передумовою ефективного захисту даних у віддаленому середовищі є глибоке й об'єктивне розуміння ландшафту кіберзагроз і основних проблем безпеки.

Як показав аналіз, основними викликами хмарній безпеці на сучасному етапі є [1, 2]:

- витоки даних і порушення конфіденційності – хмарні сервіси часто стають мішенню атак, що призводить до витоку особистої та корпоративної інформації;

- вразливості в API та управлінні доступом – неналежна автентифікація та слабкі механізми контролю доступу дозволяють хакерам проникати в систему;

- зловмисні програми й атаки на хмарні середовища – шкідливе ПЗ, фішинг-атаки та DDoS-атаки створюють загрозу стабільній роботі сервісів;

- дотримання відповідності стандартам і регуляторним вимогам – компанії повинні дотримуватися міжнародних норм безпеки, таких як GDPR, ISO 27001, SOC тощо;

- проблеми безперервності бізнесу та відновлення після інцидентів – швидке відновлення операцій після атак або збоїв є дуже важливими в умовах постійних кіберзагроз.

Сьогодні галузь кібербезпеки пропонує велику кількість різноманітних програмно-технічних рішень, які в комплексі дозволять ефективно запобігти і протидіяти загрозам хмарній безпеці, серед яких:

- шифрування даних, що передбачає використання сучасних криптографічних методів для забезпечення конфіденційності інформації;

- механізми багаторівневої автентифікації (MFA), які забезпечують посилений контроль доступу користувачів до хмарних сервісів;

– системи моніторингу та виявлення загроз, зокрема SIEM-рішень, які дозволяють здійснювати оперативне виявлення й усунення наслідків інцидентів;

– контейнери та безсерверні архітектури для підвищення захищеності додатків у хмарі завдяки ізольованим середовищам;

– резервне копіювання й реагування на кіберінциденти, завдяки яким забезпечується впровадження стратегій швидкого відновлення даних і безперервності бізнесу [2, 3].

Отже, хмарна безпека є ключовим елементом сучасної кібербезпеки і має на меті запобігання кіберзагрозам, а також захист даних і засобів їх обробки у хмарних середовищах. Для вирішення цих завдань використовують комплекс програмно-технічних засобів, а також низку організаційних та нормативних заходів. Узгоджене застосування розглянутих рішень сприятиме мінімізації загроз і підвищенню рівня захищеності хмарних середовищ.

### Література

1. Narendra, Rao & Tadapaneni, Sr & Sabri, Mustafa. Cloud computing security challenges. *SSRN Electronic Journal*. 2020. №7. P. 1-6. URL: [https://www.researchgate.net/publication/354788317\\_CLOUD\\_COMPUTING\\_SECURITY\\_CHALLENGES](https://www.researchgate.net/publication/354788317_CLOUD_COMPUTING_SECURITY_CHALLENGES)

2. Security Guidance for Critical Areas of Focus in Cloud Computing V5. 2024. *Cloud Security Alliance*. URL: <https://cloudsecurityalliance.org/research/guidance>

3. What is cloud security? *IBM*. URL: <https://www.ibm.com/think/topics/cloud-security>

# ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМ КІБЕРБЕЗПЕКИ У ВІДДАЛЕНОМУ РОБОЧОМУ СЕРЕДОВИЩІ

**Курінний О. С.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Розвиток технологій та масове впровадження віддаленої роботи зумовили нові виклики у сфері кібербезпеки. Основними загрозами є витік конфіденційних даних, фішингові атаки, недостатня захищеність домашніх мереж працівників і неналежне управління доступом. У даних тезах розглядаються сучасні методи підвищення рівня безпеки, включаючи впровадження багатофакторної автентифікації (MFA), використання VPN, застосування систем розширеного моніторингу та навчання співробітників основам кібербезпеки [1].

З переходом підприємств на гібридний та повністю дистанційний формат роботи зросла потреба в ефективному захисті корпоративної інформації. Традиційні методи кібербезпеки потребують адаптації до нових умов. Атаки на віддалених працівників стають дедалі складнішими, що вимагає нових підходів до управління ризиками.

## **Основні загрози кібербезпеки у віддаленому робочому середовищі**

1. **Фішингові атаки та соціальна інженерія** – спрямовані на викрадення паролів та іншої конфіденційної інформації.
2. **Низький рівень захисту домашніх мереж** – використання незахищених Wi-Fi-з'єднань, слабких паролів.
3. **Відсутність централізованого контролю доступу** – недостатнє застосування політик безпеки щодо корпоративних ресурсів.
4. **Зловмисне програмне забезпечення (віруси, трояни, кейлогери)** – підвищений ризик інфікування пристроїв поза корпоративною мережею [2].

## **Методи вирішення проблем кібербезпеки**

1. **Використання багатофакторної автентифікації (MFA)** – знижує ризик несанкціонованого доступу.
2. **Шифрування даних та впровадження VPN** – забезпечує захист під час передавання інформації.
3. **Моніторинг активності та антивірусний захист** – своєчасне виявлення загроз.
4. **Навчання працівників** – підвищення рівня обізнаності про основні кіберзагрози та методи їх уникнення.

Забезпечення кібербезпеки у віддаленому робочому середовищі вимагає комплексного підходу, що включає технічні та організаційні заходи [3]. Використання сучасних методів безпеки дозволяє значно знизити ризики витоку даних і зловмисних атак, що є критично важливим для стабільного функціонування підприємств у цифрову епоху.

## **Література**

1. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. № 481-р «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України».
2. NIST Special Publication 800-46. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. National Institute of Standards and Technology, 2021.
3. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації щодо безпеки віддаленої роботи, 2022 р.

# ВИКОРИСТАННЯ МЕТОДІВ КЛАСТЕРИЗАЦІЇ ДЛЯ ВИЯВЛЕННЯ ДЖЕРЕЛ ФЕЙКОВОЇ ІНФОРМАЦІЇ

**Тищенко В. С., Кушнерьов І. К.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасному інформаційному просторі поширення фейкової інформації набуло масштабного характеру, що негативно впливає на суспільну думку, політичні процеси та безпеку в цифровому середовищі. Дезінформаційні кампанії можуть бути ініційовані як окремими особами, так і організованими групами або навіть державами. У зв'язку з цим виникає необхідність у розробці та застосуванні автоматизованих підходів для виявлення джерел фейкових новин та протидії їхньому поширенню.

Одним із ефективних методів, що застосовуються для цього, є кластеризація – техніка машинного навчання, яка дозволяє групувати об'єкти за схожими характеристиками. Використання алгоритмів кластеризації дає змогу аналізувати великі обсяги даних, виявляти аномальні інформаційні потоки та ідентифікувати групи ресурсів, що поширюють неправдиву інформацію [1].

Основи кластеризації та її роль у виявленні аномалій

Кластеризація – це метод обробки даних, що використовується для групування об'єктів за подібністю їхніх характеристик. На відміну від класифікації, цей підхід не потребує попередньої розмітки даних, що дозволяє застосовувати його в ситуаціях, де апріорне знання про категорії об'єктів відсутнє. У контексті боротьби з фейковими новинами кластеризація допомагає:

- виділяти аномальні джерела інформації, що демонструють нетипову поведінку;
- групувати новини за змістом, стилем та джерелами походження;

- виявляти потенційні осередки дезінформації, які систематично продукують неправдивий контент.

Застосування алгоритмів кластеризації

Серед алгоритмів кластеризації, які широко застосовуються для аналізу інформаційних потоків, можна виділити [2]:

- K-means – популярний метод, що поділяє дані на задану кількість кластерів, дозволяючи виділити основні групи поширювачів інформації.

- DBSCAN – алгоритм, що добре працює з аномальними даними та дозволяє знаходити щільні групи взаємопов'язаних джерел.

- Ієрархічна кластеризація – метод, що створює дерево зв'язків між даними, допомагаючи виявляти взаємозв'язки між сайтами або акаунтами, які поширюють схожий контент.

Застосування цих алгоритмів у медіа-аналітиці дозволяє знаходити мережі сайтів, що одночасно поширюють певний наратив, а також виявляти синхронізовані інформаційні атаки.

Використання текстового аналізу у поєднанні з кластеризацією

Кластеризація ефективно поєднується з методами обробки природної мови (NLP), що дає змогу аналізувати характеристики текстів, а саме:

- лексичний склад – виявлення повторюваних фраз, специфічної термінології або шаблонних конструкцій у фейкових новинах;

- емоційне забарвлення – визначення рівня сенсаційності та маніпулятивного характеру контенту;

- стилістичний аналіз – ідентифікація авторських особливостей та схожості між текстами різних джерел.

Такі підходи дозволяють знаходити групи статей або повідомлень, що мають спільну мету маніпулювання громадською думкою.

Розпізнавання бот-мереж і координованих інформаційних атак

Багато фейкових новин поширюються через автоматизовані акаунти – так звані боти. Використовуючи кластеризацію, можна ефективно аналізувати такі параметри бот-мереж [3]:

- повторюваність контенту – виявлення акаунтів, що публікують однакові або схожі повідомлення у короткі проміжки часу;
- часові характеристики – аналіз активності акаунтів, що можуть працювати за чітким графіком без природної поведінки;
- структура взаємодії – виявлення груп акаунтів, що систематично поширюють контент один одного, штучно збільшуючи його охоплення.

Ці методи допомагають соціальним платформам ідентифікувати організовані кампанії з дезінформації та обмежувати їхнє поширення.

Практичне застосування в кібербезпеці та соціальних мережах

Методи кластеризації активно застосовуються великими технологічними компаніями для боротьби з фейковою інформацією. Серед практичних сценаріїв їхнього використання можна виділити:

- маркування підозрілого контенту – автоматичне визначення потенційно фейкових новин та додавання до них відповідних попереджень;
- виявлення мереж дезінформації – аналіз взаємозв'язків між сайтами, блогами та акаунтами, що координовано поширюють неправдиві дані;
- фільтрація інформації у новинних агрегаторах – визначення надійності джерел на основі історичних даних та кластерного аналізу.

У майбутньому подальший розвиток методів кластеризації та їх інтеграція з іншими технологіями (наприклад, штучним інтелектом та блокчейном) дозволить ще більш ефективно протидіяти дезінформації.

Методи кластеризації є важливим інструментом у боротьбі з фейковою інформацією. Вони дозволяють автоматизовано аналізувати великі обсяги даних, виявляти аномальні інформаційні потоки та ідентифікувати мережі джерел дезінформації. Використання таких підходів у кібербезпеці, соціальних мережах та новинних агрегаторах сприяє створенню більш надійного інформаційного середовища.

Подальший розвиток кластеризаційних алгоритмів та їх інтеграція з іншими технологіями дозволить ще більш точно виявляти фейкові новини та зменшувати їхній вплив на суспільство. Це, у свою чергу,

## Література

1. Кластеризація ключових слів. *Блог Idea Digital Agency*. URL: <https://ideadigital.agency/blog/klasterizatsiya-klychovyh-sliv/>.
2. Кластерний аналіз. *Вікіпедія*. 2023. URL: [https://uk.m.wikipedia.org/wiki/Кластерний\\_аналіз](https://uk.m.wikipedia.org/wiki/Кластерний_аналіз).
3. Microsoft Clustering Algorithm. *Microsoft Learn*. 2023. URL: <https://learn.microsoft.com/ru-ru/analysis-services/data-mining/microsoft-clustering-algorithm?view=asallproducts-allversions>.

## КІБЕРБЕЗПЕКА В СИСТЕМАХ УПРАВЛІННЯ ВЕЛИКИМИ ДАНИМИ: ВИКОРИСТАННЯ ІНСТРУМЕНТІВ POWER BI

**Марченко М. В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасних умовах цифрової трансформації обсяг даних, що генерується та обробляється, стрімко зростає. Це підвищує актуальність забезпечення надійної кібербезпеки в системах управління великими даними. Аналітичні платформи, такі як Power BI, надають широкі можливості для інтеграції, аналізу та візуалізації даних, проте разом із цим виникають ризики несанкціонованого доступу, витоку конфіденційної інформації та маніпуляції даними [1].

Power BI є потужним інструментом для обробки великих даних, що активно використовується у сфері бізнес-аналітики та управління інформацією. Однак відсутність належного рівня кіберзахисту може спричинити такі загрози:

- Компрометація даних через недостатній контроль доступу;
- Атаки на рівні мережевої інфраструктури під час передачі даних;

- Використання шкідливого програмного забезпечення для модифікації аналітичних звітів;
- Ризики витоку даних через недостатню безпеку механізмів аутентифікації, шифрування та контролю доступу під час їхнього зберігання та передачі [2].

Зі збільшенням кількості даних, що обробляються в реальному часі, виникає потреба в удосконалених засобах захисту. Без належного рівня безпеки дані можуть бути піддані зовнішнім атакам, а також внутрішнім загрозам через несанкціонований доступ або людські помилки.

Також важливо зазначити, що кібербезпека повинна бути інтегрована на всіх етапах обробки даних — від збору до візуалізації. Крім того, використання даних з зовнішніх джерел може підвищити ризик несанкціонованого доступу, тому важливо проводити ретельну перевірку таких джерел. Постійний моніторинг і аудит допоможуть своєчасно виявляти порушення безпеки та оперативно реагувати на них [3].

Використання Power BI у сфері обробки великих даних дає значні переваги в плані аналітики та прийняття рішень на основі даних, проте не можна нехтувати важливістю належного захисту інформації. Тому важливо вживати заходів для мінімізації ризиків, таких як підвищення обізнаності працівників, використання сучасних технологій захисту даних та регулярний моніторинг безпеки.

### **Література**

1. Microsoft. Power BI: Безпека. URL: <https://learn.microsoft.com/en-gb/power-bi/guidance/whitepaper-powerbi-security>
2. Microsoft. Power BI: Адміністрування безпеки. URL: <https://learn.microsoft.com/en-gb/power-bi/enterprise/service-admin-power-bi-security?source=recommendations>

3. Microsoft. Power BI: Шифрування даних з використанням ВУОК (Bring Your Own Key). URL: <https://learn.microsoft.com/en-gb/power-bi/enterprise/service-encryption-byok?source=recommendations>

## ВИКОРИСТАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙНУ ДЛЯ ПЕРЕВІРКИ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ

**Нестеров О. В.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Боротьба з дезінформацією та забезпечення автентичності цифрового контенту є пріоритетним завданням у сучасному інформаційному середовищі. Інноваційні технології, такі як блокчейн і криптографічні методи, відкривають нові можливості для верифікації даних, підвищуючи рівень довіри до цифрових ресурсів.

Блокчейн-технології забезпечують децентралізоване зберігання інформації з гарантією її незмінності та прозорості. Криптографічні хеш-функції дозволяють створювати цифрові підписи, що підтверджують походження та цілісність даних. Смарт-контракти автоматизують процеси перевірки фактів і управління довіреними джерелами, зменшуючи ризик людського впливу [1].

Важливу роль у підтвердженні інформації без розкриття конфіденційності відіграють **Zero-Knowledge Proofs (ZK)**. Цей криптографічний механізм дозволяє верифікувати правдивість тверджень, не розкриваючи їхнього змісту. Наприклад, протоколи ZK-SNARKs та ZK-STARKs використовуються для анонімної ідентифікації користувачів або перевірки цифрових документів у блокчейн-мережах (Mina Protocol, Aleo, zkSync), що поєднує захист приватності з гарантією достовірності.

Для посилення автентичності контенту застосовуються додаткові інструменти:

- Timestamping (мітки часу) фіксує момент створення або модифікації даних через платформи на кшталт OpenTimestamps.
- Децентралізовані оракули (Chainlink, API3) інтегрують зовнішні джерела інформації з блокчейном, забезпечуючи перехресну валідацію фактів.
- NFT слугують інструментом підтвердження оригінальності цифрових активів у мистецтві, медіа та журналістиці, запобігаючи підробкам.

Однак впровадження цих технологій супроводжується викликами [2]:

- Обмежена масштабованість блокчейн-мереж та висока вартість транзакцій.
- Відсутність механізмів перевірки якості первинних даних, що вносяться до системи.
- Етичні дилеми щодо зберігання особистої інформації в публічних реєстрах.

Для подолання цих обмежень пропонуються стратегії:

- Розробка гібридних архітектур, що поєднують блокчейн із ZK-доказами для балансу між прозорістю та конфіденційністю.
- Інтеграція смарт-контрактів із оракул-системами для автоматизації перевірки зовнішніх джерел.
- Оптимізація алгоритмів консенсусу для зниження енерговитрат і підвищення швидкості обробки даних [3].

Отже, комбінація блокчейн-технологій, ZK-доказів та супутніх інструментів формує комплексну систему для боротьби з дезінформацією. Подальші дослідження мають зосередитись на поліпшенні масштабованості, зменшенні витрат та розробці етичних стандартів, що забезпечать ефективне використання цих рішень у глобальному інформаційному просторі.

## Література

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
2. Ben-Sasson E., Chiesa A., Tromer E., Virza M. Scalable Zero Knowledge via Cycles of Elliptic Curves. 2014.
3. Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. 2015.

### **ОБМЕЖЕННЯ ЗАХИСТУ ВЕБ-ДОДАТКІВ ЗА ДОПОМОГОЮ WAF: ВАЖЛИВІСТЬ ІМІТАЦІЇ ДІЙ ПОТЕНЦІЙНОГО ЗЛОВМИСНИКА ДЛЯ ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСНОСТІ ЗАХИСТУ**

**Щербаненко Г. О.**

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

Веб-додатки мають критичне значення у сучасному інформаційному середовищі для бізнесу, освіти, державних установ та повсякденного життя людей, забезпечуючи доступ до даних, автоматизацію процесів та взаємодію користувачів через Інтернет. Збільшення з року в рік кількості та складності кібератак на веб-додатки вимагає застосування комплексного підходу для забезпечення їх захисту. У цій статті розглядається питання обмежень у захисті веб-додатків за допомогою технологій Web Application Firewall (WAF) та питання важливості імітації дій потенційного зловмисника з метою оцінки реальної захищеності веб-додатків від кібератак.

Web Application Firewall (WAF) є однією з найбільш поширених технологій що використовується для захисту веб-додатків. Використання WAF спрямоване на блокування шкідливих запитів та запобігання атакам. WAF застосовується для моніторингу, аналізу та блокування вхідного HTTP/HTTPS трафіку відповідно до встановлених правил [1]. Відповідно до налаштованих

правил, WAF здатний виявляти та блокувати атаки зловмисників, спрямовані на реалізацію загроз для веб-додатків, в першу чергу тих що створюють найбільші ризики – наприклад, атак ін'єкцій, які належать до категорії найбільш поширених ризиків для веб-додатків згідно рейтингу OWASP Top 10 [2].

Однак використання WAF не гарантує повного захисту. Практичний досвід свідчить, що навіть коректно налаштований WAF має велику кількість обмежень, які не дозволяють забезпечити комплексний захист для веб-додатків. В першу чергу, обмеження стосуються можливостей WAF при забезпеченні захисту від атак на логіку роботи веб-додатків. Також, правилами WAF неможливо захиститись від більшості атак спрямованих на механізми аутентифікації та авторизації. І навіть у випадку атак ін'єкцій - зловмисники постійно вдосконалюють свої атаки, що дозволяє їм обходити правила WAF спрямовані на виявлення ін'єкцій, шляхом використання різних технік обфускації.

Обмеження захисту веб-додатків за допомогою WAF підкреслює необхідність впровадження багаторівневого підходу до захисту. Одним з підходів що демонструє високий рівень ефективності є проведення тестувань на проникнення для веб-додатків, іншими словами - імітація дій потенційного зловмисника з метою оцінки захищеності об'єкту тестування.

Імітація дій зловмисника – це метод, при якому спеціалісти з кібербезпеки відтворюють сценарії атак, характерні для реальних зловмисників, з метою оцінки ефективності захисних механізмів веб-додатків [3]. Такий підхід, який часто також називають тестуванням на проникнення або пентестом, дозволяє виявляти вразливості та проблеми безпеки до того, як вони будуть знайдені та проєксплуатовані зловмисником.

При проведенні тестування на проникнення, спеціалісти «команди нападу» застосовують ті ж інструменти та техніки, що зазвичай використовують реальні зловмисники. Цей процес дозволяє виявляти не тільки безпосередньо вразливості у цільових системах, а й виявляти недоліки у налаштування систем захисту, у тому числі WAF, таким чином підсвічуючи для спеціалістів «команди

захисту» сліпі зони, які не покриваються стандартними правилами моніторингу та фільтрації. Такий підхід є корисним для формування об'єктивної та комплексної картини поточного рівню захищеності цільової системи.

Як фахівець з комерційним досвідом проведення тестувань на проникнення, я неодноразово стикався у своїй практиці з обмеженістю WAF при забезпеченні захисту веб-додатків. Нижче наведено узагальнений опис двох прикладів з моєї реальної практики тестування веб-додатків, коли надмірна надія власників веб-додатків на WAF, дозволила виявити вразливості, експлуатація яких зловмисником могла б призвести до критичних наслідків.

Приклад перший. Організація «А» мала веб-додаток, який використовується великою кількістю користувачів. Оскільки цей веб-додаток є критичним для реалізації бізнес потреб організації, його було захищено WAF. Однак, спеціалістами організації не було враховано особливості архітектури веб-додатка, а саме – використання окремого домену для обробки запитів до API. Як наслідок, захист WAF було забезпечено тільки для «основного» домену який використовується для надання користувачам доступу до візуального інтерфейсу (статичного контенту), у той час як інший домен, через який було реалізовано API веб-додатку (динамічна взаємодія) залишився незахищеним. Це дозволило під час проведення тестування на проникнення вільно досліджувати динамічну частину веб-додатка, що в кінцевому підсумку дозволило виявити декілька критичних вразливостей, експлуатація яких у ланцюжку дозволила отримати доступ до адміністративної панелі веб-додатка та доступу до локальної системи на якій цей веб-додаток було розгорнуто. Якби атаку провели реальні зловмисники, це призвело б до непоправних наслідків та значних бізнес-втрат.

Приклад другий. Організації «Б» було відомо, що на їх зовнішньому периметрі знаходиться веб-додаток що використовує застаріле програмне забезпечення, для якого існують відомі вразливості, у тому числі критичного рівня. Однак, організація прийняла рішення замість того щоб оновити програмне забезпечення, що було для неї проблемою, захистити веб-додаток за

допомогою WAF. Первинні перевірки, проведені недостатньо кваліфікованими спеціалістами організації, не виявили можливості обходу захисту WAF. Однак під час проведення тестування на проникнення більш кваліфікованими спеціалістами сторонньої організації, одну з критичних вразливостей було проексплуатовано, не дивлячись на наявний захист WAF. Для обходу захисту WAF було застосовано техніки обфускації зловмисного корисного навантаження. Проведення атаки потребувало більше часу, однак врешті решт – критична вразливість була проексплуатована і як результат, було отримано віддалене виконання коду на вразливій системі, що призвело до її повної компрометації.

Враховуючи обмеження WAF у забезпеченні захисту веб-додатків, критично важливим є впровадження багаторівневого підходу до кібербезпеки. Імітація дій реального зловмисника, шляхом проведення тестування на проникнення, відіграє ключову роль у цьому процесі. Реальні випадки доводять, що надмірна довіра до WAF може залишати критичні вразливості відкритими для експлуатації зловмисниками. Таким чином, для досягнення високого рівню захищеності веб-додатків у сучасному кіберпросторі важливо забезпечувати комплексний підхід.

## Література

1. What is penetration testing. *CLOUDFLARE*. URL: <https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/>.
2. Top 10 Web Application Security Risks. *OWASP*. URL: <https://owasp.org/www-project-top-ten/>.
3. Web application firewall (WAF). *Techtarget*. URL: <https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF>.

# МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПРОВЕДЕННЯ ЕЛЕКТРОННИХ ГОЛОСУВАНЬ

**Іщук М. О., Шевченко С. М.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному цифровому середовищі забезпечення прозорості, безпеки та доступності виборчих процесів є важливим аспектом демократичного суспільства. Традиційні методи голосування часто стикаються з проблемами, такими як підробка бюлетенів, людський фактор, низька довіра до підрахунку голосів та складність верифікації результатів.

Інноваційні підходи, зокрема використання блокчейн-технологій, дозволяють значно підвищити довіру до виборчих процесів, забезпечуючи прозорість, незмінність результатів та анонімність голосуючих. Блокчейн-голосування усуває необхідність у посередниках та централізованих органах, що зменшує ризики маніпуляцій та фальсифікацій.

Технологія Blockchain — це децентралізована та розподілена система цифрової книги, яка записує транзакції через мережу комп'ютерів таким чином, що записані транзакції не можуть бути змінені заднім числом, що робить її надзвичайно безпечною та прозорою [1]. Замість того, щоб мати центральний орган, який контролює інформацію, вона розподіляється через мережу комп'ютерів. Кожна транзакція об'єднується в «блок» і додається до ланцюжка попередніх блоків, утворюючи хронологічний і незмінний запис [2]. На рис 1 представлено архітектуру системи голосування на основі блокчейн, яка включає реєстрацію виборців, автентифікацію, голосування та підрахунок голосів [3]. На кроці 1 виборці повинні зареєструватися, надавши свій ідентифікаційний номер та інші облікові дані; блок буде створено проти запису виборця, а приватний і відкритий ключі будуть призначені цьому конкретному виборцю. На кроці 2 система додає виборця до списку на основі конкретного



## 2.Доступність.

-Голосування може здійснюватися дистанційно через інтернет, що особливо корисно для громадян, які перебувають за кордоном або мають обмежену мобільність.

