

ТРАДИЦІЇ
ЗНАННЯ
ІННОВАЦІЇ
БЕЗПЕКА
МАЙБУТНЄ



Державний університет
інтелектуальних технологій і зв'язку
Одеса, Україна

П
Н
З
І
—
8
—
2
0
2
6



ДУІТЗ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНТЕЛЕКТУАЛЬНИХ
ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ



ДУІКТ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

МАТЕРІАЛИ

VIII МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

**П
Н
З
І
—
2026**

**ЕРСПЕКТИВНІ
АПРЯМИ
АХИСТУ
ІНФОРМАЦІЇ
— 2026**

БЕЗПЕЧНЕ СУСПІЛЬСТВО
В ЦИФРОВОМУ СВІТІ



Одеса 2026 —

Міністерство освіти і науки України
Державний університет інтелектуальних технологій і зв'язку
Державний університет інформаційно-комунікаційних технологій

ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ

**Матеріали
VIII Міжнародної
науково-практичної конференції**

*26–28 серпня 2026 року
м. Одеса*

Одеса
«Астропринт»
2026

Рекомендовано до друку науково-технічною радою ДУІТЗ
(протокол № 6 від 21.09.2026 р.)

Перспективні напрями захисту інформації : матеріали VIII Між-П26 народної науково-практичної конференції (26–28 серпня 2026 р., м. Одеса) / Держ. ун-т інтелектуал. технологій і зв’язку ; Держ. ун-т інформ.-комуніац. технологій. — Одеса : Астропринт, 2026. — 180 с. ISBN 978-617-8714-60-4

У цьому збірнику містяться тези доповідей, представлених на Восьмій міжнародній науково-практичній конференції «Перспективні напрями захисту інформації», що відбулася 26–28 серпня 2026 року в Державному університеті інтелектуальних технологій і зв’язку (м. Одеса).

У публікаціях висвітлено сучасні теоретичні та практичні аспекти кібербезпеки, криптографічного захисту, технічного захисту інформації, а також нормативно-правові та організаційні питання забезпечення інформаційної безпеки в сучасних умовах.

Матеріали збірника будуть корисними для науковців, викладачів, аспірантів, студентів старших курсів відповідних спеціальностей, а також для практикуючих спеціалістів у сфері інформаційних технологій та захисту даних.

Матеріали доповідей друкуються в авторській редакції з оригіналів авторів. Відповідальність за зміст публікацій, точність викладених фактів, цитат, посилань та правопис несуть автори доповідей.

УДК 004.056

ПРОГРАМНИЙ КОМІТЕТ

Шульга В.П.	співголова програмного комітету, доктор історичних наук, проф., ректор ДУІКТ;
Назаренко О.А.	співголова програмного комітету, канд. фіз.-мат. наук, доц., ректор ДУІТЗ;
Корченко О.Г.	член-кореспондент НАН України, д.т.н., проф., перший проректор ДУІКТ;
Герасимов О.І.	д.ф.-м.н., проф., проректор з науково-педагогічної роботи та цифрової трансформації ДУІТЗ;
Карпінський М.П.	д.т.н., проф., зав. каф. програмної інженерії Університету Комісії національної освіти, Краків, Польща;
Бектурсунов Д.Н.	к.т.н., генеральний директор ТОВ НУРСАТ+, дочірня компанія АТ Казахтелеком, Алмати, Казахстан;
Іванченко Є.В.	д.т.н., проф., лауреат Національної премії України ім. Бориса Патона, директор ННІ кібербезпеки та захисту інформації ДУІКТ;
Легомінова С.В.	д.е.н., проф., зав. каф. систем та технологій кібербезпеки ДУІКТ;
Гайдур Г.І.	д.т.н., проф., зав. каф. управління кібербезпекою та захистом інформації ДУІКТ;
Туровський О.Л.	д.т.н., проф., зав. каф. технічних систем кіберзахисту ДУІКТ;
Васіліу Є.В.	д.т.н., проф., в.о. декана факультету інформаційних технологій та кібербезпеки ДУІТЗ;
Корчинський В.В.	д.т.н., зав. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Кільдішев В.Й.	д.т.н., доц. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Гаджиєв М.М.	д.т.н., проф., зав. каф. інженерії програмного забезпечення ДУІТЗ;
Фауре Е.В.	д.т.н., проф., проректор з науково-дослідної роботи та міжнародних зв’язків Черкаського державного технологічного університету;

Смірнов О.А.	д.т.н., проф., зав. каф. кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету;
Хлапонін Ю.І.	д.т.н., проф., проф. каф. інженерії програмного забезпечення та кібербезпеки Державного торговельно-економічного університету;
Рудницький В.М.	д.т.н., проф., г.н.с. Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки;
Степанов Д.М.	д.т.н., доц., зав. каф. комутаційних систем електронних комунікацій ДУІТЗ;
Онацький О.В.	к.т.н., доц. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Сідень С.В.	к.т.н., доц., зав. каф. радіоелектронних систем і технологій ДУІТЗ.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Донкогло А.С.	проректор з розвитку інфраструктури ДУІТЗ;
Васіліу Є.В.	д.т.н., проф., в.о. декана факультету інформаційних технологій та кібербезпеки ДУІТЗ;
Корчинський В.В.	д.т.н., зав. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Сідень С.В.	к.т.н., доц., зав. каф. радіоелектронних систем і технологій ДУІТЗ.
Кільдішев В.Й.	д.т.н., доц. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Стайкуца С.В.	к.ф.н., доц. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Севастєєв Є.О.	ст. викл. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Гавель С.В.	зав. лаб. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Пастухов Д.В.	викл. каф. кібербезпеки та технічного захисту інформації ДУІТЗ;
Гордієнко Д.В.	голова первинної профспілкової організації студентів ДУІТЗ.

ЗМІСТ

№		с.
1	<i>Азаров Іван Сергійович, Азаров Ілля Сергійович</i> НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ІДЕНТИФІКАЦІЇ АНОНІМНИХ КОРИСТУВАЧІВ ДЛЯ ЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР ВІД КІБЕРЗАГРОЗ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД	8
2	<i>Соколов С.М.</i> КІБЕРБЕЗПЕКА ПОТ-ОРІЄНТОВАНОЇ СИСТЕМИ МОНІТОРИНГУ ТА АВТОМАТИЧНОГО ЗУПИНЕННЯ СНС-ОБЛАДНАННЯ	12
3	<i>Гришук О. М., Гришук Р. В.</i> ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ВУЗЛА ВІД КІБЕРАТАК НА ОСНОВІ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ	15
4	<i>Мадінов М.Л., Галаган Н.В., Власенко В.О.</i> БАГАТОПАРАМЕТРИЧНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ У ВОЛОКОННО- ОПТИЧНИХ ЛІНІЯХ ЗВ’ЯЗКУ НА ОСНОВІ МОНІТОРИНГУ ФІЗИЧНОГО СТАНУ ОПТИЧНОГО ТРАКТУ	17
5	<i>Черемнов М.В., Фразе-Фразенко О.О.</i> СИНЕРГЕТИЧНИЙ МЕТОД БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	21
6	<i>Тимофєєв Д.С., Удовик І.М., Кручинін О.В.</i> ПІДВИЩЕННЯ ОСВІЩЕНОСТІ З ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В ПРОЦЕСІ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УНІВЕРСИТЕТУ	23
7	<i>Гончаров М.О., Колованова Є.П., Малахов С.В.</i> ОСНОВНІ СКЛАДОВІ КОНЦЕПЦІЇ БАГАТОРІВНЕВОГО МУЛЬТИПЛЕКСУВАННЯ ДАНИХ ПРИ РЕАЛІЗАЦІЇ ГІБРИДНОГО СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ	26
8	<i>Iurii Zhurov</i> BASELINE CONTROL COVERAGE IN RESOURCE-CONSTRAINED ORGANIZATIONS: STRUCTURAL CAUSES OF CYBERSECURITY UNDERINVESTMENT IN SMALL BUSINESS	30
9	<i>Зибін С.В., Прокопович-Ткаченко Д.І., Хохлачова Ю.Є.</i> ПІДВИЩЕННЯ ЖИВУЧОСТІ МЕРЕЖІ В УМОВАХ ДЕФІЦИТУ ЕЛЕКТРОЕНЕРГІЇ ТА КІБЕРАТАК	34
10	<i>Гавель С.М., Степанов В.О., Корчинський В.В., Богданюк І.А., Мар’ян М.О., Славич В.О.</i> АНАЛІЗ КОРЕЛЯЦІЙНИХ ВЛАСТИВОСТЕЙ ШУМОПОДІБНИХ ТАЙМЕРНИХ СИГНАЛІВ	38
11	<i>Сіренко О. І.</i> ОСОБЛИВОСТІ ВИЯВЛЕННЯ АТАК У КОНТЕЙНЕРИЗОВАНИХ СЕРЕДОВИЩАХ	40
12	<i>Бектурсунов Д.Н., Копитін Ю.В., Копитіна М.В., Корчинський В.В., Мартинова О.М., Дунаєва В.В.</i> МОДЕЛЬ ПРОЦЕСУ КІБЕРСТРАХУВАННЯ ДЛЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	43
13	<i>Царьов Р.Ю., Стайкуца С.В., Царьова Г.А.</i> ЗАСОБИ ШТУЧНОГО ІНТЕЛЕКТУ, ЯК ПЕРСПЕКТИВНА МОДЕЛЬ ЗАГРОЗИ СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	46
14	<i>Яневич О. К., Трифонова К. В., Лозовий О. О.</i> ІНТЕРФЕРЕНЦІЙНІ ЗАВАДИ У СИСТЕМАХ ШИРОКОСМУГОВОГО ДОСТУПУ МЕРЕЖАМИ БУДИНКОВОЇ ЕЛЕКТРОПРОВОДКИ, ПОБУДОВАНИМИ З ВИКОРИСТАННЯМ ПРОВІДІВ ТИПУ ШВВП ТА ВВГ-П	49
15	<i>Яневич О. К., Трифонова К. В., Чубарев О. В.</i> ІНТЕРФЕРЕНЦІЙНІ ЗАВАДИ У СИСТЕМІ ПЕРЕДАЧІ ВРЛС ПРИ ВПЛИВІ ІМПУЛЬСНИХ БЛОКІВ ЖИВЛЕННЯ	51
16	<i>Karpenko Y.V., Dubrovin V.I</i> DETECT NETWORK ATTACKS: Quantum Implementation	52
17	<i>Корченко А.О., Петченко М.В., Давиденко К.О.</i> ПРОФІЛЮВАННЯ СОЦІОТЕХНІКА ЗА ОЗНАКАМИ ВИЯВЛЕНОЇ ФІШИНГ-АТАКИ	56
18	<i>Шкурченко О.А., Аверічев І.М., Поночовний П.М.</i> МЕТОД ДЕТЕКТУВАННЯ МУЛЬТИВЕКТОРНИХ АРТ-АТАК ІЗ ВИКОРИСТАННЯМ АНСАМБЛІВ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ	58
19	<i>Бабенко К. Є.</i> МОДЕЛЬ НАСКРІЗНОЇ ЗАТРИМКИ ДОСТУПУ ДО ОНОВЛЕНОГО СТАНУ ПРОГРАМОВАНИХ БЛОКЧЕЙН-СИСТЕМ ПЕРШОГО РІВНЯ	60