-Забезпечується можливість використання спеціальних функцій для людей з інвалідністю (екранні зчитувачі, голосове управління тощо).

-Зменшується залежність від фізичних виборчих дільниць, що може бути корисним у кризових ситуаціях, таких як пандемії або стихійні лиха.

## 3.Точність.

-Використання цифрових технологій зменшує ризик помилок, пов'язаних із неправильним заповненням бюлетенів або їх пошкодженням.

-Вбудовані механізми перевірки допомагають мінімізувати можливість фальсифікації голосів або подвійного голосування.

-Система може автоматично виявляти невалідні або підозрілі голоси, що підвищує загальну якість результатів виборів.

Попри всі переваги, впровадження систем електронного голосування породжує низку технічних, правових і соціальних питань [4-5]. Зокрема:

1) технічні збої та злами – існує ризик несправностей системи інтернет-голосування, що може призвести до викривлення реальних результатів виборів;

2) витік персональних даних – можливість зловмисного використання даних виборців у корисливих цілях;

3) порушення таємниці голосування – електронні вибори вимагають авторизації, що може поставити під загрозу анонімність виборця;

4) ризик повторного голосування – цифрові технології не забезпечують повної анонімності через необхідність збереження унікальних ключів, що може дозволити повторне голосування;

5) проблеми ідентифікації виборця – встановлення особи виборця через інтернет викликає сумніви, оскільки навіть електронно-цифрові підписи

можуть бути підроблені, а їх використання є дороговартісним для багатьох країн.

Метою даного проєкту є розробка веб-сайту для проведення електронних голосувань з використанням TypeScript та блокчейну, що дозволить користувачам безпечно та зручно брати участь у виборах або опитуваннях. У рамках роботи буде проаналізовано існуючі системи електронного голосування, обґрунтовано вибір технологій та реалізовано функціональний прототип, що забезпечить безпеку, надійність та масштабованість.

### Література

1. Ohize, H.O., Onumanyi, A.J., Umar, B.U. *et al.* Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges. *Cluster Comput* 28, 132 (2025). <https://doi.org/10.1007/s10586-024-04709-8>
2. M. Rifat Hossain, F. A. Nirob, A. Islam, T. M. Rakin and M. Al-Amin, "A Comprehensive Analysis of Blockchain Technology and Consensus Protocols Across Multilayered Framework," in *IEEE Access*, vol. 12, pp. 63087-63129, 2024, doi: 10.1109/ACCESS.2024.3395536
3. Hassan, C.A., Hammad, M., Iqbal, J., Hussain, S., Ullah, S.S., Alsalman, H., Mosleh, M.A., & Arif, S.M. (2022). A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Sci. Program.*, 2022, 1383007:1-1383007:10.
4. Jafar U, Aziz MJA, Shukur Z. Blockchain for Electronic Voting System-Review and Open Research Challenges. *Sensors (Basel)*. 2021 Aug 31;21(17):5874. doi: 10.3390/s21175874.
5. Квітка С., Гусаревич Н. Застосування технології виборчого блокчейну в системі цифрового голосування. Аспекти публічного управління. 2022. Том 10. №2. С. 23-30. <https://doi.org/10.15421/152209>

# ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ

Каневецький М. О.

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

Засоби мережевої та операційної безпеки є ключовими елементами кіберзахисту організацій та окремих користувачів. Вони включають апаратні, програмні та організаційні заходи, що забезпечують захист від несанкціонованого доступу, атак, шкідливого програмного забезпечення та інших кіберзагроз. Ефективне поєднання цих засобів мінімізує ризики та підвищує стійкість систем до сучасних загроз [1].

Схема автентифікації за IEEE 802.1X (рис. 1) відображає:

- ◆ Новий пристрій (Supplicant) намагається підключитися до мережі.
- ◆ Комутатор (Authenticator) передає запит на сервер автентифікації (RADIUS).
- ◆ RADIUS-сервер перевіряє облікові дані та призначає користувача до VLAN-зони (Zone A або Zone B).
- ◆ У разі успішної автентифікації пристрій отримує доступ до своєї VLAN-зони, інакше доступ блокується.

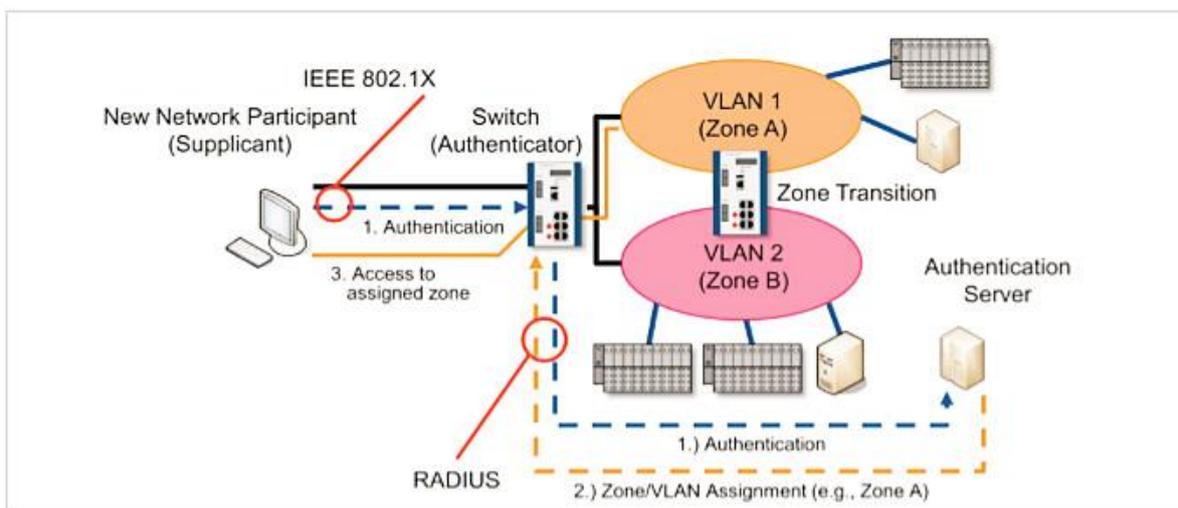


Рис. 1 Схема автентифікації за IEEE 802.1X [2]

Автентифікація базується на трьох основних факторах: те, що ви знаєте (пароль), те, що у вас є (ОТР-токен, смарт-карта) і біометричні дані (відбитки пальців, розпізнавання обличчя). Використання двох факторів одночасно (2FA) значно підвищує рівень безпеки, а багатофакторна автентифікація (MFA) забезпечує максимальний захист.

Застосування таких методів автентифікації допомагає захистити особисті дані, банківські рахунки та корпоративні системи від несанкціонованого доступу. Це критично важливо для онлайн-банкінгу, державних установ та будь-яких сервісів, що обробляють конфіденційну інформацію [3].

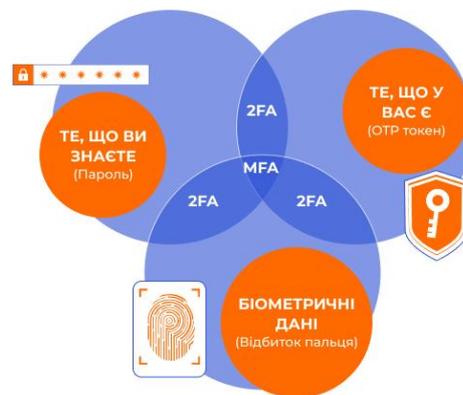


Рис. 2 Автентифікація, авторизація та ідентифікація

У наведеній таблиці "Засоби мережевої та операційної безпеки" представлені основні технології та методи захисту інформаційних систем.

Таблиця 1

### Засоби мережевої та операційної безпеки

Категорія	Засіб	Функція
Мережева безпека	Брандмауер (Firewall)	Фільтрація трафіку, блокування загроз
Мережева безпека	Системи запобігання вторгненням (IPS/IDS)	Виявлення та запобігання атакам
Мережева безпека	VPN (Віртуальна приватна мережа)	Захист даних під час передавання
Операційна безпека	Антивірусне ПЗ	Захист від вірусів та шкідливого ПЗ
Операційна безпека	Контроль доступу (RBAC, ACL)	Обмеження доступу до ресурсів
Операційна безпека	Оновлення та патч-менеджмент	Закриття вразливостей у ПО

Засоби безпеки забезпечують захист мереж і систем від загроз. Брандмауер (Firewall) створює бар'єр між внутрішньою мережею та зовнішніми загрозами, IPS/IDS аналізують трафік і блокують підозрілі дії, а VPN забезпечує безпечний зв'язок через Інтернет [4].

Антивірусне ПЗ захищає від шкідливих програм, контроль доступу обмежує права користувачів, а оновлення та патчі усувають вразливості. Використання цих технологій разом мінімізує ризики атак, витоку даних і несанкціонованого доступу, формуючи надійну систему кіберзахисту.

Впровадження комплексних засобів мережевої та операційної безпеки є необхідною умовою захисту інформаційних систем від кіберзагроз [5]. Поєднання брандмауерів, систем виявлення вторгнень, VPN, антивірусного ПЗ, контролю доступу та регулярного оновлення забезпечує надійний рівень безпеки. Це дозволяє мінімізувати ризики атак, витоку даних та несанкціонованого доступу, сприяючи стабільній та безпечній роботі інформаційної інфраструктури.

## Література

1. ЗАКОН УКРАЇНИ Про телекомунікації. Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155.
2. Natarajan Meghanathan. A Tutorial on Network Security: Attacks and Controls. Jackson State University. 2014.
3. ЗАКОН УКРАЇНИ Про основні засади забезпечення кібербезпеки України. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.
4. Aakanksha Chopra - Security Issues of Firewall. International Journal of P2P Network Trends and Technology (IJPTT). Volume 22 Number 1 January 2016
5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. Харків : Вид. ХНЕУ, 2013. 476 с.

# МЕТОДИКА ВИЯВЛЕННЯ DDoS-АТАК НА ОСНОВІ АЛГОРИТМУ ДЕНДРИТНИХ КЛІТИН

**Кузько А. В.**

Державний університет інформаційно-комунікаційних технологій

М.Київ, Україна

Метою даної статті є опис методу виявлення кіберзагроз, відомих під назвою DDoS-атак, сценаріями їх шкідливих дій та можливих наслідків для жертви. Пропонується дослідити виявлення таких атак на основі механізму імунної системи людини, і розробити приклад такої системи для майбутнього використання. Побудова такої моделі зумовлена високою різноманітністю та частими видозмінами DDoS-атак і, відповідно, необхідністю надійного захисту систем від них.

Розподілені атаки з відмовою в обслуговуванні (DDoS) є серйозними формами вторгнень у мережі. Вони переповнюють цільовий сервер великою кількістю зловмисних або неправильно сформованих пакетів, призводячи до його сповільнення або зупинки, що перешкоджає роботі легітимних користувачів.

Основним методом, який використовують зловмисники для організації відмови у доступі цільової машини залишається flood (англ. «потоп»), при якому порти цільової системи заповнюються великою кількістю пакетів. У свою чергу flood можна поділити за типами пакетів, які надсилаються:

- HTTP flood
- SYN flood
- TCP та UDP flood
- ICMP (Ping) Flood
- Ping of Death

Для виявлення подібних атак використовується велика кількість методів з різним принципом роботи. Одним із таких є алгоритм дендритних клітин

(Dendritic Cell Algorithm, скорочено DCA), що ґрунтується на роботі дендритних клітин імунної системи організмів ссавців. Даний алгоритм відповідає за класифікацію прийнятого мережевого трафіку на предмет зловмисності чи легітимності. У ході роботи системи модуль алгоритму приймає та аналізує вхідні дані і надає їм певні числові значення ( $>0$ ,  $<0$ ), покладаючись на виявлені сигнали/антигени. На основі цих значень формується статистика, з якої пізніше робиться висновок про легітимність чи шкідливість виявлених сигналів/антигенів, і, відповідно, вхідного трафіку.

Проте, варто зауважити, що можливості роботи даного алгоритму не обмежуються виявленням DDoS атак. Так, у роботі [2] група арабських дослідників запропонували використовувати алгоритм дендритних клітин (DCA) для виявлення існування одного DDoS-бота на скомпрометованій хост-машині. У цьому випадку реалізація цього алгоритму дозволяє перевірити власні машини на предмет наявності «бота» у вашій системі.

Ще одним напрямком використання даного алгоритму стало виявлення кейлоггерів за його допомогою. Використання симуляції натискань та подальший аналіз алгоритмом дендритних клітин дозволяє швидше знаходити процес кейлоггера, запобігаючи витоків конфіденційних даних [3].

Алгоритм дендритних клітин (DCA) - популяційна система, в якій кожен агент представлений так званою дендритною клітиною. Кожна клітина має можливість комбінувати відносні пропорції вхідних сигналів для створення свого набору вихідних сигналів. Дендритні клітини – це один із типів клітин імунної системи ссавців, зокрема і людини. Їхня функція полягає у обробці антигенного (зовнішнього, інородного) матеріалу та презентування його іншим імунним клітинам. На цьому механізмі і заснована робота алгоритму дендритних клітин. На Рис. 1 показано порівняння біологічного механізму DC та алгоритму DCA.

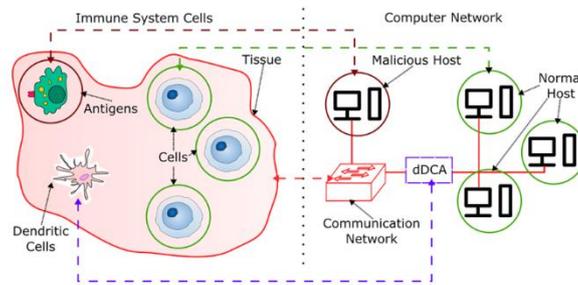


Рис. 1 Аналогія між біологічним дендритним клітковим алгоритмом та штучним імунним алгоритмом на основі dDCA[4]

Пропонована система складається з 3 частин (модулів): попередня обробка даних, виділення сигналу, та модуль DCA.

### 1. Модуль первинної обробки:

У цьому модулі з вхідного мережевого трафіку виділяються відповідні ознаки вхідного мережевого трафіку. Ці релевантні ознаки - це ознаки значення яких змінюються через наявність або відсутність аномальної активності. Отримані значення ознак потім нормалізуються, щоб масштабувати значення даних у кожній ознаці між 0 та 1.

### 2. Модуль екстракції антигену/сигналу:

Цей модуль відповідає за вилучення антигенів і сигналів із заданого нормалізованого вектора ознак у дискретному часовому просторі  $T = \{ 1, 2, \dots, t, \dots \}$ .

### 3. Модуль DCA:

Цей модуль відповідає за аналіз та присвоєння значення (зловмисний/легітимний) антигену, на основі вхідних даних. Вхідними даними для DCA є  $S(t)$  сигнали безпеки/небезпеки різних рівнів, що генеруються модулем екстракції антигену/сигналу. Вихідними, відповідно, – присвоєний кожному антигену статус.

### Робота системи:

DCA, що використовується в цій роботі, є детермінованою версією DCA. У dDCA сигнал небезпеки (D) та безпечний сигнал (S) застосовуються до рівняння обробки сигналу 1 і 2 для отримання вихідних концентрацій. У

рівнянні 1 вихідний сигнал "csm" використовується для визначення моменту, коли дендритна клітина перевищила свій термін експлуатації і, отже, готова до міграції. Вихідний сигнал "k" використовується для визначення контексту дендритної клітини. Якщо значення k більше 0, то такій клітині присвоюється значення контексту 1, що означає, що зібрані нею антигени можуть бути аномальними. В іншому випадку, якщо значення k менше 0, то клітині присвоюється контекст 0, що означає, що зібраний антиген, швидше за все, є нормальним. Після визначення контексту всіх мігруючих клітин обчислюється значення контексту зрілого антигену (MCAV) для всіх антигенів. Це значення використовується для отримання доступу до ступеня аномалії даного антигену. Тобто, антигени з MCAV, що перевищує встановлений поріг, позначаються як аномалія, в той час як антигени з MCAV нижче цього порогу позначаються як нормальні. MCAV антигену обчислюється шляхом діленням кількості антигенів типу  $\alpha$  (тих, що мають аномальний контекст) у мігруючих клітинах на загальну кількість антигену, представленого для антигену типу  $\alpha$  [1].

$$O1(csm) = S + D \quad (1)$$

$$O2(k) = D - 2S \quad (2)$$

Таким чином, після надання кожному антигену значення безпечний/небезпечний, дана система робить висновок щодо легітимності трафіку.

Використання алгоритму дендритних клітин (DCA) для виявлення DDoS-атак виявляється перспективним. DCA, який моделює імунну систему, дозволяє ефективно аналізувати мережевий трафік та виявляти аномалії, що допомагає забезпечити більш високий рівень захисту від подібних атак.

### Література

1. Obinna Igbe, Oluwaseyi Ajayi, and Tarek Saadawi Department of Electrical Engineering "Denial of Service Attack Detection using Dendritic Cell

Algorithm”, The 8th IEEE Annual Ubiquitous Computing, Electronics & Mobile, 2017

2. Y. Al-Hammadi, U. Aickelin, and J. Greensmith, “Dca for bot detection,” in Evolutionary Computation, 2008. CEC 2008. (IEEE World Congress on Computational Intelligence). IEEE Congress on. IEEE, 2008, pp. 1807–1816.

3. Шibaєв , Г., & Гальчинський , Л. (2023). Виявлення роботи кейлоггерів допомогою алгоритму дендритної клітинки з багаторазовою роздільною здатністю. Grail of Science, (30), pp. 173–176.

4. J. Greensmith, U. Aickelin, and G. Tedesco, “Information Fusion for Anomaly Detection with the Dendritic Cell Algorithm”, Information Fusion, Vol. 11, No. 1, 2010, pp.21–34.

## **МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ МАТЕРІАЛЬНО-РЕЧОВИМ КАНАЛОМ НА ОСНОВІ КОМПЛЕКСУВАННЯ ДАНИХ**

**Чабан Б. В.**

Державний університет інформаційно-комунікаційних технологій,  
м. Київ, Україна

На теперішній час у світовій науці розглядається достатньо багато методів технічного захисту інформації (ТЗІ). В той же час, протидія витоку інформації матеріально-речовим каналом залишається, здебільшого, поза увагою дослідників. У роботі [1] запропоновано метод, що дозволяє оцінити ймовірнісну захищеність об’єкта інформаційної діяльності (ОІД) від витоку матеріально-речовим каналом за часом проникнення зловмисника на ОІД.

Метою даного дослідження є розробка методу проектування системи ТЗІ на ОІД із заданими припустимими параметрами проникнення зловмисника на ОІД.

Для створення ефективної системи ТЗІ із завчасно заданими припустимими параметрами проникнення за спробами та часом необхідно дослідити розподілу ймовірності спроб злому захисту. У роботі [2] показано, що такий розподіл підпорядковується геометричному закону за умови незалежності параметра  $t_0$  від часу. У реальних умовах, на практиці, параметр  $t_0$ , який визначає властивість системи ТЗІ, залежить як від кількості спроб проникнення, так і від часу, при якому відбувається це проникнення.

Виходячи з цього, прийmemo, що  $t_0$  – параметр, що визначає властивості ТЗІ в часі і характеризує його надійність,  $t$  – поточний час, протягом якого здійснюється захист,  $p_0(t)$  – ймовірність захищеності ОІД у часі. Тоді можна визначити властивості ТЗІ через ризики захищеності у часі

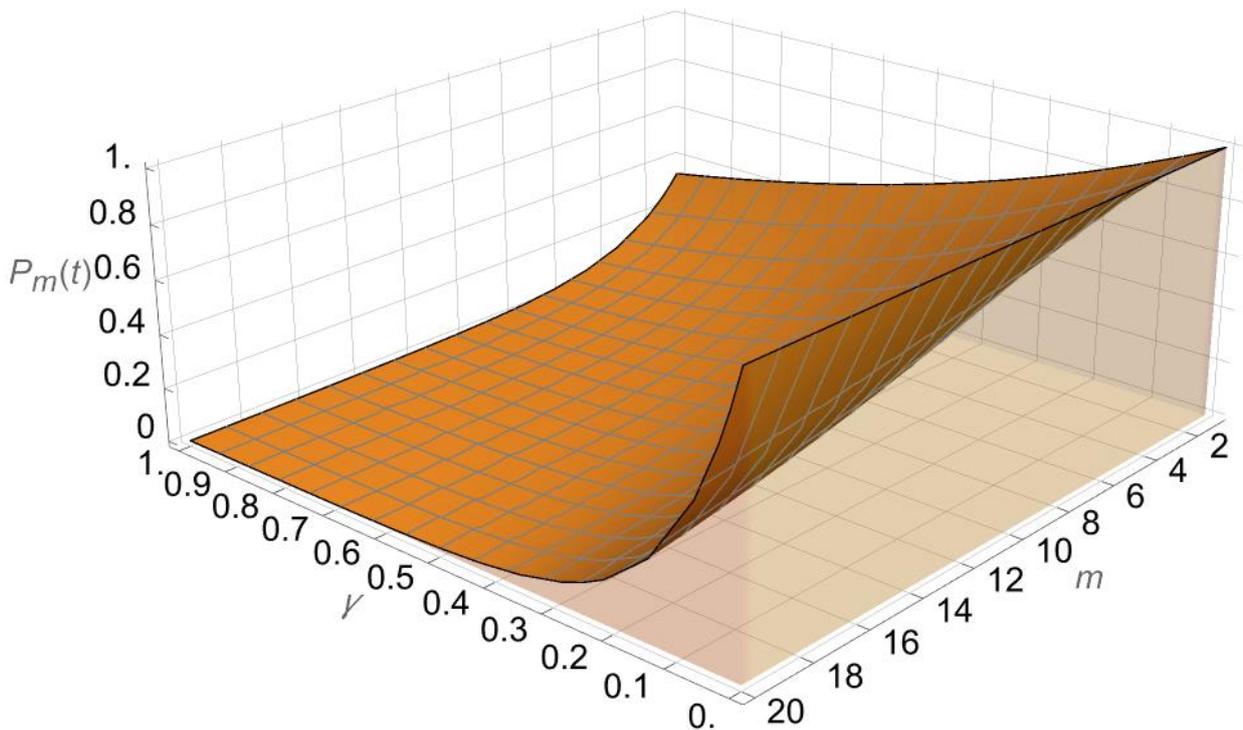
$$f(t) = (t_0 + t)p_0(t), \quad (1)$$

де  $f(t)$  – деяка функція, яка залежить від часу, має розмірність часу і визначає захисні властивості ТЗІ. У [2] показано, що щільність ймовірності проникнення на  $m$ -й спробі у часі може бути записана як

$$P_m(t) = \left[ \left( \frac{f(t)}{f(t) + t} \right)^{m-1} \cdot \left( \frac{t}{f(t) + t} \right) \right]^\gamma, \quad (2)$$

де  $t$  – поточна координата часу;  $m$  – поточна спроба проникнення на ОІД;  $\gamma$  – визначає ефективність проектованої системи ТЗІ.

Залежність  $P_m(t)$  наведено на рис. 1.



*Рис. 1 Залежність  $P_m(t)$  від кількості спроб  $m$  та ефективності проєктованого захисту  $\gamma$  при  $f(t)=20$ ,  $t=10$*

Як видно з цього рисунка, збільшення  $\gamma \rightarrow 1$  призводить до зниження  $P_m(t) \rightarrow 0$ . Як було зазначено у [2], якщо проникнення на цьому чи інших аналогічних об'єктах відбулося, то завжди  $\gamma < 1$ . При  $\gamma = 1$  проникнення можливе лише при  $m \rightarrow \infty$ , а при  $\gamma > 1$  проникнення взагалі неможливе і захищеність ОІД гарантується.

При проектуванні системи ТЗІ у якості початкових даних можна обрати або необхідний час, або спробу проникнення при відомій частоті спроб проникнення на ОІД, тобто закласти такі параметри проникнення, нижче яких проникнення не повинно бути. Якщо частота спроб проникнення невідома, можна закласти спробу  $m_{np}$  та час проникнення  $t_{np}$ .

Визначення виду функції  $f(t)$  з параметрами, властивими конкретній проєктованій системі захисту, дає змогу визначити ймовірнісну надійність технічного захисту інформації через спроби  $m$  і час  $t$  проникнень зловмисника

на ОІД. Також, за допомогою функції  $f(t)$  є можливість передбачити в якому напрямку йде прогнозований процес проникнення на ОІД, здійснювати його аналіз та розробити ефективні методи протидії такому проникненню.

### **Література**

1. Чабан, Б. В., & Котенко, А. М. Модель системи захисту інформації від витоку матеріально-речовим каналом на базі ланцюгів Маркова. Сучасний захист інформації. 2024. №4(60), Р. 46–52. URL: <https://doi.org/10.31673/2409-7292.2024.040005>.
2. Zhurilenko, B. Method of single technical information security system designing with probable reliability and given parameters of breaking. Ukrainian Scientific Journal of Information Security. 2014. №20(1), Р. 36–42. URL: <https://doi.org/10.18372/2225-5036.20.6572>.

## **РОЗРОБКА БЛОКЧЕЙН-РІШЕННЯ ДЛЯ БЕЗПЕЧНОЇ ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ**

**Юхнич Д. В.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному цифровому середовищі, де обсяг обробки конфіденційних даних стрімко зростає, забезпечення їх безпеки стає критично важливим завданням. Розробка блокчейн-рішення для безпечної передачі конфіденційних даних ґрунтується на використанні децентралізованої архітектури, що гарантує незмінність записів, автентичність транзакцій та стійкість до несанкціонованих змін.

Блокчейн – система децентралізованої обробки інформації, в якій рішення про обробку приймається за результатами голосування більшості учасників системи в ході виконання протоколу консенсусу.[6]

Ця технологія знаходить широке застосування у таких галузях:

1. Фінансовий сектор. Блокчейн використовується у криптовалютах (Bitcoin, Ethereum) та децентралізованих фінансових платформах (DeFi), що дозволяє здійснювати операції без посередників.

2. Управління ланцюгами поставок. Технологія забезпечує відстеження продукції та гарантує її якість. Наприклад, Walmart застосовує блокчейн для контролю якості харчових продуктів, а TradeLens – для оптимізації логістичних процесів.

3. Охорона здоров'я. Блокчейн дозволяє безпечно зберігати медичні записи та контролювати походження ліків, що допомагає запобігти підробкам і зберегти конфіденційність даних пацієнтів.

4. Державне управління. Електронне голосування та ведення реєстрів нерухомості на базі блокчейну підвищують прозорість процесів і знижують ризик фальсифікацій.

5. Цифрова ідентичність. Системи автентифікації, як-от uPort або Civic, використовують блокчейн для надання користувачам контролю над власними даними та забезпечення їх безпечного зберігання.

Блокчейн формує ланцюг блоків, де кожен блок містить хеш (цифровий підпис) попереднього. Це означає, що будь-яка спроба змінити дані в одному з блоків потребуватиме зміни усіх наступних, що практично не здійснено через високі обчислювальні витрати та необхідність погодження більшості вузлів мережі.[1]

Зв'язок між блоками гарантує, що навіть мінімальна зміна одних даних порушить цілісність усього ланцюга. Мережа перевіряє послідовність блоків, тому навіть спроба змінити старий блок буде виявлена.

Криптографічні алгоритми забезпечують конфіденційність та цілісність даних. За допомогою симетричного або асиметричного шифрування дані

перетворюються в незрозумілий для зломисників формат, що гарантує їхню безпеку під час передачі.[3]

Розподілена мережа забезпечує збереження інформації не централізовано, а на великій кількості вузлів. Кожен вузол мережі має копію всього ланцюга блоків, що робить атаки менш ефективними. Навіть якщо окремі вузли виходять з ладу або зазнають атак, мережа продовжує працювати, оскільки інші вузли зберігають дані. Крім того, кожен учасник має можливість перевірити історію транзакцій, що забезпечує додатковий рівень контролю.[2]

Консенсусні алгоритми забезпечують узгодженість даних у мережі. Всі вузли мають спільно погодитись із правильністю транзакцій, що запобігає шахрайству та гарантує достовірність інформації.[4]

Proof of Work (PoW) працює таким чином: кожен вузол (претендент на формування блоку) вирішує хеш-загадку, підбравши значення nonce (один з атрибутів блоку) так, щоб хеш усього блоку (який включає список транзакцій, хеш попереднього блоку та саме значення nonce) отримав потрібне значення, визначене кількістю нулів на початку. Якщо множина можливих значень складає лише 1% від загального простору, доведеться спробувати близько 100 значень, перш ніж досягти успіху. Саме тому вузли системи постійно обраховують значення nonce у сформованих блоках для отримання винагороди. Таким чином, ніхто не обирає формувача блоку, що робить систему криптовалюти децентралізованою.

Proof-of-Stake (PoS) Алгоритм працює за принципом: мережа довіряє валідатору, який володіє значною сумою у відповідній локальній валюті. Причому чим більша його частка (stake) у загальній сумі, тим вищими є його шанси на генерацію наступного блоку (й відповідно, отримання нагороди). У протоколі PoW нагороду отримують учасники, які вирішували криптографічні головоломки, щоб перевіряти транзакції та створювати нові блоки. У блокчейнах, що базуються на PoS вага голосів кожного валідатора залежить від розміру його частки. Значні переваги PoS включають: порівняно високу швидкість та енергоефективність. Замість того, щоб конкурувати з іншими,

майнери мережі закладають, ніби в ломбард, свої криптоактиви і чекають на випадкове обрання для валідації блокчейну. Валідатор – це учасник блокчейн-мережі, який бере участь у процесі консенсусу, перевіряє транзакції та додає нові блоки до ланцюга.

Отже, блокчейн-технології надають потужні інструменти для забезпечення безпеки, прозорості та незмінності даних у цифровому середовищі. Завдяки використанню децентралізованої архітектури, криптографічних методів та консенсусних алгоритмів, блокчейн забезпечує захист конфіденційної інформації, знижуючи ризики шахрайства і несанкціонованих змін.

### Література

1. Іванов, П. О., Коваль, А. В. Блокчейн-технології: основи розподілених реєстрів та їх застосування. Київ. *Наукова думка*. 2018. С. 25–33.
2. Мельник, С. П. Впровадження блокчейн-рішень у державному управлінні. Харків: *Харківський національний університет*. 2019. С. 30–38.
3. Сидоренко, О. Г. Криптовалюти та блокчейн: від теорії до практики. Львів: *Літопис*. 2020. С. 45–52.
4. Петрова, Н. В. Інновації у фінансовій сфері: блокчейн-технології в Україні. Одеса: *Одеський економічний університет*. 2021. С. 60–67.
5. Бондаренко, М. І. Блокчейн в цифровій економіці України: перспективи та виклики. Дніпро: *Економіка України*. 2022. С. 75–83.
6. Ковальчук Л.В., Кудін А.М., Кучинська Н.В. Вступ до технології блокчейн та криптовалют. Київ. *КПІ ім. Ігоря Сікорського*. 2022. С. 8–23.

## **СЕКЦІЯ 5. ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ**

### **ZERO TRUST ТА SOC: СИМБІОЗ СТРАТЕГІЙ ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВ**

**Юнак Д. О.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасне кіберсередовище характеризується зростанням складності атак та використанням новітніх методів обходу традиційних засобів захисту. Традиційні підходи до кібербезпеки, засновані на периметровому захисті, втрачають ефективність, що змушує підприємства шукати нові методи забезпечення безпеки. Одним із найефективніших сучасних підходів є модель Zero Trust, що передбачає принципи «ніколи не довіряй, завжди перевіряй». Інтеграція цього підходу з Security Operations Center (SOC) дозволяє забезпечити безперервний моніторинг, швидке реагування на інциденти та проактивний захист корпоративних інфраструктур.

Сьогодні кіберзлочинці використовують складні тактики, включаючи соціальну інженерію, атаки зсередини та експлуатацію вразливостей програмного забезпечення. Організації повинні змінити підхід до безпеки, впроваджуючи комплексні моделі контролю доступу та моніторингу. Zero Trust та SOC формують потужний дует, який сприяє створенню адаптивної архітектури безпеки, що здатна протистояти сучасним загрозам [1].

Модель Zero Trust базується на кількох ключових принципах, які спрямовані на мінімізацію ризиків та запобігання несанкціонованому доступу. Основним аспектом є мінімізація довіри: доступ до ресурсів надається за принципом найменших привілеїв (Least Privilege Access), що значно знижує

ризик компрометації системи. Користувачі та пристрої проходять ретельну перевірку перед отриманням дозволу на доступ до корпоративних даних.

Багатофакторна автентифікація (MFA) є обов'язковим компонентом Zero Trust. Вона забезпечує багаторівневий захист, що вимагає додаткових підтверджень особи, таких як одноразові паролі, біометричні дані або апаратні токени. Це значно ускладнює можливість атакуючих отримати доступ до системи, навіть якщо облікові дані були скомпрометовані.

Мікросегментація відіграє важливу роль у забезпеченні безпеки корпоративної мережі. Вона дозволяє розділити інфраструктуру на ізольовані сегменти, обмежуючи можливість бічного переміщення атакуючих у разі компрометації одного з них. Це мінімізує потенційні наслідки кіберінцидентів і дозволяє контролювати кожен рівень мережі окремо [2].

Контроль доступу в режимі реального часу є ще одним критично важливим аспектом Zero Trust. Постійний моніторинг дій користувачів та пристроїв дозволяє швидко виявляти аномалії та потенційні загрози. Використання поведінкової аналітики допомагає адаптивно оцінювати рівень довіри до кожного запиту на доступ та своєчасно блокувати потенційно небезпечні дії.

Моніторинг і аналітика є невід'ємною частиною Zero Trust. Використання SIEM-систем (Security Information and Event Management) та інших інструментів дозволяє в режимі реального часу аналізувати величезні обсяги даних, що надходять з різних джерел, та ідентифікувати потенційні загрози. Постійний аналіз та кореляція подій дозволяють підвищити ефективність реагування на інциденти та запобігати атакам ще до їх активної фази.

Інтеграція цих принципів у рамках Zero Trust дозволяє створити комплексну стратегію кібербезпеки, яка мінімізує ризики атак та забезпечує надійний захист корпоративної інфраструктури. У поєднанні з можливостями SOC ця модель стає ще більш ефективною, створюючи багаторівневий механізм протидії сучасним кіберзагрозам.

Security Operations Center (SOC) відіграє центральну роль у впровадженні та підтримці Zero Trust, оскільки забезпечує постійний контроль над усіма аспектами кібербезпеки. SOC функціонує як командний центр, що здійснює цілодобовий моніторинг, аналіз та реагування на загрози [3]. Використання SIEM-систем дозволяє не лише агрегувати логи з різних джерел, а й корелювати події, що допомагає виявляти складні атаки на ранніх стадіях.

Реагування на інциденти в рамках SOC включає як автоматизовані процеси, так і експертний аналіз. Застосування SOAR-платформ (Security Orchestration, Automation and Response) дозволяє значно прискорити реагування, усуваючи рутинні завдання та надаючи аналітикам більше часу для вирішення складних кейсів. Автоматизація процесів дає змогу швидко нейтралізувати загрози, мінімізуючи потенційний вплив атак на бізнес-процеси.

Кореляція даних є ще одним важливим аспектом роботи SOC. Вона полягає у поєднанні інформації з різних систем безпеки – від антивірусних програм до мережесих моніторингових засобів – для створення єдиної картини кіберзагроз. Завдяки цьому SOC може не лише реагувати на вже відомі атаки, а й виявляти нові, які ще не були зафіксовані у стандартних базах загроз.

Проактивний пошук загроз (Threat Hunting) є важливою частиною діяльності SOC, що дозволяє ідентифікувати приховані атаки, які не виявляються традиційними методами. Використовуючи аналіз поведінки користувачів, машинне навчання та сучасні аналітичні платформи, SOC може прогнозувати потенційні атаки та усувати їх ще до активної експлуатації зловмисниками [4].

Поєднання Zero Trust та SOC є потужною стратегією для забезпечення кіберстійкості підприємств. Інтеграція цих підходів дозволяє не лише ефективно реагувати на інциденти, а й запобігати їм, мінімізуючи ризики атак. У майбутньому розвиток штучного інтелекту, поведінкової аналітики та автоматизованих систем безпеки ще більше посилить ефективність цієї моделі, роблячи її стандартом у сфері корпоративної кібербезпеки.

## Література

1. Zero Trust security. What is a Zero Trust network?. *Cloudflare*. URL: <https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/>
2. What is zero trust? *IBM*. URL: <https://www.ibm.com/think/topics/zero-trust>
3. Building the Zero Trust Enterprise: The Role of the SOC. *Palo Alto*. URL: <https://www.paloaltonetworks.com/blog/2022/02/the-role-of-the-soc/>
4. SOC and Zero Trust: Enabling Comprehensive, Layered Security. *MCS*. URL: <https://www.microminder.com/blog/soc-and-zero-trust>

## НЕЙРОМЕРЕЖІ ПРОТИ ХАКЕРІВ: ЯК ШТУЧНИЙ ІНТЕЛЕКТ БОРЕТЬСЯ З КІБЕРЗАГРОЗАМИ НА ПЕРЕДОВІЙ

**Коврига М. В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Нейронні мережі, як підмножина штучного інтелекту (ШІ), знаходяться на передовій операцій з кібербезпеки, пропонуючи складні механізми для виявлення, протидії та пом'якшення кіберзагроз. Їх роль у кіберзахисті зростає зі збільшенням складності цифрових атак, що вимагає автономних і адаптивних заходів безпеки.

Ключовим застосуванням нейронних мереж у кібербезпеці є їхня здатність виявляти аномалії та прогнозувати кіберзагрози в режимі реального часу. Використовуючи моделі глибокого навчання, навчені на великих масивах даних мережевого трафіку, нейромережі можуть виявляти патерни, пов'язані зі зловмисною діяльністю. Ця здатність дозволяє системам безпеки вийти за рамки статичних методів виявлення на основі сигнатур і динамічно розпізнавати загрози «нульового дня» та сучасні постійні загрози (APT)[1].

Одним з помітних досягнень є інтеграція нейронних мереж у системи виявлення та реагування на кінцеві точки (EDR). Ці рішення безпеки на основі штучного інтелекту аналізують поведінкові дані з кінцевих точок, виявляючи відхилення, які вказують на потенційну загрозу. На відміну від традиційних заходів безпеки, які покладаються на заздалегідь визначені правила, нейронні мережі уможливають адаптивні стратегії захисту, постійно навчаючись на нових векторах атак.

Ще однією важливою функцією нейронних мереж є їхня здатність посилювати стратегії кібербезпеки, засновані на обмані. Технологія обману використовує згенеровані штучним інтелектом приманки для введення в оману та виявлення зловмисників у мережі. Нейронні мережі оптимізують цей процес, динамічно коригуючи розміщення і поведінку систем приманок на основі шаблонів атак, що змінюються, тим самим підвищуючи ефективність виявлення вторгнень і збору розвідданих про загрози.

Ворожий ШІ створює як можливості, так і виклики для кібербезпеки. В той час як ШІ посилює оборонні можливості, зловмисники використовують нейронні мережі для створення більш складних кібератак. Генеративні ворожі мережі (GAN) використовуються для створення варіантів шкідливого програмного забезпечення, які неможливо виявити, і обходу механізмів безпеки на основі ШІ. Крім того, автоматизовані інструменти тестування на проникнення на основі ШІ можуть виявляти вразливості системи в безпрецедентних масштабах, демонструючи як оборонні, так і наступальні наслідки застосування ШІ в кібервійні [2].

Незважаючи на цей прогрес, нейронні мережі створюють нові ризики, особливо у змагальному машинному навчанні. Зловмисники можуть маніпулювати моделями ШІ за допомогою отруєння даних, атак ухилення та методів інверсії моделей, що потенційно підриває захист кібербезпеки. Це зумовлює необхідність розробки надійних заходів безпеки ШІ, таких як пояснюваний ШІ (XAI) і федеративне навчання, щоб підвищити стійкість і прозорість моделей.

Геополітичний ландшафт також впливає на розгортання рішень для кібербезпеки на основі ШІ. Провідні країни інвестують в ШІ, щоб захистити цифрову інфраструктуру і зберегти стратегічну перевагу. Однак глобальна гонка за кібербезпеку з використанням ШІ посилює занепокоєння щодо розповсюдження кіберзброї, прогалин у регулюванні та етичних міркувань, пов'язаних з автономними кіберопераціями [3].

Нейронні мережі є ключовим досягненням у сфері кібербезпеки, оскільки вони надають розширені можливості виявлення, реагування і обману. Проте подвійний характер ШІ підкреслює необхідність постійних досліджень у сфері захисту систем безпеки, керованих ШІ, від нових загроз.

### Література

1. J. M. Padrón, Á. Ojeda-Castro. CYBERWARFARE: ARTIFICIAL INTELLIGENCE IN THE FRONTLINES OF COMBAT. *International Journal of Information Research and Review*. Vol. 04, Is. 06. 2017. P. 4208-4212. URL: [https://www.researchgate.net/publication/318130617\\_CYBERWARFARE\\_ARTIFICIAL\\_INTELLIGENCE\\_IN\\_THE\\_FRONTLINES\\_OF\\_COMBAT](https://www.researchgate.net/publication/318130617_CYBERWARFARE_ARTIFICIAL_INTELLIGENCE_IN_THE_FRONTLINES_OF_COMBAT)
2. Chakraborty A., Biswas A., Khan A. K. Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *Artificial Intelligence for Societal Issues*. Cham, 2023. P. 3–25. URL: [https://doi.org/10.1007/978-3-031-12419-8\\_1](https://doi.org/10.1007/978-3-031-12419-8_1)
3. Malicious Uses and Abuses of Artificial Intelligence. *United Nations Interregional Crime and Justice Research Institute (UNICRI)*. 2020. URL: <https://unicri.org/sites/default/files/2020-11/AI%20MLC.pdf>

## АНАЛІЗ МЕТОДІВ ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТЕЙ ЦЕНТРУ СЕРТИФІКАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

**Рабчун Д. І., к.т.н., доц., Скрипка О. В.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Центр сертифікації відіграє ключову роль у забезпеченні аутентифікації та шифрування мережевих комунікацій. Проте, як і будь-яка інша технологія, центр сертифікації має свої вразливості, які можуть бути використані зловмисниками для компрометації мережі. Метою цієї роботи є аналіз методів експлуатації вразливостей центру сертифікації та їх вплив на безпеку корпоративних мереж, зокрема Active Directory.

У середовищі Active Directory використовуються сервіси Active Directory Certificate Services (ADCS), де центр сертифікації відповідає за видачу, управління та відкликання цифрових сертифікатів, які використовуються для аутентифікації користувачів та комп'ютерів [1], а також для виконання функцій криптографії (шифрування, цифровий підпис, тощо). Сертифікати забезпечують безпечну передачу даних та підтверджують ідентичність суб'єктів у мережі. Неналежні налаштування центру сертифікації та його шаблонів сертифікатів можуть дозволити зловмиснику виконувати різні вектори атаки такі як підвищення привілеїв, крадіжка та підробка сертифікатів, а також закріплення в мережі.

Вразливості для підвищення привілеїв (ESC) — це комплекс методів, який дозволяє зловживати цими вразливими конфігураціями, надаючи зловмисникам можливість підвищення привілеїв від звичайного користувача до адміністратора домену. На поточний момент існує близько п'ятнадцяти вразливостей ESC [2], які широко використовуються зловмисниками у своїх компаніях (рис. 1).

Name	Description	Target	Publication Date	Authors	Reqs. to fully check	Reqs. to exploit
ESC1	Abuse the Client Supplies Subject flag on the CT	ADCS Template	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC	(1) Basic Prerequisites (2) Client supplies subject
ESC2	Abuse the Any Purpose EKU on the CT	ADCS Template	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC	(1) Basic Prerequisites (2) Any Purpose EKU
ESC3	Abuse the CRA EKU on the CT	ADCS Template	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC	(1) Basic Prerequisites (2) Certificate Request Agent EKU
ESC4	Abuse write privs. over a CT to make it vulnerable	ADCS Template	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC	GenericAll / WriteProperties / WriteOwner / WriteDACL privileges over the CT
ESC5	Abuse excessive privs. to take control of the PKI system	ADCS as a whole	2021-06-17	[Will S. & Lee C.] @ SpecterOps Andy Robbins @ SpecterOps	Local admin on CA server LDAP on DC	Local admin on CA server to dump CA keys; or Having SYSTEM on a DC or other authorized principal to escalate to Enterprise Admin by creating a vulnerable cert. and publishing it in the CA
ESC6	Abuse the EDITF_ATTRIBUTESUBJECTALTNAME2 flag on the CA	ADCS CA	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC RPC on CA	(1) Basic Prerequisites (2) CA has the EDITF_ATTRIBUTESUBJECTALTNAME2 flag enabled on its EditFlags registry key
ESC7	Abuse sensitive privs. over a CA	ADCS CA	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC	(1) ManageCA privilege over the CA object (to escalate) or (2) ManageCertificates privilege over the CA object (to approve requests and "bypass" manager approval required)
ESC8	Abuse Web Enrollment with coercion and relaying	ADCS CA	2021-06-17	[Will S. & Lee C.] @ SpecterOps	LDAP on DC RPC on CA	(1) Web Enrollment is enabled on the CA (2) NTLM is enabled (3) EPA (Extended Protection for Authentication) disabled (4) A relaying vector is possible (target can reach relay port + relay can reach web enrollment port on the CA)
ESC9	Implicit cert mapping abuse on vulnerable CTs	ADCS Template	2022-08-14	Oliver Lyak @ IFCR	LDAP on DC	(1) Client Auth EKU on the CT (2) CT_FLAG_NO_SECURITY_EXTENSION enabled on the CT (3) GenericWrite over an account that can Enroll on the CT
ESC10	Implicit weak cert mapping abuse on vulnerable CAs	ADCS Template	2022-08-14	Oliver Lyak @ IFCR	Local admin on CA server	(1) The CertificateMappingMethods key contains the UPN bit flag (0x4) or the StrongCertificateBindingEnforcement key is set to 0 (2) GenericWrite over an account that can Enroll on the CT
ESC11	Abuse unsigned RPC with coercion and relaying	ADCS CA	2022-11-16	Sylvain Heimiger (SploitChy) @ Compass Security	LDAP on DC RPC on CA	(1) The IF_ENFORCEENCRYPTCERTREQUEST flag is disabled on the CA (2) NTLM is enabled (3) A relaying vector is possible (target can reach relay port + relay can reach RPC ports on the CA)
ESC12	Compromise the CA private key stored in YubiHSM2 using a low-privilege user	ADCS CA Server (YubiHSM2)	2023-10-06	Hans Knobloch @ Secorvo	Low-privilege shell on CA server	Low-privilege shell on CA server that stores its private key in a YubiHSM2
ESC13	Abuse msDS-OIDToGroupLink to inherit group privs	ADCS Template	2024-02-14	Jonas Knudsen @ SpecterOps	LDAP on DC	(1) Basic Prerequisites (2) Issuance Policy is configured on the CT (3) OID Group Link is set on the Issuance Policy (4) The referenced group has sensitive privileges
ESC14	Abuse weak explicit cert mapping / write privs. to altSecurityIdentities	ADCS Template	2024-02-28	Géraud de Drouas / Jean Marsault / Jonas Knudsen @ SpecterOps	LDAP on DC Local admin on CA server	(1) Basic Prerequisites (2) Lots of complex requirements 🤖
ESC15	Abuse EKU / Application Policies confusion in version 1 CTs	ADCS Template	2024-10-08	Justin Bollinger @ TrustedSec	LDAP on DC	(1) Published CT in version 1 (2) Low-privilege user has Enroll on the CT

Рис. 1. Перелік вразливостей центру сертифікації, що спрямовані на підвищення привілеїв

Більшість існуючих методів експлуатації описані в посібнику Certified Pre-Owned, розроблений компанією SpecterOps [3]. Найбільш поширеними вразливостями у корпоративних середовищах є ESC1 та ESC8.

Шаблон сертифіката з вразливістю ESC1 дозволяє користувачам з мінімальними привілеями виконувати запити до центру сертифікації на отримання сертифікату для будь-якого об'єкта домену, вказаного користувачем. Це означає, що будь-який користувач із правами реєстрації (Enrollment Rights) може запросити сертифікат для будь-якого облікового запису, наприклад адміністратора домену, попередньо вказавши в атрибуті subjectAltName (SAN) ім'я його облікового запису. Шаблони, вразливі до ESC1, мають такі конфігурації: Client Authentication: True, Enabled: True, Enrollee Supplies Subject: True, Requires Management Approval: False, Authorized Signatures Required: 0

Вразливість ESC8 полягає у наявності вразливих конфігурацій центру сертифікації. Якщо сервер центру сертифікації дозволяє проходження аутентифікації NTLM у веб-точці видачі сертифікатів без примусового підписання протоколу (HTTPS) або без використання функції Extended Protection for Authentication (EPA), він стає вразливим до ретрансляційних атак NTLM (наприклад PrinterBug та PetitPotam). Тобто, якщо зловмисник зможе змусити доменний акаунт пройти аутентифікацію на машині зловмисника (наприклад за допомогою NTLMrelay атаки), то він може передати облікові дані жертви до центру сертифікації, щоб отримати сертифікат від імені цієї жертви. Шаблон, указаний під час ретрансляційної атаки, має бути шаблоном, у якому обліковий запис жертви має дозвіл на реєстрацію (Enrollment Rights). Тому доволі часто обліковим записом жертви є контролер домену, який має дозвіл на реєстрацію в більшості стандартних шаблонів. Центр сертифікації, вразливий до ESC8, має наступні конфігурації: Web Enrollment: Enabled, Request Disposition: Issue.

Аналіз вищезазначених методів експлуатації вразливостей центру сертифікації підтверджує, що експлуатація цих вразливостей зловмисниками може призвести до компрометації домену Active Directory та спричинити суттєві збитки для організації. Це підкреслює необхідність ретельного налаштування центру сертифікації, постійного моніторингу шаблонів сертифікатів та їх використання, а також впровадження механізмів захисту для виявлення та протидії експлуатації вразливостей. Регулярний аудит конфігурацій центру сертифікації та усунення вразливостей дозволять значно знизити ризик компрометації корпоративної мережі через слабкі місця в ADCS.