20	<i>Аверічев І.М., Зарванський М. В.</i> ФІШИНГ У КОРПОРАТИВНИХ СЕРЕДОВИЩАХ КОМУНІКАЦІЇ (SLACK, MICROSOFT TEAMS, DISCORD)	62
21	<i>Хохлячова Ю. Є., Аскеров М.Г.</i> ДОКАЗОВО КЕРОВАНІЙ ЦИФРОВИЙ ДВІЙНИК ДЛЯ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СМАРТ-РЕГІОНУ	64
22	<i>Корченко О.Г., Хохлячова Ю.Є.</i> ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ТЕОРЕТИКО-МНОЖИННОЇ МЕТРИЧНОЇ МОДЕЛІ	67
23	<i>Костюніна О. В.</i> КІБЕРБЕЗПЕКА ТА ЦИФРОВА СУПЕРВІЗІЯ: АНАЛІЗ РИЗИКІВ ТА ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ШІ-СИМУЛЯЦІЙ У ПІДГОТОВЦІ ПСИХОЛОГІВ	70
24	<i>Прокопович-Ткаченко Д. І.</i> АДАПТИВНА МІЖРІВНЕВА КООРДИНАЦІЯ МЕХАНІЗМІВ КІБЕРЗАХИСТУ І ВІДНОВЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ	73
25	<i>Онтіверо-Валлс А.</i> АНАЛІЗ КРИПТОГРАФІЧНИХ ПАРАМЕТРІВ БЕЗПЕКИ У TLS-HANDSHAKE НА ОСНОВІ ДОСЛІДЖЕННЯ CLIENT HELLO ТА SERVER HELLO	75
26	<i>Бибік Р.Т.</i> ДОСЛІДЖЕННЯ ВПЛИВУ ПОХИБОК ТА ШУМІВ НА ХАРАКТЕРИСТИКИ ІСНУЮЧИХ МЕТОДІВ ПРОСТОРОВО-ЧАСТОТНОГО ОРІЄНТУВАННЯ	78
27	<i>Бондаренко Є., Волошин В.</i> АЛГОРИТМ ОЦІНКИ ВПЛИВУ ЗАВАД НА ФАЗОВУ ПОМИЛКУ ДИСКРЕТНОЇ СИСТЕМИ СИНХРОНІЗАЦІЇ В СТАЛИХ РЕЖИМАХ СТЕЖЕННЯ ЗА НЕСУЧОЮ ЧАСТОТОЮ	84
28	<i>Васіліу Є.В., Назаренко О.А., Стайкуца С.В., Іванов В.І.</i> ПРОТОКОЛ КВАНТОВОГО РОЗДІЛЕННЯ СЕКРЕТУ НА ОСНОВІ ТРИКУБІТНИХ ГХІ-СТАНІВ ІЗ ДВОЕТАПНИМ КОНТРОЛЕМ КВАНТОВИХ КАНАЛІВ	87
29	<i>Платонова А.Ю., Севастєєв Є.О.</i> ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ВЗАЄМОДІЇ КОРИСТУВАЧА З LLM	90
30	<i>Зоріло В.В., Дудзинська Д.С.</i> ДОСЛІДЖЕННЯ ВПЛИВУ РОЗМИТТЯ ЗА ГАУСОМ НА ШУМОВІ ХАРАКТЕРИСТИКИ ЦИФРОВОГО ЗОБРАЖЕННЯ	91
31	<i>Куліковський Д.В., Бабіч Ю.О.</i> КІБЕРБЕЗПЕКОВІ РИЗИКИ ГОЛОСОВОЇ БІОМЕТРІЇ ТА ПРАВОВІ НАСЛІДКИ ЇХ РЕАЛІЗАЦІЇ У ПЛАТІЖНИХ ОПЕРАЦІЯХ	94
32	<i>Клейн О. М., Савенко Б. О.</i> МЕТОД РАНЖУВАННЯ ПРИЧИННО-ПОВ’ЯЗАНИХ ПОДІЙ БАГАТОКРОКОВОЇ КОМП’ЮТЕРНОЇ АТАКИ НА ОСНОВІ БАЙЄСІВСЬКОЇ МЕРЕЖІ	97
33	<i>Михайленко Г. О.</i> АВТОМАТИЗАЦІЯ ПРОЦЕСІВ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ N8N	101
34	<i>Мохор В.В., Дорогий Я.Ю., Ракович В.С., Цуркан В.В.</i> ПОГЛЯД НА ПАРАДИГМУ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	104
35	<i>Сільвейструп О.Р.</i> СИСТЕМА ФІЛЬТРАЦІЇ HTTP-ТРАФІКУ ВЕБ-ДОДАТКІВ WAF З ВИКОРИСТАННЯМ ML	106
36	<i>Горицький В.М.</i> БЕЗПЕКА ЗВ’ЯЗКУ ФІЗИЧНОГО РІВНЯ В МЕРЕЖАХ 5G/6G НА ОСНОВІ ЙМОВІРНІСНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ	109
37	<i>Дикий О.В., Соколов А.В.</i> ОЦІНЮВАННЯ ЛІНІЙНИХ ВЛАСТИВОСТЕЙ S-БЛОКІВ НА ОСНОВІ ЧЕТВІРКОВОЇ МОДЕЛІ АПРОКСИМАЦІЇ	113
38	<i>Царьов Р.Ю., Сідень С.В., Павлов А.С., Царьова А.Р.</i> ПОКАЗНИКИ ЯКОСТІ, ПЕРЕХІД ВІД МЕРЕЖ 5G ДО	117
39	<i>Царьов Р.Ю., Царьова А.Р., Андрухів Т.В., Міщенко Д.С.</i> ВИБІР КІЛЬКОСТІ ТОЧОК РОЗПОДІЛУ КАБЕЛЬНОЇ СИСТЕМИ ДЛЯ СЕНСОРНОГО СЕГМЕНТА ІНТЕРНЕТУ РЕЧЕЙ	120
40	<i>Іщенко А. Д., Русаловський В. Б., Калюжний Л. В., Рущенко О. В.</i> МЕХАНІЗМ АВТЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ПЛАГІНА MOSQUITTO-AUTH-PLUGIN У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ З ТОПОЛОГІЄЮ MESH	123

41	<i>Русаловський В.Б., Калюжний Л.В., Іщенко А.Д., Воронюк Д.В.</i> КОМПЛЕКСНА СИСТЕМА МОНІТОРИНГУ ТА АДАПТИВНОЇ ФІЛЬТРАЦІЇ НЕБЕЗПЕЧНОГО КОНТЕНТУ ДЛЯ КІБЕРЗАХИСТУ ДІТЕЙ У ЗАКЛАДАХ ОСВІТИ	125
42	<i>Кривченко А.А., Кривченко Ю.В.</i> РЕАЛІЗАЦІЯ ПРОГРАМНОЇ МОДЕЛІ АНАЛІЗУ ЗАХИЩЕНОСТІ КОМП’ЮТЕРНОЇ МЕРЕЖІ	129
43	<i>Бакалинський О.О.</i> АКСІОМАТИЧНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ КРИТИЧНИХ ФУНКЦІЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	131
44	<i>Анісімова К. С.</i> ТЕХНОЛОГІЇ ЕЛЕКТРОННОГО ВРЯДУВАННЯ ЯК ІНСТРУМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ УКРАЇНИ	133
45	<i>Басов В.Є., Басов С.В.</i> АНАЛІЗ КРИПТОГРАФІЧНИХ ВЛАСТИВОСТЕЙ ПОВНОЇ МНОЖИНИ БІЄКТИВНИХ ТРІЙКОВИХ S-БЛОКІВ РОЗМІРНОСТІ 2×2.	134
46	<i>Развалінов В., Русаловський В. Б., Басаковський В. А.</i> МЕТОД АДАПТИВНОГО ФОРМУВАННЯ СЕМАНТИЧНОГО ВІДЕОПОВІДОМЛЕННЯ З УРАХУВАННЯМ СТАНУ БЕЗДРОТОВОГО КАНАЛУ	137
47	<i>Трухан Д.В.</i> МЕТОДИ ТА МОДЕЛІ ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ З УРАХУВАННЯМ СТУПЕНЯ ПЕРЕКРИТТЯ ЗАГРОЗ	142
48	<i>Кононович В.Г., Стайкуца С.В.</i> СТРУКТУРНА ЦІЛІСНІСТЬ, НЕПОДІЛЬНІСТЬ ТА ЕМЕРДЖЕНТНІСТЬ – ФУНДАМЕНТАЛЬНІ ВЛАСТИВОСТІ СУЧАСНИХ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ. НАСЛІДКИ	144
49	<i>Тарасенко Я.В., Матусяк П.О.</i> ПРОБЛЕМИ РОЗМЕЖУВАННЯ ШТАТНИХ ТА АНОМАЛЬНИХ ЗМІН ІНФОРМАЦІЙНОГО СТАНУ КІБЕРФІЗИЧНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ ВІМІРЮВАННЯ	148
50	<i>Орлов Р.Р., Тарасенко Я.В.</i> ВІМІРЯНА КРИТИЧНІСТЬ ЯК ІНФОРМАЦІЙНА ОСНОВА ПРОГНОЗНОГО ОЦІНЮВАННЯ РИЗИКУ КІБЕРІНЦИДЕНТІВ	150
51	<i>Рябко І. Б., Ключініков І. М.</i> ОЦІНЮВАННЯ КРИТИЧНОСТІ ВІДМОВ БЕЗПЕКИ МЕДИЧНОЇ ЗОБРАЖУВАЛЬНОЇ КІБЕРФІЗИЧНОЇ СИСТЕМИ МЕТОДОМ IMESA	152
52	<i>Кулієв Р.Д.</i> МЕТОДИКА ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ КІБЕРЗАХИСТУ ДАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ РОЗПОДІЛЕНОГО РЕЄСТРУ	154
53	<i>Царьов Р.Ю., Квачук В.О., Опотяк Ю.В., Царьова Г. А.</i> АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СЕРВІСНИХ ПЛАТФОРМ НАДАННЯ ВЕБСЕРВІСІВ ЗА СКЛАДОВИМИ ПОКАЗНИКА НЕДОСТУПНОСТІ	157
54	<i>Царьов Р.Ю., Коваленко І.О., Андрухів Т.В.</i> КРИТЕРІЙ ДОЦІЛЬНОСТІ РЕКОНСТРУКЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ	161
55	<i>Вакар О.А., Карповський О.І.</i> АНАЛІЗ STF-ЗАВДАНЬ	164
56	<i>Бубенцова Л.В., Царьов Р.Ю.</i> ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ З ВИСОКИМ РІВНЕМ РИЗИКУ	166
57	<i>Хлапонін Ю.І.</i> ГУМАНОЇДНІ РОБОТИ В ЦИФРОВІЙ ЕКОСИСТЕМІ SMART CITY: МОЖЛИВОСТІ, ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКОВІ РИЗИКИ	169
58	<i>Хомутов О.О., Онацький О.В.</i> СЕМАНТИЧНО ОРІЄНТОВАНА СИСТЕМА ВІЯВЛЕННЯ КІБЕРАТАК НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ У SOC	171
59	<i>Сідень С.В., Кутовий М.Г.</i> АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ’ЯЗКУ 5G/6G	173
60	<i>Большакова О.В.</i> АДМІНІСТРАТИВНО-ПРАВОВІ ІНСТРУМЕНТИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: ПРАВОВІ КОЛІЗІЇ ТА НАПРЯМИ РЕФОРМУВАННЯ	176

НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ІДЕНТИФІКАЦІЇ АНОНІМНИХ КОРИСТУВАЧІВ ДЛЯ ЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР ВІД КІБЕРЗАГРОЗ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

Державний університет інформаційно-комунікаційних технологій,
вул. Солом'янська, 7, 03110, Київ, Україна
azarovphone@gmail.com, azarovforce@gmail.com

Анотація. Розглянуто нормативно-правове підґрунтя ідентифікації анонімних користувачів, дії яких загрожують об'єктам критичної інфраструктури. Порівняно одинадцять чинних актів України, Європейського Союзу і Каліфорнії за шістьма критеріями: анонімність, ідентифікація, персональні дані, параметри ідентифікації, параметри анонімності та охоплення критичної інфраструктури.