## Література

1. What is Active Directory Certificate Services? URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview>

2. ADCS Attack Techniques Cheatsheet. URL: [https://docs.google.com/spreadsheets/d/1E5SDC5cwXWz36rPP\\_TXhhAvTvqz2RGnMYXieu4ZHx64](https://docs.google.com/spreadsheets/d/1E5SDC5cwXWz36rPP_TXhhAvTvqz2RGnMYXieu4ZHx64)

3. Certified Pre-Owned Guidance. URL: [https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified\\_Pre-Owned.pdf](https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf)

## **ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ**

**Делікатний В. А.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному цифровому середовищі кіберзагрози стають дедалі складнішими та небезпечнішими для бізнесу. Атаки на критичні бізнес-сервіси можуть призвести до значних фінансових втрат, репутаційних ризиків та витоку конфіденційної інформації. Тому питання забезпечення надійного захисту бізнес-інфраструктури та оперативного реагування на інциденти є вкрай актуальним. Серед найпоширеніших загроз для бізнесу варто виділити такі, як DDoS-атаки, що призводять до перевантаження серверів і відмови у наданні послуг [1]. Фішингові атаки є ще однією серйозною проблемою, оскільки вони використовують підроблені сайти чи електронні листи для викрадення облікових даних [2]. Особливу небезпеку становлять атаки на API, які дозволяють зловмисникам використовувати уразливості у веб-сервісах для отримання несанкціонованого доступу [3]. Також великою загрозою є експлойти у програмному забезпеченні, які дозволяють використовувати не виправлені вразливості для компрометації системи.

Захист бізнес-сервісів потребує комплексного підходу, що включає моніторинг трафіку та виявлення аномалій за допомогою SIEM-систем. Також

важливим є застосування IDS/IPS-рішень, які допомагають виявляти та запобігати вторгненням. Автоматизований аналіз загроз на основі XDR-рішень дозволяє ефективно аналізувати взаємопов'язані події безпеки. Важливу роль відіграє захист API шляхом впровадження механізмів аутентифікації та контролю запитів, таких як OAuth і JWT. Безпека хмарних сервісів також потребує особливої уваги, зокрема налаштування політик доступу, шифрування даних та контроль безпеки контейнеризації.

Для ефективної протидії атакам необхідно своєчасно виявляти інциденти шляхом аналізу логів та ідентифікації аномальної активності. Після виявлення загрози проводиться її оцінка, що дозволяє визначити рівень критичності ситуації. Наступним кроком є локалізація проблеми, що передбачає ізоляцію уражених систем з метою запобігання поширенню атаки. Усунення загрози передбачає оновлення політик безпеки та виправлення вразливостей. Завершальним етапом є аналіз події та вдосконалення існуючих механізмів безпеки для запобігання подібним інцидентам у майбутньому. Використання сучасних технологій дозволяє ефективно знаходити та виправляти уразливості. Одним із ключових інструментів є сканери вразливостей, такі як Nessus та OpenVAS, які дозволяють автоматично виявляти потенційні загрози. Аналіз журналів подій сприяє кореляції даних та виявленню підозрілих патернів у мережевій активності. Інтеграція DevSecOps-підходу забезпечує впровадження безпекових заходів ще на етапі розробки програмного забезпечення. Протидія кібератакам на бізнес-сервіси вимагає комплексного підходу, що включає превентивні заходи, постійний моніторинг та оперативне реагування на інциденти. Використання сучасних технологій кіберзахисту дозволяє зменшити ризики, підвищити стійкість інфраструктури та гарантувати безперервність бізнес-процесів.

## Література

1. Quantum Cryptography for Future Networks Security: A Systematic Review. *IEEE Xplore*. URL: <https://ieeexplore.ieee.org/abstract/document/10763508>

2. AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance. SSRN. URL: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=5029406](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5029406)

3. AI sentry: reinventing cybersecurity through intelligent threat detection URL: <https://ephijs.com/index.php/SE/article/view/211>.

## **ТЕХНОЛОГІЇ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ЯК СПОСІБ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРОТИДІЇ КІБЕРАТАКАМ НА СИСТЕМИ КОМПАНІЇ**

**Журавель А. В.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

У сучасному цифровому середовищі персональні дані користувачів стають основною мішенню для кіберзлочинців. Одним із найефективніших методів захисту є використання багатофакторної автентифікації (MFA). Ця технологія базується на застосуванні кількох рівнів перевірки особи, що значно ускладнює несанкціонований доступ до інформаційних ресурсів[1].

Основні фактори автентифікації включають: 1) знання (паролі, PIN-коди); 2) володіння (смартфони, апаратні токени); 3) біометричні дані (відбитки пальців, розпізнавання обличчя). Поєднання цих механізмів підвищує рівень безпеки, оскільки компрометація одного з факторів не дає змоги отримати доступ без інших елементів перевірки [2,3].

Управління ризиками в контексті впровадження MFA включає оцінку можливих векторів атак, зокрема фішинг, перехоплення одноразових паролів та компрометацію біометричних даних. Запобігання таким загрозам можливе завдяки використанню криптографічних алгоритмів, безпечних каналів зв'язку

та адаптивної автентифікації, яка аналізує поведінкові фактори користувачів [4,5].

MFA сприяє безперервності бізнесу, оскільки забезпечує надійний захист від атак на облікові записи співробітників, що знижує ймовірність витоку даних та фінансових втрат. Особливо важливе значення має інтеграція MFA у критично важливі бізнес-системи та сервіси віддаленого доступу [6]. Крім того, застосування MFA у поєднанні з політиками нульової довіри (Zero Trust) дозволяє мінімізувати внутрішні загрози та покращити контроль доступу до корпоративних ресурсів[7,8].

Популярні методи MFA включають використання одноразових паролів (OTP), push-сповіщень, програмних та апаратних токенів, а також біометричних технологій. Однак, слід враховувати виклики, пов'язані з впровадженням цих технологій, такі як користувацький досвід, технічна сумісність та потенційні вразливості.

Впровадження багатофакторної автентифікації має супроводжуватися політиками безпеки, навчанням користувачів та регулярним аудитом механізмів захисту. Лише комплексний підхід дає змогу мінімізувати ризики несанкціонованого доступу та забезпечити кіберстійкість організації. Додатково, організаціям рекомендується використовувати адаптивну автентифікацію, яка враховує контекст користувацьких дій та поведінкові характеристики для підвищення рівня безпеки.

### **Література**

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2020.
2. Bishop M. Computer Security: Art and Science. Addison-Wesley, 2018.
3. NIST Special Publication 800-63B: Digital Identity Guidelines. Authentication and Lifecycle Management, 2021.

4. Bonneau J., Herley C., Van Oorschot P., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // IEEE Symposium on Security and Privacy, 2012.
5. ENISA. Multi-Factor Authentication: Security Models and Key Considerations, 2022.
6. OWASP. Authentication Cheat Sheet. URL: [https://cheatsheetseries.owasp.org/cheatsheets/Authentication\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html).
7. Zero Trust Architecture. NIST Special Publication 800-207, 2020.
8. Microsoft Security Blog. The Importance of Multi-Factor Authentication. URL: <https://www.microsoft.com/security/blog/>.

## **ВИКОРИСТАННЯ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СУЧАСНИХ КІБЕРАТАКАХ: КЕЙС-ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ**

**Кравець С. В.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасний цифровий простір характеризується зростаючою загрозою кібератак, що базуються на методах соціальної інженерії. Незважаючи на розвиток технологій безпеки, людський фактор залишається основним вектором атак. Зловмисники використовують психологічні маніпуляції для отримання конфіденційної інформації, обходячи технічні заходи захисту.

Методи соціальної інженерії, такі як фішинг, вішинг, смішинг та бейтинг, широко застосовуються для компрометації користувачів та організацій. В умовах гібридної війни, економічної нестабільності та цифрової трансформації необхідно розробляти ефективні заходи захисту та підвищувати рівень кіберосвіти користувачів.

## Методи соціальної інженерії [1]

1. **Фішинг** – використання підроблених повідомлень, що імітують офіційні листи, з метою отримання облікових даних. Така атака може бути масштабною або цільовою, адаптованою під конкретну жертву.

2. **Вішинг** – телефонні атаки, під час яких зловмисники використовують соціальний тиск і психологічні прийоми для створення атмосфери терміновості, що змушує жертву розкрити конфіденційну інформацію. Набуває все більшої популярності, зважаючи на стрімкий розвиток нейромереж, що дає змогу підробляти голос та манеру розмови.

3. **Смішинг** – тип фішингу при якому використовуються SMS-повідомлення для викрадення даних або зараження пристроїв. Жертви часто не підозрюють про загрозу через звичку довіряти текстовим повідомленням.

4. **Бейтинг** – метод, при якому використовується «повідомлення-приманки» через заражені або фейкові програми. Вони змушують людину виконати певні дії і допомагають зловмиснику одержати інформацію.

## Методи захисту від соціальної інженерії

1. **Розробка політик безпеки** – розробка правил поведження з інформацією та відповідальності співробітників, правильного використання робочих пристроїв, реагування/повідомлення про підозрілі запити.

2. **Багатофакторна автентифікація** – впровадження стратегії використання паролів, навчання персоналу, вирішення проблем пов'язаних зі зберіганням складних паролів, використання біометричної ідентифікації, ID токенів.

3. **Контроль користувацької активності** – аналіз дій користувача для виявлення аномальних дій користувача.

4. **Навчання співробітників** – запровадження постійної системи тренінгів, проходження курсів, залучення аутсорсингових компаній для практичного навчання, аудит.

## Порівняння методів протидії соціальній інженерії [2]

Назва методу	Опис	Переваги	Недоліки
Машинне навчання	Збір обробка та підготовка даних для глибокого навчання на основі нейромереж.	Автоматизація, швидкість, адаптивність, зниження людського фактору, масштабованість	Модель може не виявити нові типи фішингу без додаткового навчання, висока вартість і складність налаштування, потребує регулярного оновлення, великі витрати на обчислювальні потужності та зберігання даних
Захист кінцевих пристроїв	Використання антивірусного ПЗ	Запобігає зараженню системи	Потребує регулярного оновлення
PoLP	Надання мінімальних привілеїв, потрібних для роботи співробітників	Мінімізує витік даних	Може ускладнити робочі процеси
Антифіш інгові рішення	Впровадження вже наявних рішень таких як Proofpoint Email Protection, Barracuda Sentinel, Cofense PhishMe	Висока ефективність виявлення фішингових атак, практичне навчання і симуляції фішингових атак.	Висока вартість для малих і середніх бізнесів, м ожлива складність інтеграції з іншими системами.

Соціальна інженерія є одним з найефективніших методів серед кіберзлочинців [3]. Захист від перелічених загроз можливий лише за умови впровадження комплексних заходів, що включає технічні, людські та

організаційні аспекти, а також постійний пошук нових методів захисту та впровадження його.

### **Література**

1. Головка А.Ю. Інформаційна безпека: підходи та рішення. – К.: Техніка, 2020. 320 с.
2. ДСТУ 8302:2015. Бібліографічне посилання. Загальні положення та правила складання.
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020. 1184 p.

## **МЕТОДИ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ НА ОСНОВІ ПРАВОВИХ, ОРГАНІЗАЦІЙНИХ ТА ТЕХНОЛОГІЧНИХ ПІДХОДІВ**

**Куценко О. С.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Людський фактор є одним із найважливіших аспектів забезпечення інформаційної безпеки, оскільки значна частка кіберінцидентів зумовлена поведінковими характеристиками користувачів. Соціоінженерні атаки, зокрема фішинг, претекстинг та інші методи психологічної маніпуляції, спрямовані на отримання несанкціонованого доступу до інформаційних активів шляхом використання довіри, когнітивних упереджень або неувважності співробітників. Високий рівень ефективності таких атак підкреслює необхідність комплексного підходу до захисту інформаційних систем, який включає навчання персоналу,

запровадження адаптивних політик кібергігієни та імплементацію механізмів виявлення соціоінженерних загроз.

Актуальність цієї проблеми підтверджується статистичними даними. Згідно з дослідженням IBM [1], 95% кіберінцидентів є наслідком людських помилок, що свідчить про критичну роль підготовки користувачів та їх здатності розпізнавати атаки. Зокрема, однією з найбільш поширених кіберзагроз є фішинг, на частку якого припадає близько 36% успішних атак на корпоративні мережі [2]. Окрім соціоінженерних атак, значна кількість інцидентів спричинена використанням слабких або повторно застосованих паролів, що створює сприятливі умови для компрометації облікових записів через атаки типу credential stuffing та brute force.

Фактичні випадки кібершахрайства підтверджують значний вплив людського фактору на кібербезпеку організацій. Так, у 2016 році зловмисник з Литви здійснив фінансову шахрайську атаку на Google і Facebook [3], використовуючи підроблені рахунки-фактури та соціоінженерні методи маніпуляції співробітниками, що призвело до втрат у розмірі \$120 млн. Цей інцидент є показовим прикладом того, як недостатній контроль за фінансовими операціями та низька обізнаність персоналу можуть призвести до значних фінансових втрат.

Соціоінженерні атаки варіюються за складністю та методами реалізації, однак спільною характеристикою є цілеспрямоване маніпулювання поведінкою користувачів. Серед основних типів таких атак виділяють [4]:

- фішинг та його варіації (вішинг, смішинг, цільовий фішинг) – масові або цільові розсилки шкідливих повідомлень для викрадення облікових даних або ініціювання несанкціонованих дій;
- ВЕС-атаки – атаки на керівників вищої ланки з метою отримання фінансової або конфіденційної інформації;
- претекстинг – використання неправдивих контекстів (фальшивих запитів від керівництва, банківських установ тощо) для виманювання чутливих даних;

- соціоінженерні атаки із застосуванням шкідливого ПЗ – маніпулювання користувачами для встановлення шкідливого ПЗ або підключення заражених пристроїв.

З огляду на високу ефективність соціоінженерних атак та їхню здатність обходити технічні засоби захисту, мінімізація ризиків, пов'язаних із людським фактором, потребує комплексного підходу.

Одним із найефективніших заходів захисту є навчання персоналу. Практика проведення фішингових симуляцій дозволяє оцінити рівень готовності співробітників і виявити найуразливіші ланки організації. Інтерактивні навчальні програми, що моделюють реальні атаки, сприяють розвитку навичок протидії маніпуляціям, а розсилання інформаційних бюлетенів підтримує обізнаність співробітників щодо актуальних загроз. Дослідження підтверджують ефективність таких заходів: організації, що впроваджують регулярні навчання та симуляції атак, демонструють суттєве зниження кількості успішних соціоінженерних атак.

Хоча навчання персоналу та розбудова культури кібергігієни є важливими, вони залишаються недостатніми без належної нормативно-правової регламентації та інтеграції сучасних технологічних рішень. У цьому контексті особливу роль відіграють правові вимоги та стандарти інформаційної безпеки, які визначають обов'язкові заходи для забезпечення стійкості організацій до соціоінженерних загроз.

Правове регулювання відіграє важливу роль у протидії соціоінженерним атакам, оскільки встановлює вимоги щодо інформаційної безпеки та визначає відповідальність за кіберзлочини. Наприклад, в ЄС GDPR зобов'язує організації забезпечувати високий рівень захисту персональних даних, що передбачає впровадження механізмів запобігання несанкціонованому доступу. Міжнародні стандарти, зокрема ISO/IEC 27001 та ISO/IEC 27005, регламентують управління ризиками інформаційної безпеки, що включає моніторинг поведінкових аспектів користувачів. Водночас кримінальне законодавство передбачає

відповідальність за шахрайство, маніпуляції та викрадення конфіденційної інформації, що охоплює як класичні кіберзлочини, так і соціоінженерні атаки.

Окрім нормативного регулювання та організаційних заходів, важливим напрямом мінімізації ризиків соціоінженерних атак є використання сучасних технологічних рішень. Інтеграція поведінкового аналізу (UEBA – User and Entity Behavior Analytics) дозволяє ідентифікувати аномальну активність користувачів та виявляти потенційні загрози ще до їх реалізації. Автоматизований моніторинг дій привілейованих облікових записів забезпечує контроль над критичними операціями та запобігає зловживанням доступом. Впровадження архітектури Zero Trust унеможлиблює несанкціонований доступ до інформаційних систем шляхом обов'язкової верифікації всіх запитів незалежно від їхнього джерела. Комплексне застосування цих рішень забезпечує проактивне виявлення загроз і суттєво знижує ризик компрометації систем через людські помилки або маніпулятивний вплив.

Таким чином, зростаючі економічні збитки від кіберзлочинності та поширеність соціоінженерних атак підтверджують, що людський фактор залишається одним із найуразливіших елементів інформаційної безпеки. Висока ефективність таких атак вимагає комплексного підходу до їх мінімізації, що включає як правові механізми регулювання та розбудову культури кібергігієни, так і формування адаптивної системи управління ризиками, здатної своєчасно реагувати на динамічні загрози. Реальні кіберінциденти свідчать про необхідність інтеграції нормативних вимог, організаційних заходів та технологічних рішень у єдину систему, орієнтовану на безперервний моніторинг, аналіз і вдосконалення підходів до захисту від соціоінженерних загроз.

### Література

1. Cost of a Data Breach Report 2024. *IBM*. URL: <https://www.ibm.com/reports/data-breach>

2. What is phishing attack? *CLOUDFARE*. URL: <https://www.cloudflare.com/learning/access-management/phishing-attack/>
3. Lithuanian man sentenced to 5 years in prison for theft of over \$120 million in fraudulent business email compromise scheme. URL: <https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business>
4. The Importance of Employee Training in Preventing Cybersecurity Breaches. *FUDO Security*. URL: <https://fudosecurity.com/blog/2023/09/15/the-importance-of-employee-training-in-preventing-cybersecurity-breaches/>

## **МЕТОДИКА ІНТЕГРАЦІЇ СОЦІОІНЖЕНЕРНИХ СЦЕНАРІЇВ У ПРОЦЕС ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

**Карпенко М. А.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасних умовах інформаційної безпеки тестування на стійкість до соціоінженерних атак стає необхідністю. Атаки з використанням соціальної інженерії орієнтовані на людський фактор, який є найслабшою ланкою в системі безпеки. Інтеграція соціоінженерних сценаріїв у процес тестування допомагає виявити вразливості, пов'язані з людськими помилками та недоліками в політиках безпеки.

- Фішингові тести – симуляція фішингових атак для виявлення вразливостей у співробітників.
- Соціоінженерні дзвінки – перевірка реакції на спроби отримати конфіденційну інформацію через телефонні розмови.
- Фізичне проникнення – тестування безпеки фізичного доступу шляхом використання соціальної інженерії.

- Атаки з використанням заражених носіїв – перевірка обізнаності щодо використання підозрілих USB-носіїв.

- Навчання персоналу – регулярні тренінги з виявлення соціоінженерних атак.

- Симуляції атак – проведення фішингових симуляцій для підвищення обізнаності.

- Політики безпеки – створення чітких інструкцій для запобігання соціоінженерним атакам.

- Мережеві засоби захисту – використання фільтрів для блокування фішингових листів.

Таблиця 1

### Порівняльна таблиця методів

Назва методу	Опис	Переваги	Недоліки
Фішингові тести	Симуляція фішингових атак	Виявлення вразливостей користувачів	Можливе зниження довіри до ІТ-відділу
Соціоінженерні дзвінки	Перевірка реакції на телефонні атаки	Оцінка обізнаності персоналу	Необхідність у тренуваних спеціалістах
Фізичне проникнення	Тестування фізичної безпеки	Перевірка контролю доступу	Висока вартість та ризик правових наслідків
Заражені носії	Використання заражених USB	Перевірка політик щодо зовнішніх пристроїв	Можливість шкоди обладнанню

Інтеграція соціоінженерних сценаріїв у процес тестування інформаційної безпеки дозволяє виявити вразливості, пов'язані з людським фактором. Комплексний підхід, який включає фішингові тести, соціоінженерні дзвінки та фізичне проникнення, допомагає підвищити рівень безпеки організації.

## Література

1. Кабінет Міністрів України. Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України : розпорядження від 11 липня 2018 р. №481-р. URL: <http://zakon.rada.gov.ua/laws/show/96/2016>.
2. Smith J. Cybersecurity Trends and Innovations // Journal of Information Security. 2021.
3. ISO/IEC 27001:2013. Інформаційні технології — Методи забезпечення безпеки — Системи управління інформаційною безпекою — Вимоги.

## ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

**Малаш Д. О.**

Державний університет інформаційно-комунікаційних технологій

М.Київ, Україна

У сучасному цифровому середовищі кіберзагрози стають все більш складними та руйнівними. Дедалі частіше зловмисники використовують передові технології, включаючи методи штучного інтелекту (ШІ), для здійснення атак на корпоративні мережі, хмарні сервіси та інфраструктуру організацій. Відповідно, для забезпечення кіберстійкості підприємств необхідно впроваджувати інтелектуальні механізми протидії, які здатні виявляти, аналізувати та запобігати атакам у реальному часі.

Штучний інтелект у сфері кібербезпеки відкриває нові можливості для захисту цифрових активів, включаючи автоматизацію виявлення загроз, поведінковий аналіз користувачів та машинне навчання для передбачення атак.

### **Використання ШІ для аналізу та реагування на кіберзагрози**

Традиційні системи кіберзахисту, засновані на сигнатурному аналізі та статичних правилах, мають суттєві обмеження у протидії складним атакам, що

використовують динамічні та непередбачувані методи проникнення. Інтелектуальні алгоритми, навпаки, здатні ідентифікувати загрози на основі аналізу великих обсягів даних та адаптації до нових кіберзагроз.

### **ШІ у кібербезпеці виконує такі основні функції:**

- Ідентифікація аномальної активності в інформаційних системах та мережах, що може вказувати на загрозу.
- Динамічна автентифікація користувачів на основі аналізу їхньої поведінки та біометричних даних.
- Прогнозування атак шляхом аналізу історичних даних та пошуку закономірностей у діях потенційних зловмисників.
- Автоматизоване реагування на інциденти, що дозволяє миттєво блокувати підозрілі дії та ізолювати загрозливі вузли мережі.

### **Методи захисту бізнес-сервісів із використанням ШІ**

Розглянемо основні типи атак та способи їхнього виявлення за допомогою інтелектуальних систем у таблиці 1

Таблиця 1

### **Методи виявлення та протидії кібератакам за допомогою ШІ**

<b>Тип кібератаки</b>	<b>Основні характеристики</b>	<b>Методи нейтралізації на основі ШІ</b>
DDoS-атака	Аномальне зростання запитів до сервера	Виявлення підозрілого трафіку, блокування ботнетів
Фішингові атаки	Маскування під легітимні листи або сайти	Аналіз змісту за допомогою NLP, розпізнавання шкідливих посилань
Внутрішні загрози	Нестандартна поведінка користувачів	Аналіз поведінкових аномалій, виявлення нетипових дій
Експлуатація вразливостей	Використання невідомих вразливостей у ПЗ	Автоматичне сканування системи на вразливості, створення патчів
Шкідливе ПЗ	Виконання коду, що модифікує систему	Аналіз поведінки файлів, евристичний аналіз

Успішне використання штучного інтелекту у сфері кібербезпеки потребує виконання таких умов:

- Наявність великих наборів даних для навчання та тестування моделей.
- Оптимізація алгоритмів для швидкої обробки потокової інформації.
- Автоматизація процесів безпеки для зниження залежності від людського фактора.

Сучасні рішення SIEM (Security Information and Event Management), такі як Splunk, IBM QRadar та Microsoft Sentinel, вже активно використовують штучний інтелект для моніторингу інцидентів та автоматизованої реакції на загрози. Вони дозволяють аналізувати лог-файли в реальному часі та застосовувати передові методи кореляції подій.

Використання штучного інтелекту для побудови систем управління реагуванням на кібератаки є необхідним кроком у забезпеченні інформаційної безпеки підприємств. Застосування інтелектуальних алгоритмів дає змогу швидко ідентифікувати загрози, автоматизувати процеси моніторингу та значно зменшити ризики фінансових втрат через атаки.

Подальші дослідження мають бути спрямовані на вдосконалення методів адаптації алгоритмів до нових загроз, а також на розширення можливостей інтелектуальних систем у сфері активного захисту кіберпростору.

## Література

1. Розпорядження Кабінету Міністрів України від 11 липня 2018 р. №481-р "Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України". URL: <http://rada.gov.ua/laws/show/96/2016>
2. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016.
3. Chandrasekaran M. Artificial Intelligence in Cyber Security. Springer, 2021.

4. Garcia M. Cybersecurity Operations and Fusion Centers. CRC Press, 2022.

## **СЕКЦІЯ 6. БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ**

### **POST-QUANTUM SECURITY ASSESSMENT OF 5G PROTOCOLS ACROSS OSI LAYERS**

**Kotukh Yevgen, PhD in Information Security, Associate Professor**

Dnipro University of Technology

**Alexander Wyglinski, PhD in Electrical Engineering, Full Professor, Associate**

**Dean of Graduate Studies**

**Xiaoyan Sherry Sun, PhD in Information Science and Technology, Associate**

**Professor**

Worcester Polytechnic Institute, USA

Recent advances in quantum computing pose significant challenges to the security of telecommunications systems. The vulnerability assessment of 5G networks to quantum computer attacks has become particularly critical. Within many years of engineering experience developers have become more demand for protocol design and implementation and they became more reliable than the first attempts to make networking secure enough [1]. Current cryptographic protocols implemented across various OSI layers in 5G networks are largely based on mathematical problems that quantum computers could potentially solve in polynomial time.

This research presents an analysis of quantum computing threats to 5G security protocols across the Open Systems Interconnection (OSI) model. Existing solutions show the approach for wireless network assessment [2]. Our investigation spans from physical to application layers, evaluating the cryptographic resilience of current implementations against quantum-based attacks on classical algorithms. The study emphasizes authentication mechanisms, encryption protocols, and key exchange methodologies, particularly examining their vulnerability to "digital twin" attack

vectors. This focus is crucial given the potential for quantum computers to compromise traditional cryptographic safeguards, potentially enabling sophisticated impersonation attacks within 5G networks, especially within multiagent technology that can be potentially used by hackers [3].

The research aims to identify critical vulnerabilities in existing 5G security architectures and assess their readiness for the post-quantum era. By examining each OSI layer's susceptibility to quantum-based attacks, we provide a structured evaluation of current security measures and their potential weaknesses against quantum computing capabilities. Analysis of post-quantum readiness across OSI layers in 5G reveals pervasive vulnerabilities (See Table 1):

**Physical Layer (L1).** Assume that quantum vulnerability is low. Radio interface encryption and physical security implementations maintain natural resistance to quantum attacks, though quantum sensing poses potential risks to physical layer security features. “Digital twin”-like vulnerabilities can arise from inadequate physical security measures, allowing adversaries to introduce rogue devices that mimic legitimate network components. So, we should consider this layer as a main source of digital twin attacks "foundation".

Table 1

**Analysis of post-quantum readiness across OSI layers in 5G**

OSI Layer	Protocols	Vulnerabilities	Impact	Cryptographic Algorithms
Physical Layer	NR (New Radio), mmWave	Limited susceptibility; hardware-focused. Indirect impact is possible via hardware encryption weaknesses.	Minimal impact. Potential indirect effects on hardware encryption.	Physical layer encryption (unspecified algorithms, typically hardware-based)
Data Link Layer	PDCCP, RLC, MAC	Potential exploitation of encryption algorithms like SNOW 3G, AES, or ZUC.	Medium impact. Possible decryption of data frames or false data injection.	SNOW 3G, AES, ZUC

Table continued

Network Layer	IPv6, GTP-U	Compromise of IPsec through attacks on classical encryption (e.g., RSA, DH).	High impact. Interception, decryption, and manipulation of packets.	IPSec (AES, ChaCha20, RSA, DH). GTP-U
Transport Layer	TCP, UDP	Weaknesses in TLS encryption (e.g., RSA, ECC).	High impact. Session hijacking or real-time decryption of data.	TLS (AES, ChaCha20, SHA-256, RSA, ECC)
Session Layer	HTTP/2, SCTP	Similar vulnerabilities to TLS encryption as in the Transport Layer.	High impact. Disruption of service continuity and session hijacking.	TLS (AES, ChaCha20, SHA-256), EAP-AKA
Presentation Layer	NAS, TLS/SSL	TLS/SSL encryption weaknesses; potential data format and conversion exploitation.	High impact. Decryption compromises confidentiality and integrity.	TLS/SSL (RSA, ECC, AES)
Application Layer	5G-HTTP, REST API	Vulnerable due to reliance on TLS/SSL for API keys, tokens, or sensitive payloads.	Critical impact. Unauthorized access, data theft, and service disruption.	TLS/SSL (RSA, ECC, AES), HTTP encryption (AES)

Analysis of post-quantum readiness across OSI layers in 5G reveals pervasive vulnerabilities:

**Physical Layer (L1).** Assume that quantum vulnerability is low. Radio interface encryption and physical security implementations maintain natural resistance to quantum attacks, though quantum sensing poses potential risks to physical layer security features. “Digital twin”-like vulnerabilities can arise from inadequate physical security measures, allowing adversaries to introduce rogue devices that mimic legitimate network components. So, we should consider this layer as a main source of digital twin attacks "foundation".

**Data Link Layer (L2).** Assume that quantum vulnerability is medium. PDCP and MAC security protocols show vulnerabilities, particularly in stream cipher implementations like SNOW 3G and ZUC. While AES remains quantum-resistant, other protocol weaknesses enable MitM attacks in 5G implementations, compromising communication integrity. Link-layer authentication requires post-quantum updates.

**Network Layer (L3).** Assume that quantum vulnerability is high. IPSec and Mobile IP security heavily rely on RSA/ECC-based key exchanges, making them highly vulnerable to Shor's algorithm. GTP vulnerabilities, especially in GTP-U secured by quantum-vulnerable IPSec, enable traffic redirection and digital twin attacks. The layer's routing and forwarding functions become susceptible to malicious node exploitation, compromising network integrity. Urgent migration to post-quantum cryptographic solutions is required.

**Transport Layer (L4).** Assume that quantum vulnerability is high. TLS 1.3 and DTLS implementations are critically vulnerable in public key cryptography and digital signatures. Sequence number prediction vulnerabilities enable session hijacking, facilitating digital twin attacks. Current TLS configurations, supporting deprecated ciphers and lacking proper certificate validation, remain susceptible to MitM attacks. The absence of standardized quantum-resistant TLS implementations presents significant research opportunities and security challenges.

**Session Layer (L5).** Assume that quantum vulnerability is medium. Session management vulnerabilities enable session hijacking and disruption, potentially allowing digital twin attacks through legitimate session impersonation. Given the layer's reliance on TLS for security, the absence of quantum-resistant TLS implementations presents ongoing research challenges and security risks.

**Presentation Layer (L6).** Assume that quantum vulnerability is medium. Data format handling vulnerabilities can lead to buffer overflow exploits, enabling malicious code injection and digital twin establishment. The layer's security heavily depends on TLS, making quantum-resistant TLS development a critical research area for addressing current vulnerabilities.

**Application Layer (L7).** Assume that quantum vulnerability is high. HTTPS, OAuth, and OpenID protocols show critical vulnerabilities in digital certificates and signatures. Insecure APIs and improper input validation create vectors for digital twin attacks that mimic legitimate application behavior. TLS/SSL dependencies at this layer perpetuate quantum vulnerabilities, demanding comprehensive updates to post-

quantum authentication and encryption methods. Proven security approaches will be considered for authentication protocols in the future [4].

### References

1. Г. Халімов, О. Потій, О. Дунь, Є. Котух Аналіз безпеки MAC алгоритмів стандарту ISO/IEC 9797-2. Збірник робіт наукової конференції Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 1 (14), 2007 р URL: <https://ela.kpi.ua/server/api/core/bitstreams/6638674e-5f5f-45aa-a9d0-5aac01f447f5/content>
2. Є. Котух, В. Лючак, О. Страх. Один підхід до побудови індивідуальних математичних моделей захисту у бездротових сенсорних мережах. Радіотехніка, вип. 207, 2021 стор. 78-82. URL:<http://rt.nure.ua/article/view/253410>
3. C. Shoniregun, Y. Kotukh. Application of Multi-Resolution Integration Algorithm (MRIA) in RFID-based distributed sensor network. 2006, In *IEEE INFOCOM* (Vol. 23, p. 29).URL: [https://infocom2006.ieee-infocom.org/Posters/1568980659\\_Application%20of%20Multi-Resolution%20Integration/1568980659\\_Application%20of%20Multi-Resolution%20Integration%20Algorithm%20\(MRIA\)%20in%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf](https://infocom2006.ieee-infocom.org/Posters/1568980659_Application%20of%20Multi-Resolution%20Integration/1568980659_Application%20of%20Multi-Resolution%20Integration%20Algorithm%20(MRIA)%20in%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20.pdf)
4. Халімов, Г. З., & Котух, Е. В. (2012). Universal hashing algorithm on the Suzuki curve. *Eastern-European Journal of Enterprise Technologies*, 3(9(51)), 10–15.URL: <https://doi.org/10.15587/1729-4061.2011.1666>

# **АУДИТ ЯК ЕФЕКТИВНИЙ ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**

**Кривов'яз І.Я.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасний світ стає все більш залежним від інформаційних технологій, які проникли в усі сфери життя та стали невід'ємною частиною нашої буденності. Фінанси, транспорт, енергетика, охорона здоров'я та інші галузі функціонують завдяки цифровим системам, що забезпечують їхню безперервність і ефективність. Така ж глибока цифровізація поширилась і на об'єкти критичної інфраструктури (далі — ОКІ), що є основою стабільного функціонування найбільш важливих секторів діяльності держави. Будь-яке втручання в їх функціонування або порушення їх роботи може мати катастрофічні наслідки для економіки, суспільства та національної безпеки. Саме тому кіберстійкість — здатність систем протистояти кібератакам, швидко відновлювати функціонування після інцидентів та мінімізувати потенційні втрати — є критично важливою.

Початок повномасштабного вторгнення російської федерації в Україну стало справжнім викликом для ОКІ. За даними Служби безпеки України, якщо на початку вторгнення фіксувалося близько 800 атак на рік, то у 2023 році цей показник досягнув 4500 інцидентів [1]. Особливо вразливими є сектори зв'язку, оборони, об'єкти критичної інфраструктури та банківський сектор.

У контексті постійно зростаючої кількості загроз, проведення аудиту інформаційної та кібербезпеки стає важливим, а головне ефективним інструментом для підвищення рівня кіберстійкості та безперервності функціонування ОКІ. Аудит дозволяє оцінити рівень захищеності інформаційних систем, виявити потенційні вразливості, а також надати обґрунтовані рекомендації, що націлені на усунення «прогалін» в заходах

інформаційної та кібербезпеки. Це не просто перевірка на відповідність стандартам, а комплексний аналіз всіх аспектів інформаційної безпеки, який охоплює як технічні, так і організаційні аспекти. Основні переваги застосування аудиту:

- **Виявлення вразливостей та ідентифікація ризиків.** Аудит допомагає визначити слабкі місця в системах безпеки та оцінити ймовірність їх експлуатації зловмисниками.

- **Перевірка відповідності кращим стандартам та практикам.** Оцінка, наскільки інформаційні системи та заходи безпеки відповідають міжнародним стандартам (ISO/IEC 27001, NIST CSF), регуляторним вимогам (постанова КМУ №518 [2]) та внутрішнім політикам організації.

- **Оцінка ефективності заходів захисту.** Аналіз поточного стану безпеки дає змогу зрозуміти, наскільки ефективними є наявні механізми захисту та чи мінімізувати наслідки від інцидентів інформаційної та кібербезпеки.

- **Розробка рекомендацій для покращення.** На основі отриманих результатів перелік рекомендацій щодо вдосконалення політик кібербезпеки, налаштування технічного захисту та підвищення обізнаності персоналу і т.п.

- **Мінімізація потенційних втрат.** Завдяки вчасному виявленню та усуненню «слабких місць» ОКІ може уникнути значних фінансових збитків, репутаційних втрат та правових наслідків.

Реальний досвід показує, що аудит є не просто формальною процедурою, а дієвим інструментом, що допомагає оптимізувати та покращити наявні процеси захисту. Організації, які регулярно проходять такі перевірки та впроваджують заходи з підвищення безпеки, мають значно вищий рівень стійкості до кібератак та швидше відновлюють свою роботу у разі інцидентів. Тож підсумовуючи вищезазначене аудит кібербезпеки варто розглядати не як разову ініціативу, а як невід'ємну складову стратегії управління ризиками інформаційної безпеки.

## Література

1. Кількість кібератак на рік на критичну інфраструктуру України  
URL: <https://minfin.com.ua/ua/2024/05/07/126427603/>
2. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>

## ІГРОВА МОДЕЛЬ ЗАХИСТУ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

**Савченко В.А., д.т.н., проф.**

Державний університет інформаційно-комунікаційних технологій,  
м. Київ, Україна

**Возняк Р.М., д.філософії,**

**Сампір О.М., д.філософії**

Національний університет оборони України, м. Київ, Україна

Системи управління об'єктів критичної інфраструктури (ОКІ) складаються з сотень комп'ютерів, поєднаних в єдину мережу, що робить їх уразливими до різного виду кіберзагроз. У зв'язку з цим виникає нагальна потреба у розробці науково-методичного апарату захисту ОКІ від кібератак [1].

За останні роки в Україні та світі відбулося багато серйозних кіберінцидентів, які мали значний вплив на державні органи управління та організації. Атаки, типу NightKnight (2011), Shamoon (2012), BlackEnergy (2015), Petya та NotPetya (2017), SolarWinds (2020), атака на державні фінансові організації (2016), на органи юстиції (2023), на державні реєстри України (2024) та багато інших призвели до серйозних збоїв у роботі інфраструктури та

завдали збитків на мільйони доларів. З точки зору досліджень існує велика потреба розробки математичної моделі захисту ОКІ від кібератак.

Метою даного дослідження є розробка комплексної математичної моделі, яка базується на об'єктивних даних вимірювань і може стати основою в забезпеченні безпеки та надійності об'єктів критичної інфраструктури.

Для кількісної оцінки впливу кібератак на об'єкти критичної інфраструктури модель повинна враховувати: 1) уразливості ОКІ, 2) процес атаки та 3) інвестиції у систему захисту ОКІ.

Рівняння уразливості використовується для кількісної оцінки ризику атаки на ОКІ. Воно враховує уразливі місця компонентів об'єкта та їх взаємозалежність:

$$V(x) = \sum_{i=1}^n v_i(x) w_i(x), \quad (1)$$

де  $V(x)$  – уразливість об'єкта критичної інфраструктури  $x$ ;  $v_i(x)$  – уразливість  $i$ -го компонента  $x$ ;  $w_i(x)$  – вага  $i$ -го компонента ОКІ  $x$ .

Для аналізу впливу кібератак на ОКІ використовується рівняння ігрової моделі. Розглядається поведінка сторони нападу та сторони захисту, стратегії атаки та захисту ОКІ. Рівняння захисту має вигляд:

$$\text{Min}[E(U)] = \text{Min}[\alpha \times P(x, a) - \beta \times (1 - P(x, a))], \quad (2)$$

де  $E(U)$  – шкода, яка може бути заподіяна об'єкту критичної інфраструктури;  $\alpha$  – виграш нападу від кібератаки;  $P(x, a)$  – ймовірність успіху кібератаки;  $\beta$  – втрати нападу від невдалої атаки;  $x$  – ОКІ;  $a$  – дії нападника. Аналізуючи рівняння ігрової моделі, можна зрозуміти стратегії нападу та захисту і розробити контрзаходи для захисту ОКІ від кібератак.

Рівняння оптимальних інвестицій у безпеку може бути сформульоване наступним чином:

$$\pi = R(S) - C(S) - E(U), \quad (3)$$

де  $\pi$  – прибуток власника ОКІ;  $R(S)$  – дохід, отриманий об'єктом як функція рівня інвестицій у безпеку;  $C(S)$  – вартість інвестицій у безпеку;  $E(U)$  – потенціальні втрати внаслідок успішної атаки.

Ці рівняння є лише прикладом типів рівнянь, які можна використовувати в математичній моделі для захисту ОКІ від кібератак. Конкретні рівняння залежатимуть від конкретної моделі ОКІ і факторів, які впливають на захищеність об'єкта.

На основі оцінки ризиків розробляються відповідні стратегії захисту ОКІ. Ці стратегії можуть включати впровадження додаткових заходів безпеки, оновлення існуючих протоколів безпеки або розробку нових протоколів для вирішення нових загроз. Стратегії повинні бути розроблені таким чином, щоб мінімізувати ймовірність і вплив кібератаки на ОКІ.

Стратегії захисту ОКІ від кібератак, як правило, передбачають поєднання технічних, адміністративних і фізичних засобів. Технічні засоби включають такі механізми безпеки, як брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та шифрування даних. Адміністративні заходи передбачають політику, процедури та навчання, які допомагають співробітникам бути обізнаними про ризики.

Як результат даного дослідження, слід зазначити, що захист ОКІ від кібератак вимагає комплексного підходу, який враховує потенційні загрози, уразливості та ризики, пов'язані з такими атаками. Модель має враховувати ефективність існуючих заходів безпеки та розробку нових стратегій захисту для пом'якшення ризиків успішної атаки. Реалізація даної моделі може допомогти в

забезпеченні безпеки та надійності ОКІ, які необхідні для забезпечення ефективного функціонування держави.

### **Література**

1. Хавер, А. В., & Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. Сучасний захист інформації, 3(55), 12–21. <https://doi.org/10.31673/2409-7292.2023.030002>.

## **СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ**

### **РОЛЬ ДЕРЖАВНОЇ ПОЛІТИКИ У ПІДВИЩЕННІ ОБІЗНАНОСТІ ПРО КІБЕРБЕЗПЕКУ**

**Макаренко А. В.**

Державний Університет Інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасному світі, де цифрові технології пронизують усі сфери життя, кібербезпека стає одним із ключових елементів національної безпеки та стабільності. Зростання кількості кібератак, витоків даних та інших кіберзагроз свідчить про необхідність підвищення обізнаності громадян про ризики, пов'язані з використанням цифрових технологій. Державна політика відіграє вирішальну роль у формуванні культури кібербезпеки, забезпеченні інформаційної безпеки та підготовці суспільства до протидії кіберзагрозам. У цій тезі розглядаються основні аспекти державної політики, спрямованої на підвищення обізнаності про кібербезпеку, та її вплив на суспільство.

Кіберзагрози стають все більш складними та масштабними. Вони включають фішинг, віруси, шкідливе програмне забезпечення, атаки на критичну інфраструктуру та інші форми кіберзлочинності. Згідно з даними міжнародних організацій, кількість кібератак зростає щороку, а їх наслідки можуть бути катастрофічними для економіки, державних установ та приватних осіб. У таких умовах недостатньо лише технічних заходів захисту — необхідно формувати обізнаність громадян про кіберризики та навчати їх ефективним методам протидії.

Держава є основним організатором та координатором заходів у сфері кібербезпеки. Її роль полягає у:

- Розробці законодавчої бази, що регулює питання кібербезпеки.

- Створенні національних стратегій та програм, спрямованих на підвищення обізнаності громадян.

- Забезпеченні міжвідомчої взаємодії для ефективного реагування на кіберзагрози.

- Фінансуванні освітніх та інформаційних кампаній.

Наприклад, у багатьох країнах існують національні агенції з кібербезпеки, які займаються популяризацією знань про кіберризик та навчанням громадян. Державні програми часто включають розробку навчальних матеріалів, проведення тренінгів та семінарів, а також співпрацю з приватним сектором та громадськими організаціями.

Одним із найефективніших інструментів підвищення обізнаності про кібербезпеку є освітні ініціативи. Держава може:

- Впроваджувати програми з кібербезпеки в навчальних закладах, починаючи зі шкільної освіти.

- Організувати безкоштовні курси та вебінари для широкого загалу.

- Розробляти інтерактивні платформи для навчання основам кібербезпеки.

Інформаційні кампанії також відіграють важливу роль. Вони можуть включати соціальну рекламу, публікацію рекомендацій у ЗМІ та соціальних мережах, а також створення спеціальних ресурсів, де громадяни можуть отримати актуальну інформацію про кіберзагрози.

Багато країн світу вже реалізували успішні програми з підвищення обізнаності про кібербезпеку. Наприклад, у Європейському Союзі діє стратегія "Кібербезпека для всіх", яка включає освітні програми для різних вікових груп. Україна, яка стикається зі значними кіберзагрозами через геополітичну ситуацію, також активно розвиває відповідні ініціативи. Національна стратегія кібербезпеки України передбачає підвищення обізнаності громадян через співпрацю з міжнародними партнерами та впровадження сучасних підходів до освіти [1].

Незважаючи на значні зусилля, існують виклики, які ускладнюють реалізацію державної політики у сфері кібербезпеки. Серед них:

- Низький рівень цифрової грамотності серед окремих груп населення.
- Недостатнє фінансування освітніх програм.
- Швидкі темпи розвитку кіберзагроз, що вимагає постійного оновлення знань.

Проте, перспективи розвитку цієї сфери є значними. Впровадження інноваційних підходів, таких як використання штучного інтелекту для навчання або створення віртуальних симуляторів кіберзагроз, може значно підвищити ефективність державної політики [2].

Державна політика є ключовим фактором у підвищенні обізнаності про кібербезпеку. Через розробку стратегій, освітні ініціативи та інформаційні кампанії держава може забезпечити підготовку громадян до протидії кіберзагрозам. Умови сучасного цифрового світу вимагають постійного вдосконалення підходів до кібербезпеки, і саме держава має відігравати провідну роль у цьому процесі. Тільки через спільні зусилля уряду, бізнесу та громадянського суспільства можна досягти високого рівня кібербезпеки та забезпечити стабільний розвиток суспільства в цифрову епоху.

### **Література**

1. Верховна Рада України. (2017). Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. Офіційний вебпортал Верховної Ради України. URL: <https://zakon.rada.gov.ua/go/2163-19>
2. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 : станом на 3 лют. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>

# **ІННОВАЦІЙНІ ПІДХОДИ ДО НАВЧАННЯ КІБЕРБЕЗПЕКИ: ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ТА ДОПОВНЕНОЇ РЕАЛЬНОСТІ**

**Паламарчук І.В.**

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Звичайний підхід до навчання передбачає використання готових систем з фіксованими навчальними програмами. Однак такі методи є менш гнучкими, адже орієнтовані на принцип «одне для всіх». Крім того, вони часто є досить затратними, що робить їх не найкращим варіантом для навчання кібербезпеки. Такі системи спираються як на паперові матеріали (бюлетені, плакати, брошури), так і на електронні ресурси (мобільні телефони та комп'ютери). Друковані матеріали можуть передавати інформацію щодо одного чи декількох тем для певної групи користувачів. Але в сучасному світі, де кіберзагрози постійно змінюються, ці традиційні методи стають все менш ефективними. Саме тому акцент робиться на інноваційних підходах, які можуть зробити навчання кібербезпеки більш захопливим, доступним і результативним.

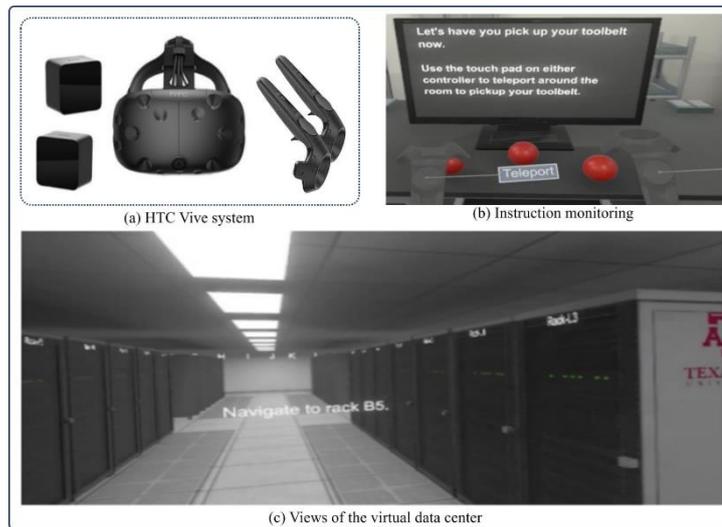
Віртуальна реальність (VR) – це технологія, яка дозволяє користувачу відчувати середовище або віртуальний світ у найбільш імерсивний спосіб[1]. У VR все, що бачить, чує та відчуває користувач, є синтетично створеним комп'ютером або електронним пристроєм. VR дозволяє моделювати місця або ситуації, до яких користувач не має фізичного доступу, що робить її корисною для навчання кібербезпеки в безпечному середовищі.

Доповнена реальність (AR) – це технологія, яка дозволяє користувачеві бачити реальний світ, але з об'єктами або контекстною інформацією, яка розширює сприйняття об'єктів, до яких вони відносяться[1]. Доповнена реальність корисна для навчання кібербезпеки, оскільки дозволяє користувачеві знаходитися перед реальною машиною, але без фактичного втручання в її роботу, тому вони можуть навчатися безпечно.

Дослідження, проведене командою Steffen et al.[2], пропонує структурований підхід до аналізу можливостей технологій віртуальної (VR) та доповненої реальності (AR) у навчанні. Автори виділяють ключові аспекти, які демонструють, як ці технології можуть покращити навчальний досвід:

1. Зменшення негативних аспектів фізичного світу :
  - зниження фізичних ризиків (наприклад, безпечне навчання на симуляціях);
  - зменшення емоційного та психологічного тиску.
2. Посилення позитивних аспектів фізичного світу :
  - підвищення емпатії завдяки імерсивним сценаріям;
  - розширення реальності через додавання корисної інформації;
  - поліпшення координації, співпраці та комунікації;
  - ефективна фільтрація та надання інформації.
3. Відтворення аспектів фізичного світу:
  - навчання через взаємодію з цифровими об'єктами;
  - зменшення витрат ресурсів;
  - доступність для осіб з фізичними обмеженнями.

У двох кейс-стадіях було показано, що VR та AR допомагають знизити фізичні та емоційні ризики, забезпечують доступ до унікальної інформації, скорочують витрати часу та ресурсів, а також дають можливість взаємодіяти з середовищами, які існували в минулому або ще не існують. Ці технології також дозволяють отримувати детальні сенсорні враження(як показано на рисунку 1, що зображає інтерфейс CiSE-ProS)[3] та фокусуватися на важливих деталях у навчальних сценаріях.