Показано, що вітчизняні акти не оперують поняттям анонімності і не називають мережових параметрів, тоді як міжнародні прямо відносять до ідентифікаторів IP-адресу, файли cookie та інші мережові ознаки. Окреслено напрям усунення виявленого розриву в межах подальшого дослідження методів ідентифікації та класифікації рівня анонімності користувачів.

Ключові слова: ідентифікація анонімних користувачів, критична інфраструктура, нормативно-правове регулювання, персональні дані, параметри ідентифікації, кіберзагрози.

1. Вступ

Захист критичної інфраструктури дедалі частіше зводиться до спроможності встановити, хто звертається до інформаційного ресурсу. Зловмисник, який діє через засоби анонімізації, залишається для системи захисту знеособленим, тому розмежування доступу, блокування та притягнення до відповідальності проти нього не спрацьовують. Стратегія кібербезпеки України відносить захист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури до пріоритетів національної безпеки, тож ідентифікація анонімних користувачів набуває і правового виміру [1].

Технічні методи формування цифрового відбитка випереджають правові конструкції, у межах яких їх застосовують.

Тому метою цієї роботи є проведення порівняльного аналізу вітчизняних і міжнародних нормативно-правових вимог щодо ідентифікації користувачів та захисту критичної інфраструктури, виявленні прогалин у регулюванні анонімності й визначенні правових обмежень для подальшого наукового дослідження.

2. Багаторівневість правового поля ідентифікації користувачів

Правове поле, у якому діють технології ідентифікації користувачів, утворене кількома рівнями регулювання. Наднаціональний рівень охоплює право Європейського Союзу. Національний рівень становлять законодавство України та законодавство окремих іноземних юрисдикцій, зокрема штату Каліфорнія. Секторальний рівень представлений актами у сфері кібербезпеки та захисту критичної інфраструктури. Спільним для всіх трьох є те, що складові цифрового відбитка, серед яких IP-адреса, ідентифікатори пристрою та файли cookie, здебільшого підпадають під означення персональних даних. Тому їх збирання й обробка регулюються законодавством про захист даних.

Для інженерної практики звідси впливає подвійний наслідок. Будь-який метод ідентифікації анонімного користувача наперед є обробкою персональних даних і потребує правової підстави. Водночас жоден із проаналізованих актів не оперує поняттям анонімного користувача та не встановлює критеріїв його розпізнавання, тому підстава для зворотної задачі лишається невизначеною.

3. Механізм адаптації законодавства України до права Європейського Союзу

Зіставлення вітчизняного та європейського регулювання потребує попереднього уточнення юридичної природи такого зіставлення. Акти Європейського Союзу не діють на території України як норми прямої дії і не мають сили вищого закону. Обов'язковість вимог європейського права виникає для України опосередковано, через міжнародно-правове зобов'язання привести національне законодавство у відповідність до *acquis communautaire*. Базовим інструментом такого зобов'язання є Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами членами, з іншої сторони. Її підписано 21.03.2014 у політичній частині та 27.06.2014 в економічній частині, ратифіковано Законом України від 16.09.2014 № 1678-VII, і вона чинна з 01.09.2017 [2]. Внутрішній механізм адаптації запроваджено раніше, Законом України від 18.03.2004 № 1629-IV «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу», який визначає адаптацію пріоритетною складовою процесу інтеграції та встановлює її поетапність [3]. Цей механізм діє й дотепер.

Євроінтеграційна динаміка останніх років посилила це зобов'язання. Рішенням Європейської Ради від 23.06.2022 Україні надано статус країни кандидата на вступ до Європейського Союзу [4]. Пізніше, 15.06.2026, на другій Міжурядовій конференції Україна - ЄС відкрито перший переговорний кластер «Основи», який охоплює верховенство права та основоположні права, функціонування демократичних інститутів і реформу публічного адміністрування [5]. Саме до цього кластера належать питання захисту персональних даних та меж

допустимого втручання у приватність, тобто та сама площина, у якій розташована задача ідентифікації користувачів. Для теми дослідження це означає, що вимоги європейських актів щодо обробки ідентифікаційних даних та щодо кіберзахисту критичної інфраструктури перестають бути зовнішнім орієнтиром і переходять у площину зобов'язань, під які має бути приведено українське законодавство. Оскільки об'єкти критичної інфраструктури є транскордонно взаємозалежними, а атаки на них здійснюються переважно знеособленими суб'єктами, імплементація узгоджених вимог до ідентифікації є не формальною вимогою членства, а безпосередньою умовою обороноздатності відповідних систем.

4. Порівняльний аналіз нормативно-правових актів

Для аналізу обрано шість параметрів правомірності ідентифікації анонімного користувача: анонімність, ідентифікація, персональні дані, параметри ідентифікації, параметри анонімності та охоплення критичної інфраструктури. Перші три показують, чи оперує акт поняттям на рівні означення, тобто чи є правова підстава розпізнавати особу за слідами в мережі. Наступні два розкривають, які ознаки акт визнає придатними для розпізнавання і які засоби їх приховування унормовує. Останній показує, чи поширюється дія акта на об'єкти критичної інфраструктури.

Легенда таблиці 1. Категорія «Пряме» означає пряме унормування відповідного параметра в акті; категорія «Часткове» вказує на опосередковане унормування, коли положення виводиться із суміжних норм або охоплює лише окремих аспект параметра; категорія «Відсутнє» вказує на відсутність норми. Поряд із категорією наведено стислий зміст норми та статті акта. Рядки-підзаголовки поділяють таблицю на три юрисдикційні блоки: національне законодавство України, міжнародне законодавство та акти Європейського Союзу, законодавство США.

Таблиця 1. Нормативно-правові акти, дотичні до ідентифікації користувачів та захисту критичної інфраструктури (станом на дату звернення 14.08.2026)

Акт	Анонімність	Ідентифікація	Персональні дані	Параметри ідентифікації	Параметри анонімності	Охоплення критичної інфраструктури
НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО (УКРАЇНА)						
Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [6]	Часткове: знеособлення персональних даних, ст. 2	Пряме: конкретно ідентифікована особа, ст. 2	Пряме: означення персональних даних, ст. 2	Часткове: біометричні та генетичні дані, ст. 7	Часткове: знеособлення без опису методів, ст. 2	Відсутнє
Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [7]	Відсутнє	Відсутнє	Часткове: об'єкти кіберзахисту, ст. 4	Відсутнє	Відсутнє	Пряме: об'єкти критичної інфраструктури, ст. 1, у зв'язку із Законом № 1882-IX
Закон України «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 № 2155-VIII [8]	Відсутнє	Пряме: електронна ідентифікація, ст. 1	Часткове: ідентифікаційні дані особи, ст. 1	Часткове: біометрія і риси користувача, ст. 1, 15	Відсутнє	Відсутнє
Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX [9]	Відсутнє	Часткове: лише ідентифікація об'єкта, ст. 1	Відсутнє	Відсутнє	Відсутнє	Пряме: означення і категорії критичності, ст. 1, 10
Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX [10]	Пряме: знеособлене (анонімне) отримання послуг, ст. 104 ч. 5, та заборона розшифрування, ст. 107 ч. 1 п. 16	Часткове: обов'язок постачальника забезпечити електронну ідентифікацію середнього і високого рівнів довіри, ст. 107 ч. 2	Часткове: власного означення немає, відсилання до Закону № 2297-VI, ст. 18 п. 3, ст. 117 ч. 4	Часткове: маршрути передачі, місцезнаходження та спроби виклику, ст. 119 ч. 1	Часткове: умови виходу з анонімності без переліку ознак, ст. 107 ч. 2, ст. 113	Часткове: безпека і сталість мереж, ст. 31, критична інформаційна інфраструктура, ст. 27

Продовження Таблиці 1

Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» від 20.11.2012 № 5492-VI [11]	Відсутнє	Пряме: ідентифікація особи, ст. 3	Пряме: склад даних Реєстру, ст. 7	Пряме: відцифровані підпис, образ обличчя та відбитки пальців, ст. 3, 7	Відсутнє	Відсутнє
МІЖНАРОДНЕ ЗАКОНОДАВСТВО ТА АКТИ ЄС						
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція № 108) [12]	Відсутнє	Часткове: особа, що може бути конкретно визначеною, ст. 2	Пряме: означення персональних даних, ст. 2	Відсутнє	Відсутнє	Відсутнє
Регламент (ЄС) 2016/679 (GDPR) [13]	Часткове: анонімна інформація поза сферою дії, п. 26 преамбули	Пряме: ідентифіковува на фізична особа, ст. 4(1)	Пряме: означення персональних даних, ст. 4(1)	Пряме: IP-адреси, файли cookie, радіочастотна ідентифікація RFID, п. 30 преамбули	Пряме: псевдонімізації, ст. 4(5)	Відсутнє
Директива 2002/58/ЄС від 12.07.2002 (ePrivacy) у редакції Директиви 2009/136/ЄС від 25.11.2009 [14, 15]	Відсутнє	Відсутнє	Часткове: інформація в термінальному обладнанні, ст. 5(3)	Часткове: файли cookie, п. 25 преамбули первинної редакції	Відсутнє	Відсутнє
Директива (ЄС) 2022/2555 (NIS 2) [16]	Відсутнє	Часткове: ідентифікація інцидентів, п. 121 преамбули	Часткове: дані, що обробляються для реагування на інциденти, п. 121 преамбули	Часткове: IP-адреси, веб-адреси URL, доменні імена та адреси електронної пошти, п. 121 преамбули	Відсутнє	Пряме: основні та важливі суб'єкти, ст. 3, додатки I і II
ЗАКОНОДАВСТВО США						
California Consumer Privacy Act (CCPA) у редакції California Privacy Rights Act (CPRA) [17]	Відсутнє	Пряме: унікальний ідентифікатор, ймовірнісний ідентифікатор, критерій «більш імовірно, ніж ні», тобто понад 50 %, розділ 1798.140	Пряме: персональна інформація, розділ 1798.140	Пряме: IP-адреси, онлайн-ідентифікатори, файли cookie, розділ 1798.140	Часткове: псевдонімізації, розділ 1798.140	Відсутнє

Розподіл оцінок у таблиці 1 є дзеркальним. Акти у сфері захисту даних, від Закону України № 2297-VI до Регламенту (ЄС) 2016/679, мають оцінку «Пряме» за персональними даними і «Відсутнє» за охопленням критичної інфраструктури, тоді як секторальні акти - Закони України № 2163-VIII і № 1882-IX та Директива (ЄС) 2022/2555 - охоплюють критичну інфраструктуру, проте ідентифікаційних ознак користувача не називають. Жоден акт не сполучає обидві площини. Оцінка «Часткове» переважає там, де положення виводять із суміжних норм, а ідентифікатори Закону України № 5492-VI є суто документарними, а не мережевими, тому для розпізнавання суб'єктів кіберзагроз непридатні.