*Рис. 1 Робочий інтерфейс програми CiSE-ProS*

Використання VR та AR-технологій у навчанні кібербезпеки показало результати у різних дослідженнях:

- CiSE-ProS : 90% студентів успішно запам'ятали фізичні рівні безпеки, а 80% зберегли знання через тиждень[3]. Студенти підкреслили реалістичність та інтерактивність VR.
- CyVR-T : Курсанти ВМС США значно покращили навички виявлення кіберзагроз завдяки симуляціям на мостиках кораблів[4].
- Lord of Secure : 90% студентів зрозуміли теми гри, а 82% відзначили краще розуміння порівняно з традиційними методами[5].
- CyberVR : Забезпечив такий же високий рівень ефективності, як традиційні методи, але зі значно більшою заангажованістю.
- SubAR : 88% учасників продемонстрували глибоке розуміння концепцій кібербезпеки, особливо у виявленні вразливостей[6].

Впровадження технологій віртуальної (VR) та доповненої реальності (AR) у навчання кібербезпеки є перспективним напрямком, який значно підвищує ефективність освітнього процесу. Ці інструменти не лише забезпечують глибоке розуміння складних концепцій через інтерактивність та реалістичні симуляції, але й сприяють тривалому збереженню знань та заохочують до активного навчання. Результати численних досліджень

підтверджують, що VR та AR-технології покращують практичні навички, знижують ризики та роблять навчання доступним для широкого кола користувачів. Таким чином, ці інноваційні підходи мають потенціал стати основою сучасної системи підготовки фахівців з кібербезпеки, задовольняючи потреби швидко змінюваного цифрового світу.

### Література

1. Training in Cybersecurity with Augmented and Virtual Reality <https://electron-project.eu/blog/training-in-cybersecurity-with-augmented-and-virtual-reality/>
2. J. Steffan, J. Gaskin, T. Meservy, J. Jenkins, and I. Wolman, “Framework of Affordances for Virtual Reality and Augmented Reality,” *Journal of Management Information Systems*, , August 4, 2019, URL: <https://www.tandfonline.com/action/showCitFormats?doi=10.1080/07421222.2019.1628877>
3. Seo, J.H.; Bruner, M.; Payne, A.; Gober, N.; McMullen, D.; Chakravorty, D.K. Using virtual reality to enforce principles of cybersecurity. *J. Comput. Sci. Educ.* 2019, 10, 81–87. URL: <https://jocse.org/downloads/jocse-10-1-13.pdf>
4. Dattel, A.; Ochoa, O.; Friedenzohn, D.; Goodwin, T.; Brodeen, H. Using Virtual Reality to Identify Cybersecurity Threats for Navy Midshipmen. 2022. URL: <https://commons.erau.edu/faculty-research-projects/21/>
5. Visoottiviseth, V.; Phungphat, A.; Puttawong, N.; Chantaraumporn, P.; Haga, J. Lord of secure: The virtual reality game for educating network security. In *Proceedings of the 2018 seventh ict international student project conference (ict-ispc)*, Nakhon Pathom, Thailand, 11–13 July 2018; pp. 1–6.
6. Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information* 2020, 11, 121. URL: <http://dx.doi.org/10.3390/info11020121>

# МЕТОДИ РОЗПІЗНАВАННЯ ФЕЙКОВИХ ПРОФІЛІВ В ПРОФЕСІЙНИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Гурінов Н.В.

Державний університет інформаційно–комунікаційних технологій  
м. Київ, Україна

У епоху цифрових технологій платформи для професійного спілкування, такі як LinkedIn, стали ключовим інструментом для розвитку кар'єри та встановлення бізнес-контактів. Однак, разом із популярністю мереж, зростає кількість фальшивих профілів, які можуть підірвати довіру, створювати ризики безпеки та зменшувати продуктивність взаємодії користувачів. Фальшивий профіль у соціальній мережі, зосередженій на професійних взаємодіях, — це обліковий запис, створений для обману інших користувачів щодо справжньої особистості, кваліфікацій або намірів власника профілю. Він може містити вигадану або вкрадену інформацію, використовувати фальшиві фотографії та видавати себе за неіснуючу особу або організацію.

Використовувати фейковий профіль можна як із легальних причин (наприклад для продажу товарів у соціальних мережах тощо), так і зі зловмисною метою (шахрайства, маніпуляції, заборонений контент тощо) [1].

Основні методи розпізнавання фейкових профілів у професійних соціальних мережах наведені на Рис.1.

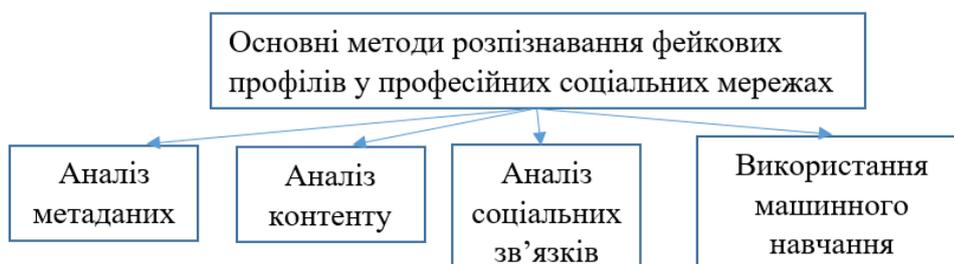


Рис.1 Основні методи розпізнавання фейкових профілів у професійних соціальних мережах

Під час **аналізу метаданих** перевіряється дата створення облікового запису. Фейкові профілі зазвичай фіксуються у часі, який передує важливим подіям, наприклад, у час висування кандидатів на вибори, або якщо потрібно досягти певної цілі дуже швидко. Наявність такої активності у новостворених профілях облікових записів свідчить про їх імовірну фальшивість.

Вказані IP адреса та місце проживання користувача також перевіряються. Варіації IP адреси, або різниця, яка може бути поміж IP адресою та місцем, в якому насправді знаходиться користувач, може вказувати на наявність або використання VPN чи проксі-серверів для замаскування справжнього місцезнаходження. Аналогічно, якщо місце розташування визначається державою, яка абсолютно не співпадає з державою, в якій користувач нібито проживає, це може вказувати на фальшивий користувацький обліковий запис. У разі спостереження за вказаним графіком активності є підозри, що його поведінка є нетиповою. Наприклад, якщо активований профіль є активним безперервно протягом доби, або ж є активність, але вона спостерігається у фіксованому короткому проміжку часу, це може свідчити, що профіль активно управляється системою чи з іншого часового поясу з метою маніпуляції. Користуючись даними про активність, можна виявити ботів або скоординовані кампанії.

**Аналіз контенту** охоплює ряд ключових метрик, спрямованих на виявлення фальшивого профілю. Відсутність фотографії профілю, стокове фото або зображення знаменитості, погана якість зображення або фото, яке виглядає занадто ідеально, можуть сигналізувати про фальшивий профіль. Також неповна, непослідовна, надто загальна або вражаюче неймовірна інформація про досвід роботи та освіту може бути червоним прапором шахрайського профілю. Для перевірки або спростування інформації можна перевірити згадані місця роботи та навчальні заклади.

Під час перевірки профілю також необхідно перевірити публікації, створені користувачем. Монотонні публікації, репости контенту з інших джерел, надмірна кількість рекламних постів та агресивна провокаційна

риторика або відсутність будь-яких особистих постів — усе це ознаки фальшивого профілю. Незвичний стиль писемності, граматичні помилки, невідповідні конструкції слів, тавтологічні вирази або слогани можуть вказувати на фальшивий профіль, особливо коли йдеться про бота або профіль, що управляється з-за кордону.

**Аналіз соціальних зв'язків** допомагає виявити фальшиві профілі, спостерігаючи за соціальною взаємодією користувача. Підозріла активність може включати надмірну кількість контактів, отриманих за конкретний проміжок часу, або надзвичайно малу кількість контактів без очевидної причини. Фальшиві профілі часто додають велику кількість контактів без розбору, або можуть мати дуже обмежену мережу контактів, всі з яких також можуть бути фальшивими. Відсутність реальної взаємодії з контактами (лайки, коментарі, репости), повторювальні коментарі під постами інших користувачів або надмірна активність у розповсюдженні певної інформації - все це сприяє припущенню про фальшивий профіль.

**Алгоритми машинного навчання** можуть аналізувати великі обсяги профілів у пошуках аномалій у даних, що можуть включати неповну або суперечливу інформацію, фотографії з стоків або згенеровані ШІ зображення, непереконливі посади або компанії та відсутність зв'язків. Машинне навчання може аналізувати позначки профілю і певним чином вказувати, що користувач активний на профілі, але є підозрілі патерни, такі як використання профілю протягом одного дня і також короткі інтервали часу.

При виявленні фейкових профілів використовується модель градієнтного бустінгу, зокрема алгоритм XGBoost (Extreme Gradient Boosting). XGBoost із високою ефективністю, масштабованістю та здатністю обробляти розріджені дані вправно класифікує та прогнозує потенційні загрози на основі історичних даних [2]. Щоб використовувати Xgboost для виявлення фейкових профілів, пропонується кілька етапів.

Збір даних. Цей етап відповідальний за характеристики профілю (інформація, активність, зв'язки, час, геолокація та текст) і створює припустимі мітки фейкових і справжніх профілів.

Навчання. Xgboost будує ансамбль дерев, додаючи нові "оптимізовані" параметри. Вони іноді ставлять обмеження, надаючи їм деякий скаляр після застосування певної метрики. XGBoost дозволяє налаштувати різні параметри оптимізатора, такі як розмір кроку, число ітерацій і т.д. [3].

Останнім етапом є класифікація, де аналізуються ознаки нового профілю, прогнозується ймовірність фейковості та оцінюється результати метриками (точність, повнота, F1-міра, AUC-ROC). Коли модель машинного навчання, наприклад XGBoost, аналізує профіль, вона не просто говорить «фейковий» або «справжній». Вона надає значення, яке натомість передає, що «профіль, найімовірніше, є фейковим». Ця ймовірність виражається у вигляді числа від 0 до 1, де 0 означає, що профіль абсолютно не схожий на фейковий; 1 – профіль з абсолютною впевненістю є фейковим. Число між 0 і 1 показує ступінь схожості профілю на фейковий.

Отже, використання технік аналізу метаданих, вмісту та соціальних зв'язків разом із підходами машинного навчання, такими як XGBoost, дозволяє ефективно виявляти та запобігати фальшивим профілям. Це, у свою чергу, зміцнює довіру та безпеку в професійних соціальних мережах, підвищуючи їхню функціональність як інструментів для кар'єрного зростання та бізнес-нетворкінгу.

### Література

1. Войтович О.П., Дудатьєв А.В., Головенько В.О. Модель та засіб для виявлення фейкових облікових записів у соціальних мережах. *Вчені записки таврійського національного університету ім. В.І. Вернадського*. Серія: Технічні науки. Частина 1. 2018. №1 Том 29(68). С.112–119.

2. Бондаренко, А., & Стаценко В. Використання методів та моделей штучного інтелекту для покращення експертних систем виявлення вторгнень.

Herald of Khmelnytskyi National University. Technical Sciences, 333(2), 2024. с. 99-106. URL: <https://doi.org/10.31891/2307-5732-2024-333-2-15>.

3. Лип'яніна-гончаренко Христина, Юрків Христина. Методи бустингового машинного навчання для нестационарних часових рядів. *International Scientific-technical journal «Measuring and computing devices in technological processes»*. 2023, Issue 3. С.19–30.

## **КІБЕРГІГІЄНА ЯК ОСНОВА БЕЗПЕЧНОГО ЦИФРОВОГО СЕРЕДОВИЩА**

**Мельниченко Н.М.**

Державний університет інформаційно-комунікаційних технологій  
М. Київ, Україна

У сучасному світі цифрові технології стали невід'ємною частиною нашого життя, що, у свою чергу, породжує нові виклики у сфері кібербезпеки. Одним із ключових факторів, що впливають на захищеність інформаційного простору, є кібергігієна – сукупність правил і звичок, спрямованих на безпечне використання цифрових технологій. Дотримання принципів кібергігієни є критично важливим як для окремих користувачів, так і для організацій, оскільки значна частина кібератак відбувається саме через людський фактор.

Основними аспектами кібергігієни є:

- Використання надійних паролів та їх регулярне оновлення є базовим правилом безпеки. Надійний пароль повинен містити комбінацію літер різного регістру, цифр та спеціальних символів. Додатково, важливим інструментом є багатофакторна аутентифікація, яка значно ускладнює несанкціонований доступ навіть у разі компрометації пароля. Завдяки ввімкнутій багатофакторній автентифікації можна запобігти 99,9% атак на облікові записи [1].

- Багато кіберзагроз виникають через використання застарілого програмного забезпечення, яке містить вразливості. Регулярне оновлення операційної системи, антивірусного ПЗ та встановлених програм є необхідним заходом для мінімізації ризиків.

- Користувачі повинні бути уважними при відкритті електронних листів, завантаженні файлів та переході за посиланнями. Фішингові атаки, які спрямовані на викрадення особистих даних, є одним із найпоширеніших методів кіберзлочинців. Ознаками шахрайських повідомлень можуть бути граматичні помилки, термінові вимоги до дії та підозрілі посилання. Навіть нешкідливий PDF-файл або документ Word може завдати шкоди вашому комп'ютеру, якщо використовує незахищені вразливості у вашому PDF або Microsoft Word [2].

- Мінімізація цифрового сліду є важливою частиною кібергігієни. Використання приватного режиму перегляду вебсторінок, відмова від зберігання паролів у браузері, а також обмеження поширення персональної інформації в соціальних мережах допомагає зменшити ризики компрометації даних.

- Кібербезпека є динамічною сферою, тому важливо регулярно оновлювати знання щодо актуальних загроз та методів їхньої нейтралізації. Корпоративні тренінги, курси з інформаційної безпеки та симуляції фішингових атак є ефективними інструментами для підвищення рівня кібергігієни серед співробітників організацій. Європейська рада вважає соціальну інженерію однією з найбільших загроз у цифровому просторі, зазначаючи, що 82% витоків даних пов'язані з людським фактором [3].

Таким чином можна дійти висновків, що дотримання правил кібергігієни є необхідною умовою для створення безпечного цифрового середовища. Формування культури кібергігієни вимагає комплексного підходу, що включає як особисту відповідальність кожного користувача, так і організаційні заходи з навчання, контролю та запобігання загрозам. У сучасних умовах саме свідоме

ставлення до кібербезпеки стає запорукою стабільної роботи інформаційних систем і захисту даних від несанкціонованого доступу.

### **Література**

1. Посібник із кібергігієни та стійкості до кіберзагроз | Security Insider. Your request has been blocked. This could be due to several reasons. URL: <https://www.microsoft.com/uk-ua/security/security-insider/practical-cyber-defense/cyber-resilience-hygiene-guide>

2. Колеснік П. Не дайте себе зламати. 10 простих налаштувань які вбережуть вас від інтернет-загроз. РБК-Україна. URL: <https://www.rbc.ua/rus/styler/dayte-sebe-zlamati-10-prostih-nalashtuvan-1739978047.html>

3. Фішинг та ентерпрайз: Як навчати співробітників протидії складним атакам |. ESKA. URL: <https://eska.global/blog/fishing-ta-enterprajz-yak-navchati-spivrobitnikiv-protidiyi-skladnim-atakam>

## **ГЕЙМІФІКАЦІЯ НАВЧАЛЬНИХ ПРОГРАМ З ВИЯВЛЕННЯ ФІШИНГОВИХ ЗАГРОЗ**

**Сколота В.В.**

Державний університет інформаційно-комунікаційних технологій  
М.Київ, Україна

Гейміфікація підвищує ефективність тренінгів з виявлення фішингових загроз, покращуючи залученість, мотивацію та запам'ятовування знань. Традиційні програми підвищення обізнаності про безпеку часто зазнають невдачі через брак інтерактивності та залученості, тоді як гейміфіковані тренінги використовують такі елементи, як бали, таблиці лідерів, бейджі та розповіді історій, щоб посилити навчання.

Емпіричні дослідження показують, що гейміфікація значно покращує безпечну поведінку користувачів. Дослідження, проведені серед працівників міжнародних корпорацій, продемонстрували зниження вразливості до фішингу після проходження гейміфікованого електронного навчання. Завдяки інтеграції викликів, винагород та змагань учасники підвищили обізнаність щодо тактик фішингу та покращили свою здатність ідентифікувати шахрайські спроби.

Спеціально розроблені рольові ігри та тренінги на основі сценаріїв підвищують ефективність програм з підвищення обізнаності про фішинг. Дослідження показують, що представлення фішингових сценаріїв у форматі розповіді покращує запам'ятовування та розуміння інформації. Елементи рольових ігор дозволяють співробітникам випробувати реальні симуляції фішингу, надаючи їм можливості для практичного навчання. Включення адаптивного навчання на основі штучного інтелекту підвищує персоналізацію, гарантуючи, що користувачі отримують навчальні модулі на основі їхніх індивідуальних профілів ризиків.

Таблиці лідерів і змагальні елементи в рамках гейміфікованого навчання сприяють підвищенню мотивації. Співробітники, які брали участь у рейтингах лідерів, демонстрували вищий рівень залученості та покращували показники виявлення фішингу. Організації, які впровадили навчання з протидії фішингу на основі гейміфікації, спостерігали зниження кількості інцидентів, пов'язаних з фішингом, на 40% порівняно з тими, хто покладався виключно на традиційне навчання.

Гейміфіковане навчання на основі штучного інтелекту адаптується до поведінки користувачів, надаючи цільовий зворотний зв'язок і вправи на основі сценаріїв. Алгоритми машинного навчання оцінюють індивідуальну продуктивність, коригуючи складність навчальних модулів відповідно до рівня кваліфікації. Такий адаптивний підхід гарантує, що користувачі, які мають труднощі з ідентифікацією фішингових атак, отримують додаткове підкріплення, тоді як просунуті користувачі взаємодіють з більш складним контентом.

Елементи гейміфікації впливають на зміну поведінки, зміцнюючи позитивні навички безпеки. Дослідження показують, що системи навчання з винагородою, коли учасники заробляють бали за правильне розпізнавання фішингових атак, значно покращують довгострокову обізнаність у сфері безпеки. Інтерактивні вікторини, імітація фішингових атак та рольові завдання допомагають працівникам розвивати проактивне мислення щодо безпеки.

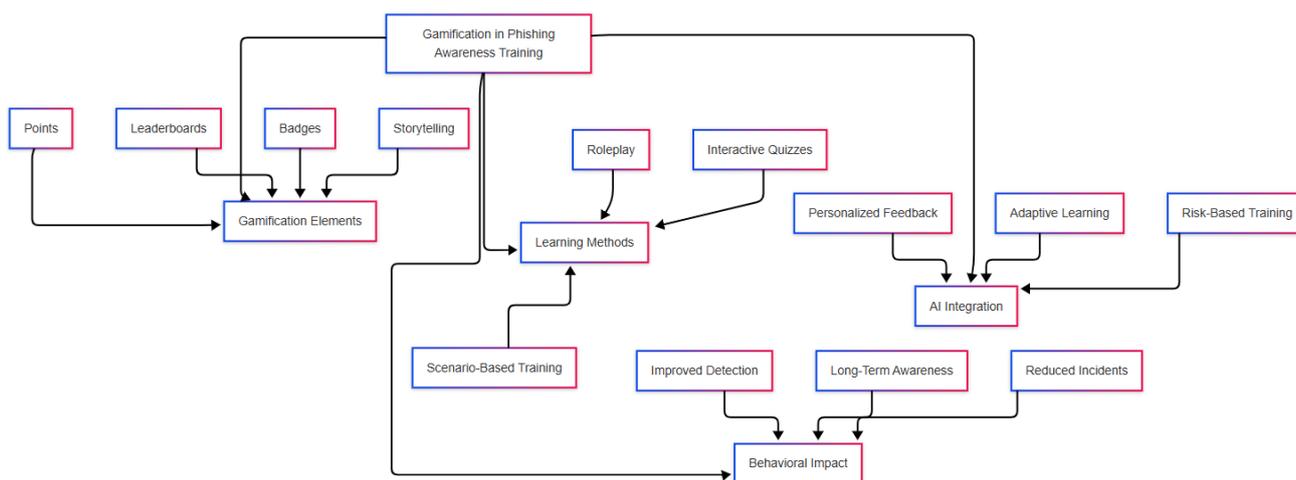


Рис. 1. Гейміфікація навчання з навчальних програм

Організації, які використовують серйозні ігри та змагання «Захоплення прапора» (CTF), повідомляють про підвищення рівня готовності до безпеки. Ці інтерактивні методи навчання імітують реальні сценарії атак, вимагаючи від учасників аналізувати, виявляти та реагувати на спроби фішингу. Гейміфіковані змагання з кібербезпеки сприяють спільному навчанню та розробці командних стратегій пом'якшення загроз.

Незважаючи на свої переваги, навчання з протидії фішингу на основі гейміфікації стикається з проблемами, серед яких масштабованість, опір користувачів та підтримання довготривалої взаємодії. Дослідження показують, що гейміфікацію слід постійно оновлювати новими сценаріями та загрозами, щоб забезпечити її актуальність. Крім того, інтеграція соціальної взаємодії, такої як командні завдання та співпраця з однолітками, підвищує ефективність.

Порівняльні дослідження підкреслюють перевагу гейміфікації над традиційними методами навчання у підвищенні обізнаності про фішинг. У той час як традиційні тренінги базуються на пасивному навчанні, гейміфіковані підходи активно залучають користувачів, зміцнюючи принципи безпеки через навчання на власному досвіді. Організації, які використовують гейміфікацію, повідомляють про вищий рівень дотримання політик безпеки та меншу вразливість до фішингових атак.

Майбутні досягнення в гейміфікованих тренінгах з підвищення обізнаності про фішинг включатимуть аналітику на основі штучного інтелекту, поведінкову біометрію та симуляції фішингу в реальному часі. Ці інновації сприятимуть адаптивному навчанню, що дозволить організаціям розвивати більш стійку культуру безпеки та зменшити вплив загроз соціальної інженерії.

### Література

1. Tchakounté, F.; Kanmogne Wabo, L.; Atemkeng, M. A Review of Gamification Applied to Phishing. *Preprints*. 2020. URL: <https://doi.org/10.20944/preprints202003.0139.v1>
2. Gamified Tailored Roleplay Story-based Phishing Awareness Training / W. Wijaya et al. *International Journal of Data Science and Advanced Analytics*. 2023. Vol. 4. P. 146–153. URL: <https://doi.org/10.69511/ijdsaa.v4i0.156>
3. Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours / P. Bitrián et al. *Journal of Business Research*. 2024. Vol. 179. P. 114685. URL: <https://doi.org/10.1016/j.jbusres.2024.114685>

# **ІННОВАЦІЙНІ НАВЧАЛЬНІ ТЕХНОЛОГІЇ З КІБЕРБЕЗПЕКИ: СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ**

**Родіонов В.Ю.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Враховуючи інтенсивність розвитку сучасних інформаційних технологій та інформаційно-комунікаційних систем (ІКС), які забезпечують передавання, оброблення та зберігання даних, актуальність захисту інформаційних ресурсів набуває все більш важливого значення. У зв'язку з цим зростає потреба у висококваліфікованих фахівцях з кібербезпеки, здатних ефективно реагувати на нові загрози та забезпечувати захист інформаційних систем. Інноваційні навчальні технології відіграють ключову роль у підготовці таких спеціалістів, забезпечуючи доступ до сучасних знань та практичних навичок у сфері кібербезпеки.

Сучасні освітні методи у сфері кібербезпеки активно розвиваються завдяки впровадженню новітніх технологій, таких як віртуальні лабораторії, платформи кіберполігонів, гейміфікація, штучний інтелект та дистанційне навчання. Одним із ключових елементів навчального процесу є використання кіберполігонів – спеціалізованих віртуальних середовищ, що імітують реальні мережеві інфраструктури та дозволяють студентам і фахівцям відпрацьовувати практичні навички в умовах, наближених до реальних атак. Такі платформи, як Cyber Range, Hack The Box та TryHackMe, надають можливість інтерактивного навчання та розвитку компетенцій з аналізу вразливостей, реагування на інциденти та етичного хакінгу.

Гейміфікація стає все більш популярним підходом у кіберосвіті. Вона дозволяє мотивувати учасників за допомогою конкурсів, квестів та симуляційних атак, таких як Capture The Flag (CTF). Такі змагання не лише

підвищують інтерес до навчання, але й допомагають розвинути критичне мислення та практичні навички аналізу загроз.

Також важливим аспектом є використання штучного інтелекту та машинного навчання у навчальних платформах. Інтерактивні системи, що адаптують навчальні матеріали відповідно до рівня знань користувача, дозволяють ефективніше засвоювати матеріал та надавати індивідуальні рекомендації. Наприклад, персоналізовані тренажери на базі AI можуть аналізувати типові помилки студентів та пропонувати додаткові завдання для покращення розуміння складних тем.

Дистанційне навчання та масові відкриті онлайн-курси (MOOC) також відіграють значну роль у кіберосвіті. Платформи, такі як Coursera, Udemu, Cybrary та SANS Cyber Aces, надають доступ до якісного контенту, сертифікаційних програм та інтерактивних тренінгів з кібербезпеки. Важливим аспектом є те, що завдяки онлайн-навчанню студенти та фахівці мають змогу отримувати актуальні знання незалежно від місця перебування.

Перспективи розвитку інноваційних освітніх технологій у кібербезпеці пов'язані з подальшою інтеграцією технологій віртуальної (VR) та доповненої реальності (AR), розвитком адаптивних освітніх платформ та автоматизацією процесів навчання. Використання VR/AR дозволить створювати інтерактивні сценарії навчання, де студенти зможуть практикувати навички реагування на кіберінциденти у віртуальному середовищі, що підвищить рівень підготовки до реальних загроз.

Штучний інтелект відіграватиме ще більшу роль у персоналізації навчального процесу, автоматичному оцінюванні знань та аналізі прогресу студентів. Також можна очікувати зростання використання блокчейн-технологій для забезпечення захисту освітніх даних, сертифікації навичок та перевірки автентичності освітніх документів.

Крім того, важливим напрямом є розширення співпраці між освітніми закладами, бізнесом та урядом у розробці практико-орієнтованих програм підготовки спеціалістів. Створення спеціалізованих кіберцентрів, де студенти

зможуть отримувати реальний досвід роботи з кіберзагрозами, стане важливим кроком у підготовці нових поколінь фахівців.

### Література

1. Scalable Learning Environments for Teaching Cybersecurity Hands-on. URL: <https://arxiv.org/abs/2110.10004>
2. Корпоративна кібербезпека: Роль ШІ у захисті даних. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>
3. СТАЛИЙ РОЗВИТОК СИСТЕМИ ФОРМАЛЬНОЇ КІБЕРОСВІТИ: РЕФЛЕКСІЯ СУЧАСНИХ КОНЦЕПТІВ. URL: <https://ela.kpi.ua/server/api/core/bitstreams/c4ea075b-a9c3-489a-93b3-76e2539a62d4/content>

## ВИКОНАННЯ ЗАХОДІВ З КІБЕРГІГІЄНИ (КІБЕРБЕЗПЕКИ) ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННИХ ПРИСТРОЇВ ТА ПРОГРАМНИХ ЗАСТОСУНКІВ

**Новохатній Д.Ю.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

У сучасному цифровому суспільстві, де інформаційні технології проникають у всі сфери життя, питання кібербезпеки набуває критичного значення. Кібергігієна, як системний підхід до захисту персональних даних та інформаційних систем, стає невід'ємною частиною культури використання електронних пристроїв та програмних застосунків. Під кібергігієною розуміють комплекс профілактичних заходів, спрямованих на мінімізацію ризиків кіберзагроз та забезпечення безпеки інформаційного середовища. Подібно до

того, як особиста гігієна допомагає запобігти розповсюдженню хвороб, кібергігієна запобігає поширенню кіберзагроз та захищає цифрову інфраструктуру від потенційних атак.

### Ключові елементи кібергігієни

Надійні паролі є першою лінією захисту від несанкціонованого доступу до електронних пристроїв та облікових записів. Рекомендується створювати складні паролі довжиною не менше 12 символів, що містять комбінацію великих і малих літер, цифр та спеціальних знаків. Критично важливо уникати використання однакових паролів для різних сервісів, оскільки компрометація одного облікового запису може призвести до вразливості всіх інших.

Для ефективного управління паролями доцільно використовувати спеціалізовані менеджери паролів, які дозволяють генерувати унікальні складні паролі та безпечно зберігати їх. Такі рішення як Bitwarden, LastPass, 1Password або KeePass надають можливість централізованого управління обліковими даними при збереженні високого рівня захисту.

Двофакторна автентифікація (2FA) забезпечує додатковий рівень захисту, вимагаючи підтвердження особистості користувача через другий канал, наприклад, за допомогою SMS-коду, електронної пошти або спеціального застосунку для автентифікації. Впровадження 2FA значно підвищує безпеку облікових записів, навіть у разі компрометації паролю.

Регулярне оновлення операційних систем, програмних застосунків та антивірусного програмного забезпечення є критично важливим компонентом кібергігієни. Оновлення часто містять виправлення виявлених вразливостей, які можуть бути використані зловмисниками для несанкціонованого доступу до системи.

Рекомендується налаштувати автоматичне оновлення для операційної системи та програмного забезпечення. При цьому важливо забезпечити, щоб оновлення завантажувалися лише з офіційних джерел, оскільки фальшиві оновлення можуть містити шкідливий код.

Для організацій доцільно розробити політику управління оновленнями, яка передбачає тестування оновлень перед масовим впровадженням та встановлення пріоритетів для критичних оновлень безпеки.

Використання антивірусного програмного забезпечення є необхідною умовою для захисту від шкідливих програм. Сучасні антивірусні рішення здатні виявляти та блокувати різноманітні типи загроз, включаючи віруси, трояни, шпигунське програмне забезпечення та програми-вимагачі.

Окрім встановлення антивірусного ПЗ, важливо регулярно проводити сканування системи на наявність загроз та слідкувати за оновленнями антивірусних баз даних. Додатковим захистом може слугувати використання брандмауера, який контролює вхідний та вихідний мережевий трафік.

Для запобігання зараженню шкідливим ПЗ користувачам рекомендується:

1. Уникати відкриття електронних листів від невідомих відправників
2. Не переходити за підозрілими посиланнями
3. Завантажувати програмне забезпечення лише з офіційних джерел
4. Не вставляти невідомі USB-накопичувачі у свої пристрої

Регулярне створення резервних копій важливої інформації є ключовим аспектом кібергігієни, що дозволяє мінімізувати втрати у разі кібератаки, технічної несправності пристрою або випадкового видалення даних.

Для організацій рекомендується розробити комплексну політику резервного копіювання, яка визначає частоту створення копій, методи шифрування резервних даних та процедури перевірки цілісності та відновлення інформації.

Захист мережевого з'єднання є важливою складовою кібергігієни. При використанні домашньої мережі необхідно змінити стандартні облікові дані адміністратора маршрутизатора, встановити надійний пароль для Wi-Fi та налаштувати шифрування WPA3 або WPA2.

При підключенні до публічних мереж Wi-Fi слід усвідомлювати потенційні ризики та використовувати VPN (віртуальну приватну мережу) для шифрування трафіку. VPN створює захищений тунель для передачі даних,

запобігаючи перехопленню конфіденційної інформації зловмисниками.

Для організацій рекомендується впровадження сегментації мережі, яка дозволяє ізолювати критичні системи від менш захищених компонентів мережі, обмежуючи потенційний вплив кібератаки.

### Література

1. Державна служба спеціального зв'язку та захисту інформації України URL: <https://cip.gov.ua/ua>
2. CERT-UA URL: <https://cert.gov.ua/>

## ЕТИКА В КІБЕРПРОСТОРИ: ВІДПОВІДАЛЬНІСТЬ КОРИСТУВАЧІВ ЗА ЦИФРОВИЙ СЛІД

**Кодимський О.М.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасний світ неможливо уявити без цифрових технологій. Щодня мільярди користувачів залишають за собою величезні обсяги даних, які формують їхній цифровий слід. Це стосується як особистого життя, так і професійної діяльності. Використання соцмереж, мобільних додатків, онлайн-банкінгу, електронної пошти та інших цифрових сервісів призводить до створення детального профілю кожного користувача.

Однак, далеко не всі усвідомлюють наслідки своїх дій у кіберпросторі. Відсутність належного контролю над особистими даними може призвести до витоків конфіденційної інформації, кіберзлочинності, маніпуляцій, а також до репутаційних та фінансових ризиків. У цьому контексті постає питання етичної відповідальності користувачів за свій цифровий слід.

Актуальність дослідження зумовлена швидким розвитком

інформаційних технологій та постійним зростанням обсягів персональних даних у кіберпросторі. Регулювання цих процесів на рівні законодавства все ще знаходиться в стадії розвитку, тому особиста відповідальність кожного користувача відіграє ключову роль у забезпеченні цифрової безпеки.

Цифровий слід – це інформація, яку користувач залишає в мережі Інтернет під час взаємодії з цифровими технологіями. Він формується з різних джерел: соціальні мережі, пошукові системи, електронна пошта, фінансові операції, мобільні додатки, а також дані, що автоматично збираються під час перегляду вебсторінок. Ця інформація може бути використана як з позитивною, так і з негативною метою: персоналізація контенту, покращення сервісів, створення рекламних профілів або ж кіберзлочинцями для фішингових атак, маніпуляції та шантажу. Цифровий слід поділяється на два основних види – активний і пасивний. Дивитися рис. 1



Рис.1 Цифровий слід

Активний цифровий слід формується свідомо: це публікації, коментарі, реєстрації на вебсайтах, заповнення форм, надсилання повідомлень. Пасивний цифровий слід, навпаки, створюється без прямої участі користувача. Наприклад, файли cookie, які зберігають історію відвіданих сайтів, або ж

геолокаційні дані смартфона, що автоматично фіксують переміщення людини.

Значний вплив цифровий слід має на конфіденційність та безпеку користувача. З одного боку, цифрові технології надають зручність та швидкість доступу до інформації, однак водночас вони створюють загрозу витоку особистих даних. Відомі випадки, коли необачне поводження з цифровим слідом призводило до втрати грошей, репутації, а інколи навіть ідентичності. Наприклад, шахраї можуть використовувати особисті дані для оформлення кредитів, створення фейкових акаунтів або ж для шантажу.

Крім того, цифровий слід має значний вплив на репутацію. Дедалі більше компаній перед прийомом на роботу перевіряють акаунти потенційних співробітників у соціальних мережах. Невдалі публікації, старі коментарі або компрометуючі фото можуть негативно вплинути на кар'єру людини. Навіть якщо інформація була видалена, у деяких випадках вона може зберігатися у кеші пошукових систем або архівах до управління інформаційною безпекою.

### **Література**

1. Що таке цифровий слід і як його мінімізувати. URL: <https://proit.ua/shcho-takie-tsifrovii-slid-i-iak-iogho-minimizuvati/>
2. Цифровий слід. URL: [https://uk.wikipedia.org/wiki/Цифровий\\_слід](https://uk.wikipedia.org/wiki/Цифровий_слід)
3. Kolesnikova I. A. Digital traces: concepts and their meaning in the investigation of criminal offenses. Juridical scientific and electronic journal. 2023. No. 10. P. 472–475. URL: <https://doi.org/10.32782/2524-0374/2023-10/114>

# ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ ЯК ЗАСІБ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

**Онщенко В.О.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Сучасний кіберпростір є не лише майданчиком для обміну інформацією, а й ареною для протидії дезінформації та маніпулятивному контенту, що становлять серйозну загрозу як для окремих користувачів, так і для організацій. Одним із ключових засобів запобігання цим загрозам є формування культури кібербезпеки, яке включає впровадження освітніх програм, підвищення обізнаності про цифрові ризики та навчання методам перевірки інформації.

Дезінформація використовується для маніпулювання суспільною думкою, підриву довіри до офіційних джерел та створення хаотичного інформаційного середовища. Її розповсюдження здійснюється через соціальні мережі, месенджери, автоматизовані системи, а також у рамках таргетованих інформаційних кампаній [1].

Розвиток культури кібербезпеки сприяє зниженню впливу дезінформації шляхом впровадження програм цифрової грамотності та навчання методам перевірки інформації, зокрема фактчекінгу, аналізу джерел та розвитку критичного мислення [2]. Підвищення рівня обізнаності щодо механізмів інформаційних маніпуляцій дозволяє створити більш стійкий інформаційний простір.

На рис 1 наведено схему, що ілюструє процес формування культури кібербезпеки як ефективного засобу протидії дезінформації.

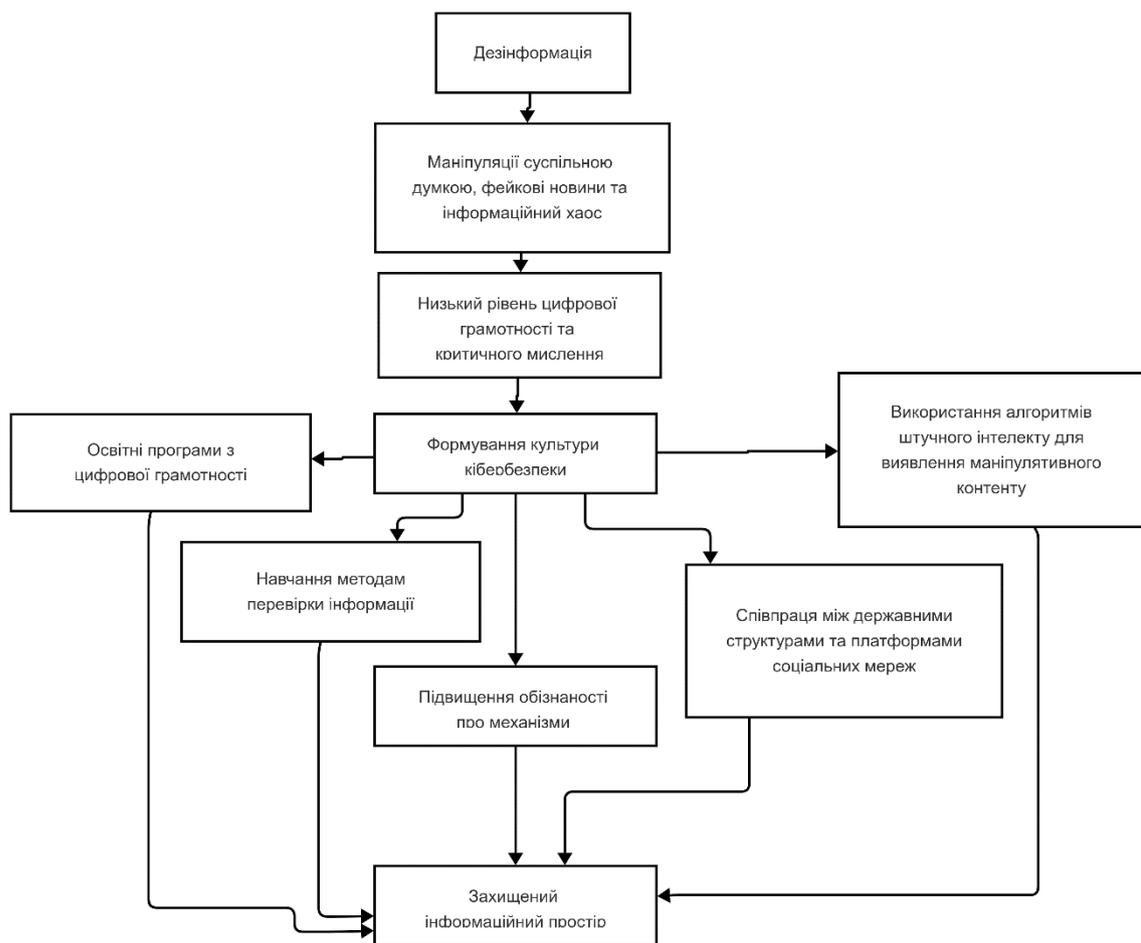


Рис.1 Схема процесу формування культури кібербезпеки як ефективного засобу протидії дезінформації

Дезінформація виступає як вихідна загроза, що спричиняє маніпуляції суспільною думкою, розповсюдження фейкових новин та створення інформаційного хаосу.

Ці процеси посилюються через низький рівень цифрової грамотності та недостатній розвиток критичного мислення серед користувачів.

Для протидії цьому формується культура кібербезпеки, яка охоплює комплекс заходів:

- Освітні програми з цифрової грамотності,
- Навчання методам перевірки інформації (фактчекінг, аналіз джерел),
- Підвищення обізнаності про механізми інформаційних маніпуляцій,

- Співпраця між державними структурами та платформами соціальних мереж,
- Використання алгоритмів штучного інтелекту для виявлення маніпулятивного контенту.

В результаті реалізації цих заходів формується захищений інформаційний простір, де вплив дезінформації суттєво знижується.

Успішний досвід боротьби з дезінформацією демонструють як міжнародні організації, так і технологічні компанії, що реалізують програми інформаційної безпеки в навчальних закладах, співпрацюють з державними структурами та соціальними медіа для протидії фейковим новинам, а також застосовують алгоритми штучного інтелекту для виявлення маніпулятивного контенту [3].

Таким чином, формування культури кібербезпеки є важливим компонентом стратегії протидії дезінформації. Підвищення цифрової грамотності та розвиток навичок перевірки інформації сприятимуть створенню більш захищеного інформаційного простору, а подальші дослідження можуть бути спрямовані на розробку інноваційних освітніх програм і автоматизованих рішень для виявлення інформаційних загроз.

## Література

1. European Commission. Tackling Disinformation Online. 2022. URL: <https://ec.europa.eu>.
2. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe, 2017. URL: <http://dx.doi.org/10.1503/cjs.011719>
3. Zannettou S. et al. Disinformation on Social Media: Analyzing How People Respond to Fake News. 2020. URL: <https://aisel.aisnet.org/cais/vol53/iss1/9>

# РІВЕНЬ ОБІЗНАНОСТІ ПЕРСОНАЛУ ЯК ВИЗНАЧАЛЬНИЙ ЧИННИК ПРОТИДІ СОЦІОІНЖЕНЕРНИМ АТАКАМ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

**Редькіна А. В.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

З розвитком цифрових технологій та розширенням інформаційних систем організацій зловмисники дедалі частіше використовують соціоінженерні методи атак. Вони базуються на маніпулюванні людською психологією, змушуючи користувачів несвідомо розголошувати інформацію або виконувати дії, що можуть призвести до отримання зловмисником несанкціонованого доступу до даних або ресурсів. Соціоінженерні атаки є особливо небезпечними, оскільки спрямовані не на вразливості технічних систем, а на експлуатацію людського фактора, який залишається найменш передбачуваним компонентом у системах безпеки (табл. 1) [1].

Таблиця 1

## Основні види соціоінженерних атак

Вид атаки	Опис	Наслідки для бізнесу
Фішинг	Надсилання підроблених електронних листів або повідомлень, що імітують легітимні комунікації.	Викрадення паролів, витік конфіденційних даних, компрометація корпоративних облікових записів.
Вішинг	Телефонні дзвінки, під час яких зловмисники видають себе за колег, представників банків або держорганів.	Розголошення критичної інформації, компрометація особистих або корпоративних даних.
Смішинг	Фішингові SMS або месенджер-повідомлення, що містять шкідливі посилання або запити на введення даних.	Встановлення шкідливого ПЗ, витік персональних або фінансових даних, зараження пристроїв.
BEC (Business Email Compromise)	Використання скомпрометованої корпоративної пошти або її підробка для фінансового шахрайства.	Фінансові втрати через шахрайські транзакції, витік комерційної та фінансової інформації.
Претекстинг	Маніпуляція жертвою через створення довірчої ситуації для	Отримання несанкціонованого доступу до даних, фінансові та

Попри розвиток технологій захисту, жодні технічні засоби не можуть повністю нівелювати ризики, пов'язані з людськими помилками. Низький рівень обізнаності співробітників щодо соціоінженерних загроз сприяє успішності таких атак, що може призвести до компрометації конфіденційної інформації, фінансових втрат або порушення безперервності бізнес-процесів. Отже, підвищення рівня обізнаності персоналу є необхідною складовою стратегії кібербезпеки будь-якої організації.

У сучасному корпоративному середовищі недостатньо лише розгорнути передові програмно-апаратні засоби захисту: засоби ідентифікації та автентифікації, системи виявлення та запобігання вторгненням, системи контролю доступу, захист кінцевих точок тощо. Ефективна стратегія безпеки вимагає комплексного підходу, що поєднує технологічні рішення із заходами організаційного характеру, спрямованими на підвищення рівня обізнаності [2].

Підвищення рівня обізнаності персоналу є багатокomпонентним процесом, що включає навчальні програми, тестування рівня обізнаності, впровадження політик безпеки та аналіз результатів реалізованих заходів [3].

Практичні навчальні заходи, такі як спеціалізовані тренінги, онлайн-курси та імітаційні атаки, дозволяють співробітникам навчитися розпізнавати потенційні загрози та реагувати на них відповідно до внутрішніх політик безпеки. Дослідження у сфері кібербезпеки підтверджують, що інтерактивне навчання, засноване на сценаріях реальних атак, є більш ефективним порівняно з традиційними лекційними методами.

Впровадження механізмів періодичного тестування персоналу на сприйнятливість до соціоінженерних атак, зокрема через контрольовані фішингові кампанії, дозволяє виявити групи підвищеного ризику. Аналіз результатів таких перевірок допомагає вдосконалити навчальні програми та адаптувати політики безпеки відповідно до виявлених слабких місць.

Організаційні заходи, зокрема політики використання паролів, багатофакторної автентифікації, обмеження доступу до критично важливих ресурсів та застосування принципу найменших привілеїв (PoLP), сприяють мінімізації ризиків, пов'язаних із людським фактором. Важливим напрямом є впровадження концепції “нульової довіри” (Zero Trust), яка передбачає постійну верифікацію користувачів та пристроїв незалежно від їхнього розташування у мережі.

Для оцінки результативності програм з підвищення обізнаності застосовуються регулярні аудити інформаційної безпеки, аналіз інцидентів та зворотний зв'язок від співробітників. Виявлення трендів у поведінці персоналу дозволяє коригувати навчальні програми та впроваджувати додаткові заходи для підвищення рівня кіберстійкості організації.

Таким чином, комплексний підхід до забезпечення кібербезпеки включає не лише технічні засоби захисту, але й організаційні заходи, спрямовані на підвищення рівня обізнаності персоналу. Розвиток культури безпеки, впровадження політик інформаційної безпеки та постійне навчання співробітників суттєво зменшують ризики успішного здійснення соціоінженерних атак, а оцінка ефективності впроваджених заходів та постійний моніторинг загроз дозволяють організаціям адаптувати стратегії захисту до нових викликів кіберпростору, що є необхідною умовою для забезпечення безпеки корпоративного інформаційного середовища.

### **Література**

1. 2024 Data breach investigations report. *Verizon*. URL: <https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf>
2. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

3. NIST SP 800-50 Rev. 1. Building a Cybersecurity and Privacy Learning Program. URL: <https://doi.org/10.6028/NIST.SP.800-50r1>

## **ПРОБЛЕМИ Й ВИКЛИКИ ФОРМУВАННЯ ОБІЗНАНОСТІ Й НАВЧАННЯ З КІБЕРБЕЗПЕКИ**

**Сніжко В. М.**

Державний університет інформаційно-комунікаційних технологій,  
м. Київ, Україна

Зростання складності кіберзагроз і залежності бізнесу від інформаційно-комунікаційних систем вимагає від організації не лише технічних рішень, а й заходів впливу на так званий людський фактор, який залишається одним із найслабших місць в системі безпеки організації. Так, згідно з дослідженнями Verizon Data Breach Investigations Report (DBIR) понад 68% кібератак стають можливими внаслідок людських помилок [1]. З огляду на це важливість інформування й навчання персоналу з кібербезпеки збільшується з кожним днем.

Водночас, процеси підвищення обізнаності й навчання з кібербезпеки стикаються з низкою проблем та викликів.

Однією з найбільш болючих проблем є відставання змісту навчання від динамічного розвитку технологій захисту інформації [2]. Технології розвиваються все швидше, і відповідно ускладнюється робота, пов'язана з кібербезпекою (проектування, впровадження, захист і підтримка систем, мереж та даних). Однак, система освіти не здатна синхронно оновлювати навчальні програми через брак знань і практичних навичок.

Інший набір проблем пов'язаний із методами та підходами до підготовки і проведення інформаційно-освітніх заходів і охоплює відсутність регулярних та послідовних програм навчання, складність і нерідко застарілість навчальних

матеріалів і брак перевірки отриманих в результаті знань і навичок. До того ж навчальні курси часто слабо адаптовані до реальних загроз, з якими можуть зустрітися працівники на своїх робочих місцях, а також не використовують нові інтерактивні, ігрові й симуляційні методи навчання.

Значне занепокоєння викликає низький рівень мотивації та залученості співробітників до навчального процесу. У персоналу багатьох малих компаній виявлено так званий синдром “Зі мною такого не станеться”, який відображає переконання працівника, що загрози стосуються лише великих компаній чи державних установ. Результатом такого ставлення є недостатня особиста відповідальність працівників за дотримання правил кібергігієни.

Наступною проблемою, яка негативно впливає на рівень обізнаності й кваліфікації персоналу з питань кібербезпеки, є недостатня інтеграція навчання з кібербезпеки в процеси найму й адаптації нових працівників. Відсутність інформування й навчання з кібергігієни на початкових етапах працевлаштування призводить до того, що новоприбулі співробітники не усвідомлюють важливість безпечної поведінки в кіберсередовищі і можуть несвідомо стати причиною витоку даних або успішної атаки [2].

З огляду на те, що кібератаки стають все складнішими, і жодна компанія сьогодні не може ефективно протистояти загрозам без інформаційної взаємодії з іншими учасниками ринку, серйозним викликом є налагодження належної співпраці та обміну актуальною, об’єктивною та структурованою інформацією між різними організаціями. Завдяки об’єднанню зусиль багатьох приватних, неурядових і державних гравців вдасться забезпечити належне інформування, вчасне виявлення загроз, ефективне реагування й відновлення після інцидентів.

Отже, навчання та формування обізнаності персоналу з питань кібербезпеки є одним із ключових чинників ефективного забезпечення кібербезпеки організації. Впровадження ефективних освітніх програм, використання новітніх технологій навчання, інтеграція кібербезпеки у всі бізнес-процеси і тісна співпраця між різними організаціями дозволять знизити ризики та підвищити рівень стійкості кожної з них до кіберзагроз.