Найпоказовішим є зіставлення за анонімністю та її параметрами. Жоден з одинадцяти актів не подає визначення анонімного користувача, переліку ознак для його розпізнавання чи порогових значень, що відмежовували б звичайне користування засобами приватності від зловживання нею. Найближчими є Закон України № 1089-IX із правом на знеособлене отримання послуги та Регламент (ЄС) 2016/679 із псевдонімізацією, проте обидва описують стан даних чи умови надання послуги, а не стан користувача, який навмисно приховує свої мережеві ознаки.

5. Аналітичні висновки зіставлення

Дефініція персональних даних у Регламенті (ЄС) 2016/679 ширша за означення чинного Закону України № 2297-VI, бо прямо охоплює онлайн-ідентифікатори. На усунення розбіжності спрямований законопроект № 8153, прийнятий за основу 20.11.2024. Розрив означень лишається відкритим.

Регулювання цифрового відбитка в Європейському Союзі й надалі спирається на Директиву 2002/58/ЄС, оскільки проєкт нового регламенту про приватність електронних комунікацій відкрито рішенням Європейської комісії від 16.07.2025. Тому режим згоди на доступ до інформації на кінцевому обладнанні лишається чинним обмеженням для активних методів ідентифікації.

Пряме значення для критичної інфраструктури мають Директива (ЄС) 2022/2555, яка розширює коло підзвітних суб'єктів і вимоги до реагування, та Закон України № 1882-IX, що визначає національний режим таких об'єктів. Обидва зобов'язують виявляти та зупиняти кіберінциденти, не надаючи інструментарію для встановлення того, хто їх спричиняє. Обов'язок є, а інструмента немає.

Транскордонний характер кібератак обумовлює міжнародний вимір проблеми: як зазначено у фахових джерелах, ефективний кіберзахист критичної інфраструктури та збереження конфіденційності даних у кіберпросторі неможливі в межах виключно національного контуру й вимагають гармонізованого міждержавного регулювання [18].

6. Висновки

1. Правове поле ідентифікації багаторівневе, а складові цифрового відбитка, як-от IP-адреса, ідентифікатори пристрою та файли *cookie*, на всіх рівнях є персональними даними, тому будь-який метод ідентифікації анонімного користувача є їх обробкою і потребує правової підстави.

2. Зіставлення права Європейського Союзу та законодавства України юридично коректне, оскільки європейські акти не діють в Україні як норми прямої дії, але підлягають імплементації через механізм адаптації, закріплений Угодою про асоціацію та Законом України № 1629-IV і посилений набуттям статусу країни кандидата й відкриттям переговорного кластера «Основи».

3. Означення персональних даних у Регламенті (ЄС) 2016/679 ширше за означення Закону України № 2297-VI, а розбіжність усуває законопроект № 8153, прийнятий за основу 20.11.2024, тому цей напрям гармонізації першочерговий для правомірного застосування методів ідентифікації.

4. Секторальні акти, Закони України № 2163-VIII і № 1882-IX та Директива (ЄС) 2022/2555 зобов'язують захищати критичну інфраструктуру, проте ознак ідентифікації користувача не визначають, а сама директива згадує IP- і вебадреси лише в пункті 121 преамбули, у контексті реагування на інциденти. Тому обов'язок протидії кіберзагрозі не має правового інструмента встановлення джерела.

5. Жоден з одинадцяти актів не дає ні означення анонімного користувача, ні параметрів виявлення для протидії кіберзагрозам. Право захищає дані ідентифікованої особи, а зворотна задача, легітимна ідентифікація того, хто зловживає анонімністю проти критичної інфраструктури, поза регулюванням.

6. Виявлена прогалина є одночасно термінологічною і правовою. Це обґрунтовує потребу подальшого наукового дослідження методів ідентифікації та класифікації рівня анонімності користувачів для захисту критичної інфраструктури в межах чинних вимог щодо обробки персональних даних.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021> (дата звернення: 13.08.2026).
2. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : міжнародний договір від 27.06.2014 : ратифіковано Законом України від 16.09.2014 № 1678-VII : чинна з 01.09.2017 : редакція від 14.10.2025. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 13.08.2026).
3. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу : Закон України від 18.03.2004 № 1629-IV : редакція від 04.11.2018 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1629-15> (дата звернення: 13.08.2026).
4. European Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations, 23 June 2022 : EUCO 24/22. URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/> (дата звернення: 13.08.2026).
5. EU and Ukraine open first accession negotiations cluster : European Commission, Directorate-General for Enlargement and Eastern Neighbourhood, 15.06.2026. URL: https://enlargement.ec.europa.eu/news/eu-and-ukraine-open-first-accession-negotiations-cluster-2026-06-15_en (дата звернення: 13.08.2026).

6. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : редакція від 14.06.2025 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 13.08.2026).

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 19.10.2025 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 13.08.2026).

8. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII : редакція від 18.12.2024 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 13.08.2026).

9. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : редакція від 21.09.2024 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1882-20> (дата звернення: 13.08.2026).

10. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : редакція від 30.05.2026 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1089-20> (дата звернення: 13.08.2026).

11. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 № 5492-VI : редакція від 27.06.2026 / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/5492-17> (дата звернення: 13.08.2026).

12. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Рада Європи, 28.01.1981 : ратифіковано Законом України від 06.07.2010 № 2438-VI : чинна для України з 01.01.2011. Офіційний вісник України. 2011. № 1. Ст. 85. URL: https://zakon.rada.gov.ua/laws/show/994_326 (дата звернення: 13.08.2026).

13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1-88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 13.08.2026).

14. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Communities. 2002. L 201. P. 37. URL: <https://eur-lex.europa.eu/eli/dir/2002/58/oj> (дата звернення: 13.08.2026).

15. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. Official Journal of the European Union. 2009. L 337. P. 11-36. URL: <https://eur-lex.europa.eu/eli/dir/2009/136/oj> (дата звернення: 13.08.2026).

16. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/172, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union. 2022. L 333. P. 80-152. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата звернення: 13.08.2026).

17. Law & Regulations : California Privacy Protection Agency : офіційний вебсайт. URL: <https://cprpa.ca.gov/regulations/> (дата звернення: 13.08.2026).

18. Данченко Т. В., Грозан В. О. Співробітництво держав щодо забезпечення захисту особистих даних у кіберпросторі. Молодий вчений. 2021. № 5 (93). С. 312-315. DOI: <https://doi.org/10.32839/2304-5809/2021-5-93-59> (дата звернення: 13.08.2026).

УДК 004.7:621.9

Соколов С.М.

**КІБЕРБЕЗПЕКА ІОТ-ОРІЄНТОВАНОЇ СИСТЕМИ МОНІТОРИНГУ
ТА АВТОМАТИЧНОГО ЗУПИНЕННЯ СНС-ОБЛАДНАННЯ**

Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, Україна
s.sokolov@csn.khai.edu

Анотація. Розглянуто вимоги до кіберзахисту Іот-орієнтованої системи моніторингу СНС-операцій, інтегрованої з ERP/PDM/MES IT-Enterprise та здатної ініціювати автоматичне або напівавтоматичне зупинення обладнання. Запропоновано зоновану ОТ/ІТ-архітектуру (виробничий/корпоративний рівні) з промисловою DMZ (Demilitarized Zone), локальним контуром прийняття рішень, криптографічним захистом OPC UA (Open Platform Communications Unified Architecture), розмежуванням прав і незмінним журналюванням. Визначено заходи протидії підміні телеметрії, повторному відтворенню команд, компрометації нейромоделі та витоків технологічної інформації. Обґрунтовано, що ERP не повинна мати прямого керуючого доступу до верстата, а критичні команди мають проходити локальну перевірку безпеки.

Ключові слова: CNC, Іот, кібербезпека, ОТ, ERP, IT-Enterprise, OPC UA, автоматичне зупинення, цифровий двійник.

Актуальність та характер загроз. Система контролю CNC-операцій на машинобудівному підприємстві об'єднує верстат із ЧПУ, датчики та сенсори, Іот-шлюз, аналітичний модуль, технологічна операція у цифровому поданні, а також ERP систему (в нашому case study це українська IT-Enterprise). Ця система обробляє різні параметри: оберти шпинделя, подача по осях, координати, вібрації, температури, струми приводів, стан програми, інструмент й партії деталей, і в процесі своєї роботи може сформувати попередження, коригування або команду зупинення. Через фізичний вплив на обладнання така система належить до операційного рівня, де порушення цілісності або доступності може мати наслідком брак, пошкодження інструменту, невідповідний простій, аварійну ситуацію. NIST SP 800-82 Rev. 3 рекомендує проєктувати захист ОТ з урахуванням специфічних вимог до безпеки, надійності та реального часу [1]. Основними загрозами є підміна Іот-телеметрії, атака типу «людина посередині», повторне виконання раніше виконаної валідної команди, крадіжка облікових даних, переміщення даних з корпоративної мережі до ОТ, шкідлива зміна порогів або нейромоделі, відмова в обслуговуванні та витік CNC-програм, параметрів режимів різання, даних про деталі й виробничі замовлення.

Сегментація та напрямки обміну. Архітектуру доцільно будувати за принципом зон і каналів ISA/IEC 62443 [2, 3]. Окремими зонами мають бути: верстати та локальні контролери; промислові edge-шлюзи; промислова демілітаризована зона (IDMZ) з брокером, історіаном(для збору, зберігання та аналізу історичних даних від обладнання) та сервісом інтеграції; корпоративна зона ERP; зона адміністрування та резервного копіювання. Прямий маршрут ERP–CNC забороняється. Обмін даними з ERP містить лише необхідний виробничий контекст і перевірені агреговані дані, тоді як технологічні дані спочатку обробляються локально. За відсутності потреби у передачі команд керування доцільно використовувати односторонній канал або шлюз, налаштований тільки на публікацію Іот. Якщо двосторонній обмін потрібен, то дозволяється лише явно визначені сервіси, адреси, типи повідомлень і частоти запитів; будь-які інші з'єднання блокуються міжмережевими екранами ОТ-класу.