## Література

1. Data Breach Investigations Report (DBIR). 2024. *Verizon*. URL: <https://www.verizon.com/business/resources/reports/dbir/>
2. NIST Special Publication 800-181 Workforce Framework for Cybersecurity (NICE Framework). Revision 1. 2020. *NIST*. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

## СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

### ПІДХІД ЄВРОПЕЙСЬКОГО СОЮЗУ ДО КІБЕРБЕЗПЕКИ У СФЕРІ ЗАКОНОДАВСТВА

**Дарій В.Р.**

Державний університет інформаційно-комунікаційних технологій м.Київ,  
Україна

В епоху цифрових технологій питання кібербезпеки, а особливо ті, що стосуються роботи критичної інфраструктури та захисту конфіденційності даних, стають дедалі актуальнішими. Зростання числа кіберзлочинів, витоків даних, атак на критичну інфраструктуру та зловживання персональними даними вимагає від законодавців прийняття рішучих заходів для забезпечення безпеки у цифровому. Європейський Союз, розуміючи важливість цих питань, активно працює над створенням правової бази для захисту конфіденційності громадян та забезпечення кібербезпеки. Законодавчі акти ЄС у цій сфері не лише встановлюють стандарти та правила для обробки та зберігання даних, але й покликані захистити права громадян, забезпечити стабільність роботи критичної інфраструктури та сприяти співробітництву країн у протистоянні кіберзагрозам. Одним з найважливіших законодавчих актів є Загальний регламент захисту даних GDPR [1]. Він встановлює суворі стандарти обробки персональних даних та надає громадянам ЄС контроль над їхніми даними. Це сприяє підвищенню довіри до цифрових послуг і стимулює інновації. Наприклад, GDPR забезпечує право на доступ до даних, право на забуття та право на перенесення даних, що надає користувачам більший контроль над їхньою інформацією.

Конвенція Ради Європи про кіберзлочинність, також відома як Будапештська конвенція [2], була прийнята у 2001 році і є першим

міжнародним договором, спрямованим на боротьбу з кіберзлочинами. Конвенція встановлює єдині стандарти для криміналізації певних дій у кіберпросторі, таких як незаконний доступ до комп'ютерних систем, незаконне перехоплення даних, а також створення та поширення шкідливих програм. Основні положення конвенції включають криміналізацію кіберзлочинів, міжнародне співробітництво та встановлення процедур для збирання електронних доказів та проведення обшуків і вилучень у кіберпросторі.

Європейська стратегія кібербезпеки, вперше запроваджена у 2013 році[3], спрямована на створення безпечного та надійного цифрового середовища для громадян і підприємств ЄС. Стратегія передбачає розвиток законодавчої бази, підвищення обізнаності про кіберзагрози та підтримку міжнародної співпраці. Основні напрямки стратегії включають створення та впровадження нормативно-правових актів для забезпечення кібербезпеки на національному та міжнародному рівнях, організацію навчальних програм та кампаній для інформування громадян і підприємств про кіберзагрози та заходи захисту, підтримку співпраці з іншими країнами та міжнародними організаціями для ефективного реагування на глобальні кіберзагрози, а також забезпечення безпеки критично важливих систем та мереж, що мають значення для національної безпеки та економіки.

Іншим важливим документом є Директива NIS (Network and Information Security), ухвалена у 2016 році [4]. Ця директива спрямована на забезпечення високого рівня безпеки мережевих та інформаційних систем у всьому ЄС. Вона зобов'язує операторів критичної інфраструктури (енергетичні, транспортні, банківські сектори, сфери охорони здоров'я) вживати відповідні заходи кібербезпеки і повідомляти про серйозні інциденти національним органам. Директива NIS також сприяє співпраці між державами-членами через створення мережі національних контактних точок.

Ще один важливий документ - Регламент ЄС щодо захисту недоторканності приватного життя у секторі електронних комунікацій (ePrivacy Regulation), який доповнює положення GDPR [5]. Регламент спрямований на

забезпечення конфіденційності в електронних комунікаціях і включає правила щодо використання файлів cookie, маркетингових повідомлень та обробки метаданих.

У впровадженні нормативно-правових актів, спрямованих на кібербезпеку та захист конфіденційності, Європейський Союз досяг значних успіхів. Це привело до підвищення рівня захисту персональних даних громадян, зміцнення прозорості та довіри до цифрових послуг, а також посилення міжнародного співробітництва у боротьбі з кіберзлочинністю. Громадяни ЄС отримали більший контроль над своїми даними, а компанії стали зобов'язані дотримуватися високих стандартів безпеки інформації, що сприяє розвитку більш надійного та безпечного цифрового середовища. Як приклад, декілька відомих компаній були притягнуті до відповідальності через невідповідність вимогам до безпеки даних:

- **Google:** У 2019 році Google було оштрафовано на 50 мільйонів євро за недотримання вимог щодо прозорості обробки персональних даних [6]. Це стало потужним сигналом для інших компаній про серйозність виконання вимог GDPR.

- **British Airways:** У 2020 році авіакомпанію British Airways було оштрафовано на 20 мільйонів євро [7] за неналежні заходи захисту персональних даних під час кібератаки, що призвела до витоку даних понад 400 000 клієнтів.

- **H&M:** У 2020 році компанію H&M було оштрафовано на 35 мільйонів євро [8] за незаконне зберігання та обробку персональних даних своїх співробітників.

Сприяння ефективному розслідуванню та переслідуванню кіберзлочинців дозволило країнам проводити спільні операції, обмінюватись інформацією і таким чином об'єднувати зусилля у боротьбі з глобальними кіберзагрозами. Крім того, були запроваджені навчальні програми та інформаційні кампанії, спрямовані на підвищення обізнаності громадян та підприємств про кіберзагрози. Ці ініціативи сприяли покращенню захисту критично важливих

інфраструктур та забезпеченню стабільності роботи цифрового середовища у компаніях.

### Література

1. Regulation (EU) 2016/679 of the European Parliament and of the Council. General Data Protection Regulation (GDPR). Official Journal of the European Union. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32016R0679>
2. Council of Europe. Convention on Cybercrime (Budapest Convention). URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
3. European Commission. EU Cybersecurity Strategy for the Digital Decade. URL: [https://ec.europa.eu/digital-strategy/our-policies/eu-cybersecurity-strategy\\_en](https://ec.europa.eu/digital-strategy/our-policies/eu-cybersecurity-strategy_en)
4. Directive (EU) 2016/1148 of the European Parliament and of the Council. NIS Directive. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148>
5. European Commission. Regulation on Privacy and Electronic Communications (ePrivacy Regulation). URL: [https://ec.europa.eu/digital-strategy/our-policies/eprivacy-regulation\\_en](https://ec.europa.eu/digital-strategy/our-policies/eprivacy-regulation_en)
6. Data Privacy Manager. 5 biggest GDPR fines so far 2020. URL: <https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/>
7. ICO fines British Airways £20m for data breach. BBC News. URL: <https://www.bbc.com/news/technology-50516744>
8. Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations. Reuters. URL: <https://www.reuters.com/article/us-hm-gdpr-idUSKBN1XH2X8>

# ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРІНЦИДЕНТИ: ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ У ПРОТИДІІ КІБЕРЗАГРОЗАМ ДЛЯ БІЗНЕСУ

**Коровін В.П.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Юридична відповідальність за кіберінциденти є критично важливим питанням у сучасному бізнесі, оскільки компанії все частіше стикаються з кіберзагрозами. Кіберінциденти, включаючи витік даних, атаки з використанням програм-вимагачів та несанкціонований доступ, мають правові наслідки, які поширюються на корпоративне управління, дотримання нормативних вимог та фінансову відповідальність.

З правової точки зору, бізнес підпадає під дію різних національних та міжнародних нормативно-правових актів, які встановлюють зобов'язання щодо заходів кібербезпеки та захисту даних. Загальний регламент про захист даних (GDPR) в Європейському Союзі передбачає суворе дотримання протоколів безпеки даних, вимагаючи від бізнесу захищати персональні дані та повідомляти про порушення протягом 72 годин [1]. Недотримання GDPR може призвести до значних фінансових санкцій. Аналогічно, Закон США про обмін інформацією щодо кібербезпеки (CISA) заохочує компанії ділитися розвідданими про загрози з державними установами, хоча й викликає занепокоєння щодо конфіденційності даних та обмежень відповідальності. В обох юрисдикціях компанії можуть бути притягнуті до відповідальності за недбалість, якщо вони не вживають належних заходів кібербезпеки.

Корпоративна відповідальність за кіберінциденти виходить за рамки штрафів, передбачених законодавством, і поширюється на цивільні судові процеси. Витоки даних часто призводять до колективних позовів, коли постраждалі особи вимагають компенсації за фінансові втрати, емоційні страждання або шкоду репутації. Гучні справи, такі як витік даних Equifax,

ілюструють, як компанії можуть бути притягнуті до відповідальності за нездатність захистити конфіденційну інформацію. Суди все частіше звертають увагу на те, чи проявили організації належну ретельність при впровадженні систем кібербезпеки, а невиконання цієї вимоги може становити юридичну недбалість [2].

Страховання кібербезпеки з'явилося як інструмент управління ризиками, проте його ефективність є предметом дискусій. Хоча поліси кіберстрахування покривають фінансові втрати від кібератак, часто виникають суперечки щодо обсягу покриття, особливо щодо того, чи недбалість або недотримання протоколів безпеки позбавляє права на відшкодування збитків. Страхові поліси також не звільняють бізнес від регуляторних санкцій або репутаційної шкоди, що підкреслює необхідність комплексних стратегій кібербезпеки.

Етичні міркування у протидії кіберзагрозам стосуються балансу між заходами безпеки та правами на приватність. Уряди та бізнес повинні забезпечувати кібербезпеку, не посягаючи на свободу особистості. Здійснення масового стеження під приводом кібербезпеки викликає занепокоєння щодо надмірного державного контролю. Крім того, етичні дилеми виникають, коли уряди прагнуть отримати доступ до зашифрованих даних, як це видно з дебатів щодо шифрування бекдорів [3].

Правові та етичні аспекти кібербезпеки вимагають адаптивного підходу. Закони повинні розвиватися, щоб протистояти новим загрозам, які несуть штучний інтелект (ШІ), інтернет речей (IoT) і технологія блокчейн. Етичні рамки повинні надавати пріоритет прозорості, підзвітності та захисту цифрових прав. Бізнес повинен впроваджувати проактивне управління кібербезпекою, інтегруючи оцінку ризиків, дотримання нормативних вимог та етичні міркування, щоб зменшити відповідальність та підвищити цифрову стійкість.

## Література

1. Combating Cybercrime: Economic and Legal Aspects / O. V. Sviatun et al. *WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS*. 2021. Vol. 18. P. 751–762. URL: <https://doi.org/10.37394/23207.2021.18.72>
2. E. Ok., J. Aria, D. Jose, C. Diego. The Impact of Cybersecurity Laws on Legal Procedures and Case Law. 2025. URL: [https://www.researchgate.net/publication/387625093\\_The\\_Impact\\_of\\_Cybersecurity\\_Laws\\_on\\_Legal\\_Procedures\\_and\\_Case\\_Law](https://www.researchgate.net/publication/387625093_The_Impact_of_Cybersecurity_Laws_on_Legal_Procedures_and_Case_Law)
3. Cybersecurity. Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. *European Economic and Social Committee*. 2018. URL: <https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf>

## ПРАВОВЕ РЕГУЛЮВАННЯ ТА СТАНДАРТИЗАЦІЯ ЗАХОДІВ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

**Борисюк Д.Ю.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Критична інфраструктура (КІ) є однією з найбільш уразливих сфер для кібератак, що можуть призвести до значних економічних, соціальних та навіть національних загроз. Враховуючи зростаючу кількість атак на об'єкти критичної інфраструктури, важливе значення набуває правове регулювання та стандартизація заходів кіберзахисту, що дозволяє ефективно координувати дії державних органів, бізнесу та міжнародних партнерів у цій сфері [1].

Основними завданнями правового регулювання кіберзахисту критичної інфраструктури є:

1. Визначення об'єктів КІ та їх класифікація за рівнем критичності.
2. Запровадження вимог щодо управління кіберризиками для власників і операторів КІ.
3. Регламентація заходів реагування на кіберінциденти та відновлення після атак.
4. Забезпечення міжнародної співпраці у сфері кібербезпеки.
5. Розробка механізмів державного контролю та аудиту безпеки об'єктів КІ.

На міжнародному рівні існує низка нормативно-правових актів та стандартів, що визначають вимоги до кіберзахисту критичної інфраструктури. Серед основних можна виокремити:

- Директива NIS2 (Network and Information Security Directive 2), яка встановлює підвищені вимоги до суб'єктів критичної інфраструктури у країнах ЄС щодо управління ризиками та обміну інформацією про загрози [2].
- Стандарти ISO/IEC 27001 та 27002, що надають рекомендації щодо побудови систем управління інформаційною безпекою.
- Національні законодавчі ініціативи, такі як Закон України "Про основні засади забезпечення кібербезпеки України", що визначає правові засади захисту КІ [3].

Важливим аспектом правового регулювання кібербезпеки є гармонізація міжнародних стандартів із національними нормативно-правовими актами. Це дозволяє забезпечити узгоджений підхід до управління кіберризиками та сприяє ефективній взаємодії між державними органами та приватним сектором. Окрім цього, стандартизація кіберзахисту сприяє розробці уніфікованих вимог до технічних і організаційних заходів захисту інформаційних систем [4].

Слід зазначити, що кіберзагрози постійно еволюціонують, тому необхідно впроваджувати механізми динамічного оновлення стандартів та регламентів. У цьому контексті важливу роль відіграє співпраця державних органів із приватним сектором, оскільки саме компанії є основними власниками та операторами критичної інфраструктури. Впровадження принципів Public-Private

Partnership (PPP) сприяє ефективному розподілу відповідальності за кібербезпеку між державою та бізнесом.

Одним із ключових викликів у сфері кіберзахисту критичної інфраструктури є стрімкий розвиток кіберзагроз. Нові методи атак, зокрема АРТ (Advanced Persistent Threats), атаки на ланцюги постачання та використання вразливостей у промислових системах, вимагають постійного оновлення нормативної бази та впровадження адаптивних механізмів захисту [2]. Тому важливим є створення механізмів швидкого реагування на інциденти, що передбачають обмін інформацією про загрози в режимі реального часу та координацію дій між різними суб'єктами кібербезпеки.

Ще одним важливим напрямом є посилення вимог до сертифікації засобів захисту та незалежного аудиту безпеки об'єктів КІ. Використання лише сертифікованих рішень дозволяє підвищити рівень довіри до систем захисту та зменшити ризики експлуатації вразливостей.

Крім технічних заходів, необхідно також зосередитися на людському факторі. Навчання персоналу, підвищення рівня обізнаності про кіберзагрози та розробка чітких інструкцій щодо реагування на інциденти відіграють важливу роль у забезпеченні кіберстійкості КІ. Регулярні тренування та симуляції атак дозволяють перевірити готовність до реальних загроз та вдосконалити процедури реагування.

Таким чином, ефективне правове регулювання та стандартизація заходів кіберзахисту критичної інфраструктури є важливими умовами безпечного функціонування державних і приватних структур. Комплексний підхід, що включає законодавчі ініціативи, міжнародне співробітництво та впровадження сучасних стандартів безпеки, дозволяє мінімізувати ризики та підвищити стійкість критичних систем до кібератак.

## **Література**

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT).
2. Директива (ЄС) 2022/2555 Європейського парламенту та Ради від 14 грудня 2022 року (NIS2).
3. Ністор О. М. Управління інформаційною безпекою підприємства : навчальний посібник. Київ : НАУ, 2020. 256 с.
4. Закон України "Про основні засади забезпечення кібербезпеки України". Відомості Верховної Ради України, 2017.

## **ЗАКОНОДАВЧА ТА НОРМАТИВНА БАЗА КІБЕРСТІЙКОСТІ**

**Астащенко М.О.**

Державний університет інформаційно-комунікаційних технологій  
м.Київ, Україна

Забезпечення кіберстійкості є одним із ключових пріоритетів для держав, бізнесу та міжнародних організацій. У зв'язку зі зростанням кіберзагроз уряди приймають нові закони та вдосконалюють нормативні акти для зміцнення цифрової безпеки. Міжнародна співпраця відіграє важливу роль у боротьбі з кіберзлочинністю та забезпеченні загальної кіберстійкості.

Імплементация міжнародних угод відіграє важливу роль у регулюванні кіберпростору. Будапештська конвенція[1] про кіберзлочинність є основним міжнародним документом, що регулює протидію кіберзлочинам, а Другий додатковий протокол до неї спрямований на спрощення обміну електронними доказами. Директива ЄС NIS2[2] встановлює посилені вимоги до кібербезпеки критичних секторів економіки. Міжнародна співпраця розвивається через ініціативи Європолу та Інтерполу[5], які створюють глобальні системи обміну

інформацією про кіберзлочини. НАТО уклало угоди щодо спільних операцій у разі кібератак.

Регулювання цифрової економіки охоплює впровадження стандартів кібербезпеки для електронної комерції, криптовалют і цифрового підпису. Фінансові організації, що працюють із цифровими активами, також підлягають регулюванню. Для вдосконалення правової бази необхідно покращити механізми екстрадиції кіберзлочинців, створити глобальні нормативи відповідальності за атаки на критичну інфраструктуру та запровадити міжнародний реєстр кіберзлочинців.

Більшість країн мають розроблені стратегії кібербезпеки, що визначають основні заходи із захисту цифрового простору. Законодавчі ініціативи включають ухвалення в Україні Закону "Про основні засади забезпечення кібербезпеки України"[4]. У США діє Закон про кібербезпеку 2022, що вимагає звітування компаній про кіберінциденти, а в ЄС прийнято Директиву NIS2, яка регулює безпеку даних. Захист критичної інформаційної інфраструктури забезпечується через обов'язкову сертифікацію підприємств у таких сферах, як енергетика, транспорт і фінанси. Для оперативного реагування на кіберінциденти створюються національні центри CERT та CSIRT.

Важливими напрямками удосконалення є впровадження обов'язкових аудитів кібербезпеки для державних і приватних установ, забезпечення прозорого фінансування державних програм кібербезпеки та підвищення кваліфікації спеціалістів у цій сфері.

Штучний інтелект, Інтернет речей та квантові обчислення створюють нові виклики у сфері кібербезпеки. В ЄС розробляється Закон про штучний інтелект, який визначає ризики та стандарти безпеки, а в Китаї діють закони, що обмежують використання ШІ у чутливих сферах. Для Інтернету речей запроваджуються стандарти безпеки, що спрямовані на запобігання масовим атакам. Регулюється і безпечне розгортання 5G-мереж для зменшення ризиків шпигунства та кібератак. Важливим напрямком удосконалення є встановлення

єдиних стандартів відповідальності за помилки штучного інтелекту, а також підвищення рівня криптографічного захисту IoT-пристроїв.

З огляду на зростаючі кібератаки питання захисту персональних даних стає дедалі актуальнішим. Регулювання персональних даних здійснюється на основі Загального регламенту захисту даних (GDPR)[3] в ЄС. В Україні ухвалено законопроект "Про захист персональних даних", який гармонізує законодавство з європейськими стандартами. Контроль за витоками інформації здійснюється через запровадження штрафів і вимог щодо обов'язкового повідомлення про витоки даних у багатьох країнах світу. Посилення відповідальності за витоки даних у державному секторі та розробка міжнародних механізмів запобігання нелегальному збору інформації є пріоритетними завданнями.

Жорсткість санкцій за кіберзлочини стала важливим кроком у боротьбі з кіберзлочинністю. У багатьох країнах введено кримінальну відповідальність за DDoS-атаки, фішинг і злом баз даних. Діють спеціалізовані підрозділи кіберполіції, що займаються розслідуванням кіберзлочинів. Для подальшого вдосконалення цієї сфери необхідно спростити юридичні процедури боротьби з міжнародною кіберзлочинністю та посилити відповідальність за атаки на критичну інфраструктуру.

## Література

1. Будапештська конвенція про кіберзлочинність: міжнародний договір від 23.11.2001 р. URL: [https://zakon.rada.gov.ua/go/994\\_575](https://zakon.rada.gov.ua/go/994_575)
2. Директива ЄС NIS2 щодо мережевої та інформаційної безпеки: Директива Європейського Парламенту і Ради ЄС від 14.12.2022 р. URL: <https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua>
3. Загальний регламент захисту даних (GDPR): Регламент ЄС 2016/679 від 27.04.2016 р. URL: <https://ccl.org.ua/positions/dyrektyva-yevropejskogo-soyuzu->

shhodo-merezhevoyi-ta-informacijnoyi-bezpeky-nis2-ta-robota-systemy-domennyh-imen-dns

4. Закон України "Про основні засади забезпечення кібербезпеки України" №2163-VIII від 05.10.2017 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

5. Політики та рекомендації Інтерполу та Європолу щодо кібербезпеки URL: <https://www.europol.europa.eu/cybercrime>

## **PCI DSS ТА SWIFT: ПРОБЛЕМАТИКА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ ВІДПОВІДНОСТІ**

**Касторнов К. Ф.**

Державний університет інформаційно-комунікаційних технологій  
м. Київ, Україна

Стандарти інформаційної безпеки, що регламентують захист даних фінансових установ, містять низку положень, впровадження яких може виявитися складним у контексті уніфікованого застосування. Ця складність зумовлена необхідністю адаптації загальних вимог до особливостей конкретних організацій, які або прагнуть отримати сертифікацію відповідно до відповідного стандарту, або самостійно забезпечують відповідність встановленим вимогам з метою підвищення рівня інформаційної безпеки.

Одним із таких регуляторних положень є вимога PCI DSS 11.4.3 щодо періодичного проведення зовнішніх тестувань на проникнення, а також їх здійснення після кожних значних змін в інфраструктурі. Однак визначення критичності змін та необхідність частого тестування створюють додаткове фінансове та операційне навантаження на організації, що працюють у сфері платіжних технологій. Таким чином, постає завдання розроблення методики,

яка дозволить диференціювати зміни за рівнем впливу на безпеку та оптимізувати підхід до тестувань.

Забезпечення постійної відповідності вимогам PCI DSS вимагає підтримання процесної відповідності стандарту протягом усього року між аудитами. Зокрема, вимога 11.4.3 [1] передбачає проведення зовнішніх тестувань після кожної значущої зміни в середовищі платіжних даних (CDE), включаючи модифікацію апаратного або програмного забезпечення, зміну потоків даних, оновлення допоміжної інфраструктури та зміну постачальників послуг [1]. Висока вартість таких тестувань зумовлює необхідність використання диференційованого підходу, який дозволить визначати реальну критичність змін та доцільність проведення позапланових тестувань.

Раціональним рішенням є застосування *customized approach*, який передбачає використання адаптивної методики оцінки значущості змін. Такий підхід, ґрунтуючись на принципах PCI DSS, враховує специфіку бізнес-процесів, масштаб інфраструктури та характер потенційних загроз, забезпечуючи оптимальний баланс між відповідністю стандарту та економічною доцільністю тестувань на проникнення. Це, своєю чергою, сприяє підвищенню ефективності безперервного контролю безпеки у фінансових установах.

Ще одним прикладом подібних вимог є необхідність не лише формального впровадження обов'язкових контролів, але й їх динамічної адаптації до змін у середовищі загроз. Так, контроль 4.2 (Operating System Privileged Accounts Control) [2] регламентує застосування багаторівневого контролю доступу до критичних облікових записів, що включає обов'язкове використання багатофакторної автентифікації (MFA) та мінімізацію доступу відповідно до принципу найменших привілеїв (PoLP).

Проте на практиці організації стикаються з низкою ускладнень під час впровадження цих вимог, зокрема через залежність від застарілих систем, труднощі інтеграції MFA з існуючими корпоративними середовищами, ризики,

пов'язані з використанням привілейованих облікових записів зовнішніми підрядниками та постачальниками послуг тощо.

Оптимізація механізмів контролю доступу до привілейованих облікових записів може бути реалізована через використання alternative implementations, що передбачає:

- контекстно-залежну автентифікацію, яка базується на поведінковому аналізі та геолокаційних даних користувача;
- динамічний моніторинг сесій привілейованих облікових записів із можливістю автоматичного блокування підозрілих дій;
- градуйоване застосування MFA, адаптоване до рівня ризику конкретної сесії;
- впровадження MFA за рахунок використання різних факторів на різних етапах отримання доступу до критичних систем (наприклад, доменна авторизація при підключенні до робочої станції, OTP, або подібна реалізація для VPN, двонаправлений (mutual) SSL для отримання доступу до адміністративної консолі) замість впровадження MFA на єдиному етапі отримання доступу до певних систем.

Таке рішення дозволить знизити ризики компрометації привілейованих облікових записів у SWIFT-інфраструктурі, забезпечуючи водночас врахування технологічних та організаційних обмежень фінансових установ.

Таким чином, впровадження стандартів інформаційної безпеки у фінансових організаціях потребує не лише формального дотримання нормативних вимог, але й адаптації контролів відповідно до реальних загроз та операційних особливостей. Використання гнучких методів оцінки змін та альтернативних механізмів контролю доступу є перспективним напрямом підвищення кіберстійкості фінансових установ, забезпечуючи баланс між інформаційною безпекою, відповідністю регуляторним вимогам та економічною ефективністю впровадження заходів захисту.

## Література

1. Стандарт PCI DSS (Payment Card Industry Data Security Standard) v4.0.1

URL: [https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4\\_0\\_1.pdf](https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf)

2. SWIFT CSCF (Customer Security Controls Framework) v2025. URL:

[https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf\\_dd/63.0/CSCF\\_v2025\\_20240701.pdf?logDownload=true](https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/63.0/CSCF_v2025_20240701.pdf?logDownload=true)