Захищена передача даних. Для машинного рівня доцільно використовувати OPC UA у режимі SignAndEncrypt із взаємною автентифікацією застосунків за сертифікатами X.509, перевіркою списків довіри та відкликання сертифікатів. Захищений канал OPC UA забезпечує конфіденційність, цифровий підпис повідомлень, цілісність даних та автентифікацію клієнта і сервера [4]. Галузева специфікація OPC UA для верстатів забезпечує безпечний уніфікований доступ до інформації про стани обладнання, події, виробничі завдання та ключові показники ефективності (KPI) [5]. Для обміну даними через REST або MQTT між промисловою демілітаризованою зоною (IDMZ) та ERP-системою слід використовувати TLS 1.3/mTLS, спеціальні облікові записи, короткострокові токени доступу та суворо визначений перелік дозволених API. Кожне повідомлення повинно містити ідентифікатор джерела, часову мітку, порядковий номер і одноразове випадкове значення (nonce). Сервер має відхиляти повідомлення з простроченою часовою міткою, повторно використаним nonce, порушеною послідовністю або некоректним цифровим підписом. Синхронізація часу повинна здійснюватися від контрольованого внутрішнього джерела NTP/PTP, оскільки некоректний системний час порушує коректне зіставлення телеметричних даних, керуючої програми верстата з ЧПК (CNC) та відповідного виробничого замовлення.

Захист контуру автоматичного зупинення. ERP не повинна генерувати безпосередню команду аварійного зупинення. Вона передає номер замовлення, операції, деталі, партії та дозволені режими, але рішення про втручання формується локальним edge-модулем і перевіряється промисловим контролером або безпечовим PLC. Незалежні апаратні блокування, аварійні кнопки та штатні функції безпеки ЧПУ мають вищий пріоритет і не можуть бути скасовані нейромережею. Автоматична дія дозволяється тільки в області повноважень, яка була попередньо валідована, та тільки для визначених верстатів, операцій, діапазонів параметрів та версій політики. Втрата зв'язку з ERP не повинна створювати довільний керуючий вплив; система переходить до заздалегідь визначеного безпечного режиму локальної роботи.

$$u_{stop} = 1 \Leftrightarrow Auth \wedge Integrity \wedge Freshness \wedge Policy \wedge Safety$$

У наведеній умові Auth означає успішну автентифікацію джерела, Integrity - правильний криптографічний підпис, Freshness - актуальність команди та відсутність повторного відтворення, Policy - відповідність контекстній політиці, Safety - дозвіл локального контуру функціональної безпеки. Якщо хоча б одна умова не виконується, керуюче повідомлення не надходить до обладнання, а подія реєструється та передається оператору/інженеру ІБ для подальшого аналізу.

Керування ідентичностями та конфігураціями. Доступ надається за принципами мінімальних привілеїв і принципу нульової довіри (Zero Trust): мережеве розташування саме по собі не створює довіри, а кожний користувач, сервіс і пристрій мають повторно автентифікуватися/авторизуватися [6]. Для операторів, технологів, адміністраторів ERP і ОТ застосовуються різні ролі; привілейований доступ обов'язково потребує MFA, обмеження списку адміністраторських станцій і обмеження в часі роботи. Забороняються спільні облікові записи. Сертифікати, ключі та секрети зберігаються у спеціалізованих засобах TPM/HSM або захищеному сховищі, а не у відкритих конфігураційних файлах. ПЗ edge-шлюзу, правила, порогові значення та нейромережеві моделі підписуються; при запуску механізмом безпечного завантаження (Secure Boot) виконується перевірка хешу і цифрового підпису довіреного видавця. Кожна зміна має номер версії, автора, підставу, результати тестування і придатний для автоматичного повернення попередній стан.

Перевірка даних і захист нейромережевого контуру. Перед передаванням до аналітичного блоку, дані проходять перевірку схеми вимірювання, одиниць вимірювання, фізично можливих меж, часової послідовності та узгодженості взаємопов'язаних сигналів. Різка зміна масштабу, «завислий» сенсор або датчик, невідповідність стану програми та навантаження або поява телеметрії від невідомого ідентифікатора розглядаються як ознаки атаки чи несправності. Підозрілий потік ізолюється і не використовується для автоматичного донавчання. Для протидії навмисному спотворенню навчальних даних (data poisoning) для кожної навчальної вибірки повинно бути відоме та підтверджене її походження. Вона повинна мати підписаний опис складу даних (маніфест), бути пов'язана з результатами контролю якості та містити перевірені мітки. Нова модель штучного інтелекту спочатку повинна працювати в режимі спостереження (shadow mode), тобто аналізувати реальні дані та формувати результати без впливу на роботу обладнання чи виробничий процес. Після цього модель випробовується на обмеженій пілотній ділянці. Введення моделі в повноцінну експлуатацію дозволяється лише після перевірки хибнонегативних і хибнопозитивних рішень, калібрування, аналізу впливу на ОЕЕ та можливості повернення до попередньої версії моделі (rollback) у разі виникнення проблем. Нейромодель не повинна мати можливості змінювати встановлені апаратні обмеження, порушати функції безпеки обладнання або обов'язкові технологічні правила, визначені технологом.

Конфіденційність і запобігання витоку. Для будь-якої компанії конструкторсько-технологічні дані (техпроцеси, креслення, специфікації), CNC-програми, геометрія деталей, параметри інструменту, дані про замовлення і результати контролю, тощо можуть становити державну, комерційну або службову таємницю. Тому при обміні з ERP-системою передаються мінімально необхідні атрибути: ідентифікатор операції, статус, агреговані характеристики, подія відхилення та підтверджений результат. Високочастотні сирі сигнали, файли CAD/CAM і повні CNC-програми не залишають ОТ-зону без окремого дозволу. Дані в сховищах шифруються, ключі відокремлюються від баз даних, права на експорт і масове читання блокуються засобами DLP. Резервні копії мають бути зашифрованими, незмінними та періодично перевірятися відновленням згідно вимог ISO 27001. Строк зберігання задається для всіх типів даних, а після завершення терміну зберігання застосовується контрольоване видалення.

Журналювання, виявлення атак і реагування. Критичні події - автентифікація, зміна сертифіката, моделі або порогів відхилення, автоматичне зупинення, відхилена команда, ручне підтвердження, оновлення ПЗ та експорт даних - фіксуються у централізованому журналі з обмеженим доступом. Для виявлення підміни доцільний ланцюжок хешів, у якому кожний запис залежить від попереднього. Пасивний ОТ IDS (система виявлення вторгнень у промисловому контурі) контролює нові вузли, незвичні протоколи, зміну напрямку трафіку, сканування, аномальну частоту запитів і спроби запису у read-only сегментах. Система централізованого збору, аналізу та контролю подій інформаційної безпеки (SIEM) отримує події з IDMZ та інтеграційних сервісів, але не створює активного навантаження на контролери. План реагування має передбачати локальну ізоляцію скомпрометованого шлюзу, перехід на штатне керування верстатом, відкликання сертифікатів, відновлення довіреної конфігурації, збереження доказів і перевірку цілісності перед повторним підключенням.

$$H_i = \text{SHA-256}(H_{i-1} \| m_i \| t_i \| id_i)$$

Тут H_i є контрольним значенням i -го запису, m_i - змістом події, t_i - часовою міткою, id_i - ідентифікатором джерела. Зміна або вилучення раніше записаної події порушує ланцюжок і може бути виявлена під час аудиту.

Безпечне тестування функцій автоматичного зупинення. До введення в експлуатацію функція перевіряється окремо від робочого виробництва у декілька етапів. Спочатку застосовуються записані телеметричні послідовності та цифровий двійник, далі — тестування із залученням реального контролера, після чого система працює у режимі спостереження без фактичного впливу на верстат. Перевіряються штатні відхилення, граничні стани, відмова окремого давача, розсинхронізація часу, обрив зв'язку, дублювання пакета, прострочений сертифікат, підміна адреси вузла, помилкова команда, атака на доступність, тощо. Окремо моделюються сценарії, у яких ERP надсилає некоректний контекст, з метою підтвердити, що помилка на корпоративному рівні не може безпосередньо спричинити небезпечний керуючий вплив. Автоматичне зупинення допускається лише після вимірювання максимальної затримки від появи небезпечної ознаки до спрацювання локального контуру, підтвердження пріоритету апаратних функцій блокування та перевірки відновлення після хибного спрацювання. Для кожного сценарію задаються очікуваний безпечний стан, допустимий час реакції, перелік журналів і критерій успішності. Зміна алгоритму, моделі, протоколу або контролера вимагає повторної валідації відповідного набору тестів.

Критерій приймання та експлуатаційний контроль. Перед промисловим розгортанням необхідно підтвердити, що жодна команда не приймається без валідного сертифіката, підпису, часової мітки та дозволеної ролі; повторене повідомлення гарантовано відхиляється; компрометація ERP не надає доступу до CNC-контролера; втрата зовнішнього зв'язку не викликає локальні функції забезпечення безпеки; а конфіденційні дані не можуть бути масово експортовані сервісним обліковим записом. Додатковими показниками є частка невідомих активів у ОТ, час відкликання сертифіката, максимальний час ізоляції шлюзу, успішність відновлення резервної копії, повнота журналів і кількість невинуватених автоматичних зупинок. Після запуску виконується постійний контроль базової мережевої поведінки, стану сертифікатів, цілісності ПЗ, актуальності переліку дозволених з'єднань і пристроїв, конфігурацій міжмережевих екранів та появи невідомих USB підключень. Оновлення систем спочатку перевіряються на тестовому комплекті; критичні вразливості компенсуються

сегментацією, блокуванням сервісу або віртуальним виправленням (Virtual Patching), якщо негайне оновлення суперечить вимогам доступності. Організаційний цикл керування ризиками доцільно узгодити з основними функціями NIST CSF 2.0 [7]: управління кіберризиками, ідентифікація активів і ризиків, захист, виявлення кіберінцидентів, реагування на них та відновлення після інцидентів [7].

Організаційні заходи та безпека ланцюга постачання. Технічні засоби не усувають ризик помилок персоналу й компрометації постачальника. Для інтеграторів, розробників аналітики та супроводу ERP системи необхідні договірні вимоги щодо повідомлення про вразливості, контроль походження компонентів, перелік залежностей ПЗ, підписані та валідні пакети оновлення і заборона постійних віддалених облікових записів. Віддалений доступ надається лише за попередньо погодженою заявкою, через контрольований захищений проміжний сервер (bastion host) та з обов'язковою багатфакторною автентифікацією (MFA), записом сесії та автоматичним завершенням після погодженого вікна. Персонал має окремо навчатися роботі з фішингом, змінними носіями, сертифікатами та реагуванню на нетипові рекомендації нейромоделі. Ролі власника технологічного процесу, відповідального за кібербезпеку, адміністратора ERP і розробника моделі розділяються; одна особа не повинна одночасно створювати, затверджувати та вводити в експлуатацію критичну зміну. Періодичні навчання мають включати сценарії компрометації edge-шлюзу, витоку CNC-програми, масового відкликання сертифікатів і відновлення роботи в локальному режимі.

Висновки. Кіберзахист ІІoT-системи моніторингу CNC-операцій повинен будуватися як багаторівневий захист ОТ, а не як розширення звичайної корпоративної мережі. Ключовими рішеннями є сегментація на зони та канали, IDMZ, відсутність прямого керуючого доступу ERP до верстата, криптографічно захищений OPC UA, мінімальні привілеї, локальна перевірка команд і незмінне журналювання. Автоматичне зупинення допустиме лише в межах валідованих сценаріїв та під контролем незалежних функцій безпеки. Зменшення витоку досягається мінімізацією даних, локальною обробкою сирого телеметрії, шифруванням, DLP і контрольованим життєвим циклом ключів, моделей та конфігурацій. Запропоновані заходи дають змогу інтегрувати CNC-рівень з ERP-системою без створення прямого каналу несанкціонованого впливу на технологічний процес.

Література

1. Stouffer K., Pease M., Tang C. Y. et al. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg : NIST, 2023. DOI: 10.6028/NIST.SP.800-82r3.
2. ANSI/ISA-62443-3-2-2020. Security for Industrial Automation and Control Systems. Part 3-2: Security Risk Assessment for System Design. Research Triangle Park : ISA, 2020.
3. ANSI/ISA-62443-3-3-2013. Security for Industrial Automation and Control Systems. Part 3-3: System Security Requirements and Security Levels. Research Triangle Park : ISA, 2013.
4. OPC Foundation. OPC Unified Architecture. Part 2: Security Model. Version 1.05.06. URL: <https://reference.opcfoundation.org/specs/OPC-10000-2/> (дата звернення: 21.08.2026).
5. OPC Foundation, VDW. OPC UA for Machine Tools. Part 1: Machine Monitoring and Job Management. Version 1.02.0. URL: <https://reference.opcfoundation.org/specs/OPC-40501-1/> (дата звернення: 21.08.2026).
6. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : NIST, 2020. DOI: 10.6028/NIST.SP.800-207.
7. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg : NIST, 2024. DOI: 10.6028/NIST.CSWP.29.
8. IT-Enterprise. Виробництво: ERP, MES, ІІoT та цифрове управління виробничими процесами. URL: <https://www.it.ua/products/manufacturing> (дата звернення: 21.08.2026).

УДК 004.056.53:004.942

¹Гришук О. М.

²Гришук Р. В.

ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ВУЗЛА ВІД КІБЕРАТАК НА ОСНОВІ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ

¹Національний університет оборони України

Hry.Olga@gmail.com

²Військова академія (м. Одеса)

Prof.Hry@gmail.com

Анотація. Розкрито ідею дослідження захищеності блокчейн-вузлів від кібератак на основі диференціально-ігрових моделей. Блокчейн-вузол під впливом кібератаки запропоновано описувати графом станів. У формалізованому вигляді граф станів являє собою систему диференціальних рівнянь Колмогорова-Чепмена в диференціально-ігровій постановці. Розв'язок системи диференціальних рівнянь запропоновано знаходити операційним методом диференціальних перетворень. На відміну від відомих операційних методів, зокрема перетворень Лапласа, Фур'є тощо, запропонований метод дозволяє знаходити розв'язки системи

рівнянь в реальному масштабі часу при збереженні точності вихідної моделі. Результатом розв’язку системи диференціальних рівнянь є ймовірності станів блокчейн-вузла під впливом кібератаки, оптимальна стратегія його кіберзахисту, поточний та гарантований рівні захищеності. Аналіз отриманих результатів дозволяє обґрунтовано підійти до кіберзахисту блокчейн-технологій на рівні вузлів від різних типів кібератак.

Ключові слова: блокчейн-вузол, диференціальна гра, рівень захищеності, стратегія, кібератака, модель.

Блокчейн технологія захищеного розподіленого реєстру знайшла широке застосування в багатьох критичних застосунках – від банківського сегменту [1] до оборонного сектору [2]. Разом з тим не зважаючи на заявлений високий рівень її захищеності, вона й надалі залишається об’єктом кібератак [3].

Останнім часом під кібератаки все частіше підпадають окремі блокчейн-вузли [4]. Серед кібератак на окремі блокчейн-вузли особливу небезпеку становлять атаки затемнення [5] та атаки з використанням троянського шкідливого програмного забезпечення [6]. Їх особливості проявляються у ході поширення на рівні вузла. Відповідно, блокчейн-вузол на однакових часових інтервалах має різні показники захищеності. Саме тому на сьогодні не існує універсальних стратегій кіберзахисту блокчейн-вузлів. Водночас кібератаки одного класу мають схожу динаміку поширення, що дозволяє їх своєчасно ідентифікувати та вживати необхідних заходів кіберзахисту.

Дослідження таких властивостей блокчейн-вузлів під впливом кібератак доцільно здійснювати засобами математичного моделювання. Як такий засіб дослідження безпекових властивостей блокчейн-вузлів пропонується метод диференціальних перетворень [7]. При цьому формалізовану постановку завдання дослідження захищеності блокчейн-вузла запропоновано сформулювати в диференціально-ігровій постановці [8]. На відміну від відомих досліджень [9], [10] та ін. запропонований підхід має на меті знаходження ймовірностей перебування блокчейн-вузла під впливом кібератаки у будь-якому з досліджуваних станів, оптимальну стратегію його кіберзахисту, поточний та гарантований рівні захищеності.

Технологія дослідження блокчейн-вузла від кібератак на основі диференціально ігрових моделей включає такі етапи.

Перший етап. Будується граф кібератаки на блокчейн-вузол з використанням моделі напівмарківського процесу. Такий підхід забезпечує опис станів блокчейн-вузла з урахуванням його ймовірісно-часових характеристик. При переході блокчейн-вузла з одного стану в інший під впливом обраних гравцями стратегій функції розподілу часу знаходження блокчейн-вузла у різних станах можуть мати різні розподіли. Ця властивість напівмарківських процесів забезпечує адекватність моделі реальним процесам, які протікають в блокчейн-вузлі під час кібератаки на нього.

Другий етап. На основі графової моделі станів блокчейн-вузла під впливом кібератаки складається система диференціальних рівнянь Колмогорова-Чепмена з обов’язковим дотриманням умов нормування за визначених початкових станів.

Третій етап. На третьому етапі у формалізованому вигляді задається плата гри – рівень захищеності блокчейн-вузла під впливом кібератаки. У більшості випадків вона визначається максимінним критерієм оптимальності, що ґрунтується на зваженій ймовірності перебування блокчейн-вузла під кібератакою протягом усього часу її перебігу.

Четвертий етап. З огляду на великі об’єми інформації, що підлягають обробленню в реальному масштабі часу, на четвертому етапі використовується метод диференціальних перетворень, або його модифікації залежно від вимог до точності збереження вихідної моделі.

П’ятий етап. На заключному п’ятому етапі шляхом математичного моделювання знаходяться ймовірності перебування блокчейн-вузла під впливом кібератаки у будь-якому з досліджуваних станів, оптимальна стратегія його кіберзахисту, поточний та гарантований рівні захищеності.

Знайдені оцінки є підґрунтям для обрання дієвих стратегій кіберзахисту блокчейн-вузла від різних типів кібератак.

У доповіді з метою практичної апробації запропонованого підходу проведено дослідження захищеності блокчейн-вузла від кібератак, зокрема Екліпс-атаки та атак із використанням троянського шкідливого програмного забезпечення, на основі їх диференціально-ігрових моделей.

Аналіз одержаних результатів показав [11]:

за однакових вихідних умов Екліпс-атака становить більшу загрозу для захищеності блокчейн-вузла, ніж атака з використанням троянського шкідливого програмного забезпечення. За оптимальної поведінки обох гравців рівень гарантій захищеності при Екліпс-атаці становить не більше 0,677, тоді як для атак із використанням троянського шкідливого програмного забезпечення цей показник досягає 0,806. Таким чином, різниця між отриманими значеннями становить близько 16 %;

зміна стратегій гравців безпосередньо впливає на рівень захищеності блокчейн-вузла, причому найбільший вплив має стратегія гравця кібернападу. Для Екліпс-атаки збільшення інтенсивності кібератаки більш ніж на 25 % відносно оптимальної стратегії призводить до переходу блокчейн-вузла в незахищений стан, що створює передумови для його подальшого адміністрування атакуючим гравцем. Водночас за умови збереження гравцем кібернападу оптимальної стратегії відхилення стратегії кіберзахисту від оптимального значення хоча й зменшує рівень захищеності, проте він залишається в межах допустимого рівня ризику;

для атаки з використанням троянського шкідливого програмного забезпечення залежність рівня захищеності від стратегій гравців має менш критичний характер. За оптимальних стратегій рівень гарантій становить 0,806, що свідчить про вищу стійкість блокчейн-вузла порівняно з результатами, отриманими для Екліпс-атаки. Навіть за відхилення гравців від оптимальних стратегій блокчейн-вузол не переходить у незахищений стан. Разом із тим таке відхилення супроводжується зростанням ймовірності отримання інфікованих файлів та їх запуску власником блокчейн-вузла, що, відповідно, підвищує ризик компрометації та знижує загальний рівень його захищеності.

Висновки. Запропонований диференціально-ігровий підхід дає змогу оцінювати захищеність блокчейн-вузла від кібератак, визначати ймовірності його станів та рівень захищеності залежно від стратегій гравців.

За результатами дослідження встановлено, що Екліпс-атака становить більшу загрозу для блокчейн-вузла, ніж атака з використанням троянського шкідливого програмного забезпечення. Отримані результати підтверджують можливість застосування запропонованих моделей для оцінювання та прогнозування захищеності блокчейн-вузла.

Перспективним напрямом є розширення запропонованих моделей для дослідження інших типів кібератак.

Література

1. Thakur V., Raju G. The role of blockchain technology in strengthening security, transparency, and trust in banking transactions: A conceptual and empirical review of distributed ledger applications in modern financial systems // *Bank and Policy*. 2026. Vol. 6, No. 1. P. 107–119. Art. 9. <https://doi.org/10.56334/bpj/6.1.9>.
2. Гришук О., Гришук Р. Цифрова валюта центрального банку та криптовалюта як альтернативні джерела фінансування оборони України в умовах економічної турбулентності // *Кібербезпека: освіта, наука, техніка*. 2026. Vol. 1, No. 33. P. 613–624. Art. 1235. <https://doi.org/10.28925/2663-4023.2026.33.1235>.
3. TRM Labs. 2026 Crypto Crime Report // *TRM Labs*. 2026.
4. Das J., Al Tasin S. A., Rabbi M. F., Ferdous M. S. A Survey of Attacks on Blockchain Systems Using a Layer-based Approach // *Computer Networks*. 2025. Vol. 265. Art. 111274.
5. Rehman Z., Gregory M. A., Gondal I., Dong H., Ge M. Eclipse Attacks in Blockchain Networks: Detection, Prevention, and Future Directions // *IEEE Access*. 2025. Vol. 13. P. 25918–25933. doi: 10.1109/ACCESS.2025.3538837.
6. Hryshchuk O., Hryshchuk R. Evaluation of Blockchain Node Security Against Eclipse Attacks and Trojan Malware Using Differential Game Models // *Cybersecurity: Education, Science, Technique*. 2026. No. 4 (32). P. 633–653. Art. 1150. <https://doi.org/10.28925/2663-4023.2026.32.1150>.
7. Pukhov G. E. Computational structure for solving differential equations by Taylor transformations // *Kybern Syst Anal*. 1978. Vol. 14. P. 383–390. doi: 10.1007/BF01074670.
8. Гришук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень. Житомир: Рута. 2010. 280 с.
9. Zhiyong L., Shuyi W., Weiwei S., Jiahui L., Jianming W. Research on security situation awareness algorithm of Markov differential game blockchain model // *The Journal of China Universities of Posts and Telecommunications*. 2023. Vol. 30, No. 4. P. 105–120.
10. Zhou C., Xing L., Liu Q., Wang H. Semi-Markov Based Dependability Modeling of Bitcoin Nodes Under Eclipse Attacks and State-Dependent Mitigation // *International Journal of Mathematical, Engineering and Management Sciences*. 2021. Vol. 6, No. 2. P. 480–492. doi: 10.33889/IJMEMS.2021.6.2.029.
11. Гришук О. М., Гришук Р. В. Оцінювання захищеності блокчейн-вузла від Екліпс-атаки та троянського шкідливого програмного забезпечення на основі диференціально-ігрових моделей // *Кібербезпека: освіта, наука, техніка*. 2026. No. 4 (32). P. 633–653. Art. 1150. <https://doi.org/10.28925/2663-4023.2026.32.1150>.

УДК 621.391

Мадінов М.Л., Галаган Н.В., Власенко В.О.

БАГАТОПАРАМЕТРИЧНИЙ МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ У ВОЛОКОННО-ОПТИЧНИХ ЛІНІЯХ ЗВ’ЯЗКУ НА ОСНОВІ МОНІТОРИНГУ ФІЗИЧНОГО СТАНУ ОПТИЧНОГО ТРАКТУ

Державний університет інформаційно-комунікаційних технологій
nmadinov@gmail.com

Анотація. У роботі досліджено проблему захисту інформації у волоконно-оптичних лініях зв’язку в умовах можливого фізичного втручання в оптичний тракт та несанкціонованого відбору частини оптичного сигналу. Проаналізовано основні механізми виникнення каналів витоку інформації, пов’язані з локальними згинами оптичного волокна, введенням оптичних відгалужувачів, втручанням у місця з’єднань та зміною параметрів поширення оптичного випромінювання. Обґрунтовано необхідність переходу від традиційного контролю окремих характеристик лінії до комплексного моніторингу її фізичного стану. Запропоновано

багатопараметричний підхід до виявлення потенційного несанкціонованого втручання, який передбачає спільний аналіз потужності прийнятого оптичного сигналу, загасання, характеристик зворотного розсіювання, коефіцієнта бітових помилок, оптичного відношення сигнал/шум та часових параметрів передавання. Сформовано вектор функціонального стану оптичного тракту та запропоновано інтегральний показник аномальності для оцінювання відхилення поточного стану лінії від еталонного. Для узагальненої оцінки захищеності введено коефіцієнт фізичної стабільності оптичного тракту, що враховує нормовані відхилення контрольованих параметрів та їх вагові коефіцієнти. Запропоновано використання еталонного рефлектометричного профілю для виявлення та просторової локалізації аномальних змін у волоконно-оптичній лінії. Наукова новизна одержаних результатів полягає в розвитку методу захисту інформації на основі багатопараметричного розпізнавання функціонального стану фізичного оптичного каналу, що створює можливість розмежування нормального функціонування, природної деградації, фізичного пошкодження та потенційного несанкціонованого втручання. Запропонований підхід може бути використаний під час побудови автоматизованих систем моніторингу та захисту магістральних, корпоративних і спеціалізованих волоконно-оптичних мереж зв'язку.

Ключові слова: волоконно-оптична лінія зв'язку, захист інформації, інформаційна безпека, несанкціонований доступ, оптичний канал витоку інформації, багатопараметричний моніторинг, оптична рефлектометрія, функціональний стан, виявлення аномалій, фізична стабільність оптичного тракту.

Сучасні волоконно-оптичні лінії зв'язку (ВОЛЗ) є базовим фізичним середовищем транспортних, магістральних, корпоративних і спеціалізованих телекомунікаційних мереж. Їх широке застосування визначається значною пропускну здатністю, малим загасанням оптичного сигналу, можливістю передавання інформації на великі відстані, електромагнітною сумісністю та відсутністю електричної провідності між передавальною і приймальною сторонами. Водночас поширене уявлення про практично абсолютну захищеність оптичного волокна від несанкціонованого перехоплення інформації не повною мірою відповідає сучасним умовам функціонування телекомунікаційної інфраструктури.

На відміну від металевих ліній передавання, волоконно-оптичний тракт практично не створює традиційного побічного електромагнітного випромінювання. Проте це не виключає можливості формування оптичного каналу витоку інформації. Несанкціонований доступ може здійснюватися через фізичне підключення до волокна, використання оптичних відгалужувачів, порушення умов повного внутрішнього відбиття, контроль випромінювання в місцях з'єднань та пошкоджень, а також через навмисне створення локальних згинів волокна. Тому захист ВОЛЗ доцільно розглядати не лише як задачу криптографічного захисту переданих даних, а як комплексну задачу контролю фізичного стану оптичного середовища.

Аналіз способів несанкціонованого доступу до інформаційних потоків у ВОЛЗ та відповідних методів протидії показує необхідність поєднання фізичних, апаратних і програмних механізмів захисту [1]. Особливого значення набуває оперативне виявлення змін параметрів оптичного тракту, які можуть бути пов'язані не лише з природною деградацією лінії, а й зі спробою прихованого підключення.

Основна частина

Фізично передавання інформації у ВОЛЗ ґрунтується на поширенні модульованого оптичного випромінювання по серцевині волокна за умов, близьких до повного внутрішнього відбиття. Для ідеалізованої лінії потужність оптичного сигналу на відстані (L) може бути представлена залежністю

$$P(L) = P_0 \cdot 10^{-\alpha L/10},$$

де P_0 – потужність оптичного сигналу на вході лінії;

$P(L)$ – потужність сигналу на відстані (L);

α – коефіцієнт загасання, дБ/км;

L – довжина оптичного тракту, км.

З погляду інформаційної безпеки принципово важливим є те, що будь-яке несанкціоноване втручання, яке супроводжується відбором частини оптичної потужності, зміною геометрії волокна або внесенням додаткового оптичного компонента, потенційно змінює параметри цього балансу.

Одним із можливих способів перехоплення є створення локального макрозгину. Зі зменшенням радіуса кривизни частина мод перестав утримуватися серцевиною, унаслідок чого певна частка оптичної потужності виходить за межі волокна. Таке випромінювання потенційно може бути зареєстроване фотоприймальним пристроєм без повного розриву лінії. Інший спосіб передбачає безпосереднє введення в тракт оптичного розгалужувача, що забезпечує контрольований відбір частини потужності.

Тому традиційна модель захисту, побудована за принципом «зашифрувати інформацію – передати – розшифрувати», є необхідною, але недостатньою. Перспективнішою є концепція контрольованого фізичного оптичного каналу, за якої сама лінія зв'язку розглядається як об'єкт безперервного діагностування.

Для цього пропонується характеризувати стан захищеної ВОЛЗ вектором

$$X(t) = [P_r(t), \alpha(t), R(t), BER(t), OSNR(t), \tau(t)],$$

де $P_r(t)$ – потужність прийнятого оптичного сигналу;

$\alpha(t)$ – оцінене загасання;

$R(t)$ – характеристика зворотного розсіювання;

$BER(t)$ – коефіцієнт бітових помилок;

$OSNR(t)$ – відношення оптичного сигналу до шуму;

$\tau(t)$ – часові характеристики проходження сигналу.

У нормальному стані параметри повинні перебувати в межах деякої допустимої області

$$X(t) \in \Omega_n,$$

де Ω_n – область параметрів нормального функціонування оптичного тракту.

Відхилення одного показника ще не повинно автоматично інтерпретуватися як несанкціонований доступ. Наприклад, зниження прийнятої потужності може бути наслідком температурних змін, старіння компонентів, механічних навантажень або погіршення стану конекторного з'єднання. Саме тому доцільно аналізувати сукупність взаємопов'язаних параметрів, а не застосовувати єдиний поріг за потужністю.

Інтегральний індикатор аномального стану можна представити у вигляді

$$A(t) = w_1 \Delta P(t) + w_2 \Delta \alpha(t) + w_3 \Delta R(t) + w_4 \Delta BER(t) + w_5 \Delta OSNR(t),$$

де $\Delta P(t)$, $\Delta \alpha(t)$, $\Delta R(t)$, $\Delta BER(t)$, $\Delta OSNR(t)$ – нормовані відхилення відповідних параметрів від їх базових значень; $W_1, \dots, W_5$ – вагові коефіцієнти.

Умова

$$A(t) > A_{кр}$$

може розглядатися як ознака переходу лінії до аномального стану, що потребує додаткової перевірки.

Апаратно-програмний підхід до захисту ВОЛЗ є перспективним саме тому, що дозволяє поєднати контроль фізичних параметрів тракту з алгоритмічним прийняттям рішення щодо наявності ознак несанкціонованого втручання [1].

Важливим засобом фізичного контролю є оптична рефлектометрія. Введення тестового імпульсу та аналіз сигналу зворотного релеївського розсіювання дозволяють сформувати своєрідний «профіль» оптичної лінії. Поява нового локального загасання, зміна відбиття або зміщення характеристик окремої ділянки може свідчити про пошкодження, зміну конфігурації чи стороннє втручання.

Для захищеної лінії доцільно зберігати еталонну рефлектограму

$$R_0(z),$$

де z – координата вздовж оптичного тракту, та порівнювати її з поточною характеристикою

$$R(z, t).$$

Тоді функцію відхилення можна визначити як

$$\Delta R(z, t) = R(z, t) - R_0(z) \vee.$$

Якщо

$$\Delta R(z, t) > R_{кр}$$

для певної координати z , система може не лише зафіксувати аномалію, але й локалізувати потенційне місце втручання.

У сучасній захищеній ВОЛЗ цей принцип доцільно реалізовувати не як періодичну ручну діагностику, а як неперервний автоматизований моніторинг фізичного рівня. Такий підхід переводить оптичну лінію з пасивного середовища передавання в активний об'єкт інформаційної безпеки.

Іншим напрямом є застосування пасивних оптичних пристроїв, які дозволяють контролювати параметри передавання та формувати додаткові рубежі фізичного захисту. Українськими дослідниками О. О. Маньком, О. С. Шматком та А. Б. Петренком розглянуто можливості використання пасивних оптичних пристроїв для підвищення захищеності волоконно-оптичних ліній і мереж [2]. Такий підхід є важливим з огляду на те, що захист реалізується без істотного ускладнення активного обладнання тракту.

Разом із тим розвиток високошвидкісних мереж вимагає переходу від окремих засобів протидії до багаторівневої архітектури захисту, яка може бути представлена як

$$S_{зах} = \{S_{фіз}, S_{мон}, S_{крипт}, S_{мер}, S_{анал}\},$$

де $S_{фіз}$ – засоби фізичного захисту кабельної інфраструктури;

$S_{мон}$ – система моніторингу параметрів оптичного тракту;

$S_{крипт}$ – криптографічні механізми;

$S_{мер}$ – мережеві механізми автентифікації та контролю доступу;

$S_{анал}$ – інтелектуальна підсистема виявлення аномалій.

Практична реалізація захисту повинна враховувати енергетичний бюджет конкретної ВОЛЗ. Сумарні втрати можна визначити як

$$\Delta \Sigma = \alpha L + N_{сАс} + N_{рАр} + A_{дод},$$

де αL – втрати у волокні; $N_{сАс}$ – сумарні втрати у з'єднаннях; $N_{рАр}$ – втрати в рознімних з'єднаннях; $A_{дод}$ – додаткові втрати, зумовлені іншими компонентами тракту.

Розрахунок захищеної ВОЛЗ повинен передбачати не лише виконання умови працездатності приймача, а й формування достатнього запасу потужності для розпізнавання аномальних змін.

На цій основі доцільно ввести коефіцієнт фізичної стабільності захищеного оптичного тракту

$$KFS = 1 - \Sigma(w_i \cdot \delta_i),$$

де δ_i – нормоване відхилення (i)-го контрольованого параметра від його еталонного значення; W_i – ваговий коефіцієнт, причому

$$\Sigma w_i = 1.$$

Для нормального стану (KFS) наближається до 1. Поступове його зниження свідчатиме про деградацію параметрів лінії, тоді як різка локальна зміна може розглядатися як ознака потенційного фізичного втручання.

Наукова новизна полягає у розвитку підходу до захисту інформації у ВОЛЗ на основі спільного аналізу фізичних та інформаційних параметрів оптичного каналу в режимі реального часу. На відміну від традиційного контролю, орієнтованого переважно на перевищення порогового значення загасання або виявлення фізичного пошкодження, пропонується використовувати багатопараметричну модель стану оптичного тракту.

Принцип прийняття рішення можна представити як

$$X(t) \rightarrow F[X(t), X_0] \rightarrow A(t) \rightarrow C(t),$$

де $X(t)$ – поточний вектор параметрів; X_0 – еталонний профіль лінії; F – функція аналізу відхилень; $A(t)$ – інтегральний показник аномальності; $C(t)$ – результат класифікації стану.

Доцільно передбачити щонайменше чотири класи:

$C(t) \in \{\text{нормальний стан; природна деградація; пошкодження; потенційне втручання}\}.$

Саме розмежування природної деградації та потенційного несанкціонованого доступу є принципово важливим. Звичайна порогова система може сформувати тривогу як через незаконне підключення, так і через погіршення стану з'єднання. Багатопараметричний аналіз дозволяє враховувати характер, швидкість, просторову локалізацію та взаємозв'язок змін.

Перспективним розвитком запропонованої моделі є застосування алгоритмів машинного навчання для визначення аномальних комбінацій параметрів. У цьому випадку система навчається на масиві даних нормальної експлуатації та визначає ступінь відхилення нового стану від сформованого профілю. Це особливо актуально для магістральних мереж великої протяжності, де статичні порогові значення не завжди забезпечують необхідну достовірність контролю.

Таким чином, перспективна система захисту ВОЛЗ повинна функціонувати за замкненим циклом:

вимірювання $\rightarrow$ формування профілю $\rightarrow$ виявлення відхилення $\rightarrow$ класифікація $\rightarrow$ локалізація $\rightarrow$ реагування.

У разі виявлення критичної аномалії система може автоматично сформувати повідомлення оператору, активувати поглиблену рефлектометричну діагностику, переключити інформаційний потік на резервний маршрут або тимчасово обмежити передавання критично важливих даних через потенційно скомпрометований сегмент.

Висновки. Захист інформації у волоконно-оптичних лініях зв'язку є комплексною науково-технічною задачею, яка не може бути зведена виключно до застосування криптографічних алгоритмів. Незважаючи на високий рівень фізичної захищеності оптичного середовища порівняно з металевими лініями, існує принципова можливість несанкціонованого відбору частини оптичної потужності через локальні згини, введення відгалужувачів, втручання в місця з'єднань та інші зміни структури тракту.

Встановлено, що перспективним напрямом розвитку систем захисту є перехід від пасивної моделі протидії до безперервного контролю функціонального стану фізичного оптичного каналу. Для цього запропоновано використовувати комплекс параметрів, що включає прийняту оптичну потужність, загасання, характеристику зворотного розсіювання, BER, OSNR та часові параметри сигналу.

Запропоновано формувати еталонний профіль ВОЛЗ і визначати відхилення поточного стану від нього за допомогою інтегрального показника аномальності. Додатково введено коефіцієнт фізичної стабільності оптичного тракту (KFS), який дозволяє узагальнено характеризувати ступінь відхилення контрольованих параметрів від нормального стану.

Наукова новизна підходу полягає у представленні захисту ВОЛЗ як задачі багатопараметричного розпізнавання функціонального стану оптичного тракту, що дозволяє розмежовувати нормальне функціонування, природну деградацію, фізичне пошкодження та потенційне несанкціоноване втручання. Подальший розвиток такого підходу доцільно пов'язати із застосуванням методів машинного навчання для адаптивного визначення аномалій та автоматичної локалізації потенційно скомпрометованих ділянок оптичної мережі.

Література

1. Васильківський М. В., Паламарчук Р. П. Методи захисту волоконно-оптичних ліній зв'язку // *Матеріали XLVII науково-технічної конференції підрозділів Вінницького національного технічного університету, Вінниця*, 14–23 березня 2018 р. Вінниця : ВНТУ, 2018.
2. Манько О. О., Шматок О. С., Петренко А. Б. Використання пасивних оптичних пристроїв для захисту інформації у волоконно-оптичних лініях зв'язку та мережах // *Захист інформації*. 2017. Т. 19, № 2. С. 143–147.

3. Микола М.Л.; Галаган (Руденко)Н.В. Standards as a basis for information and communication technologies // INNOVATIVE TECHNOLOGIES AND SCIENTIFIC SOLUTIONS FOR INDUSTRIES 2024-12-12 | Journal article DOI: 10.30837/2522-9818.2024.4.153 Journal article

УДК 004.056.5:004.7

¹Черемнов М.В., ²Фразе-Фразенко О.О.

СИНЕРГЕТИЧНИЙ МЕТОД БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

¹Міжнародний університет
cheremnovmaksym@gmail.com

²Одеський національний університет ім. І.І.Мечникова
frazenko@gmail.com

Анотація. У роботі проведено комплексний аналіз концептуальної кризи традиційних засобів периметрового захисту та обґрунтовано необхідність переходу до парадигми нульової довіри в корпоративних мережах об'єктів критичної інфраструктури. Виявлено, що головним обмеженням існуючих систем управління доступом є дискретність перевірок, яка дозволяє зловмисникам приховано діяти всередині легітимних каналів зв'язку після викрадення криптографічних ідентифікаторів. Для подолання цієї вразливості залучено математичний апарат нелінійної динаміки, зокрема показник Херста та ентропію Цаліса, що забезпечують виявлення аномалій у структурі та хаотичності зашифрованого трафіку без його дешифрування. На основі отриманих результатів синтезовано інтегральну математичну модель динамічного рівня довіри, яка реалізує синергетичний зв'язок між суворою бінарною логікою електронного підпису та безперервним поведінковим профілюванням мережевих вузлів.

Ключові слова: нульова довіра, критична інфраструктура, синергетична автентифікація, кібербезпека, криптографія, моделювання.

Трансформація ландшафту кіберзагроз та розмиття периметра корпоративних мереж об'єктів критичної інфраструктури зумовлюють перехід від традиційної моделі «замкненого контуру» до парадигми нульової довіри (Zero Trust) [1]. В основі існуючих систем захисту лежить дискретна логіка авторизації, що математично описується функцією [5]:

$$D(s, o, e) = \begin{cases} 1, \text{ якщо } P(A_s, A_o, A_e) = True \\ 0, \text{ інакше} \end{cases}$$

Проте такий підхід оперує параметрами середовища A_e лише в момент ініціалізації сесії t_0 . Головним обмеженням дискретності є припинення контролю після успішної перевірки, що створює «вікно вразливості» для горизонтального переміщення порушника всередині встановленого каналу [1]. Фундаментом ідентифікації при цьому виступає інфраструктура відкритих ключів (PKI), де надійність ланцюжка довіри визначається ймовірністю:

$$P_{trust}(t) = \prod_{i=1}^L (1 - p_{c,i}(t)) \cdot (1 - P_{revoc}(t))$$

Дана модель демонструє залежність від ризиків компрометації ключів центрів сертифікації ($p_{c,i}$) та затримок у списках відкликання (P_{revoc}), що в умовах АРТ-атак (Advanced Persistent Threat – розвинена стала загроза) робить статичну довіру до сертифіката недостатньою [4].

Процес ініціалізації сесії через криптографічне рукостискання характеризується часовим показником

$$T_{hs} = 2 \cdot \tau_{rtt} + t_{gen_{cli}} + t_{ver_{srv}} + t_{gen_{srv}} + t_{ver_{cli}}$$

Значні обчислювальні витрати сервера на верифікацію (t_{versrv}) та генерацію (t_{gensrv}) підписів у порівнянні з мінімальними витратами атакуючої сторони створюють умови для атак на виснаження ресурсів (DoS) [6]. Більше того, після завершення фази T_{hs} система фактично «спіпне», оскільки традиційні методи не аналізують динаміку зашифрованого трафіку [1]. Це зумовлює методологічну суперечність: криптографічні методи забезпечують строгість лише на старті, тоді як поведінкові методи потребують часу для накопичення даних, але стають ефективними саме під час сесії.

Для подолання цього розриву необхідний перехід до аналізу метаданих та нелінійної динаміки трафіку. Враховуючи самоподібну природу мережевих потоків, ключовим індикатором безпеки є показник Херста (H), розрахований за методом найменших квадратів [3]:

$$H = \frac{\ln \left(E \left[\frac{R(m)}{S(m)} \right] \right) - \ln C}{\ln m}$$

Зниження цього параметра нижче межі 0.5 свідчить про стан антиперсистентності, що математично підтверджує руйнування фрактальної структури легітимного трафіку через впровадження аномальних пакетів [3]. Для детектування прихованих етапів вторгнень використовується ентропія Цаліса:

$$S_q = \frac{1}{q-1} \cdot \left(1 - \sum_{i=1}^K p_i^q \right)$$

яка, будучи узагальненням ентропії Шеннона, завдяки індексу неекстенсивності q забезпечує вищу чутливість до рідкісних подій та малих флуктуацій [2].

Синергетичний метод полягає у формуванні інтегрального рівня довіри:

$$T_{\int}(t) = \alpha \cdot K_{pki}(t_0) \cdot e^{-\mu \cdot (t-t_0)} + \beta \cdot (1 - \tanh(\omega_1 \cdot |H_{ref} - H(t)| + \omega_2 \cdot |S_{ref} - S(t)|))$$

Результат РКІ-перевірки (K_{pki}) поступово деградує під впливом коефіцієнта «старіння» μ , що вимагає безперервного підтвердження легітимності через поведінкові метрики (H , S). Використання функції гіперболічного тангенсу ($\tanh$) забезпечує швидке падіння рівня довіри при найменших відхиленнях від еталонних профілів (H_{ref} , S_{ref}). Для математичної коректності моделі застосовуються умови нормування:

$$\begin{cases} \alpha + \beta = 1 \\ \omega_1 + \omega_2 = 1 \end{cases}$$

Архітектурно цей метод реалізується через дворівневу структуру (рис. 1), де верхній контур (РКІ) здійснює вхідний контроль, а нижній аналітичний контур забезпечує безперервну корекцію довіри, дозволяючи миттєво блокувати сесію при деградації інтегрального показника.



Рисунок 1 – Структурна схема комплексного методу захисту

Висновки. На основі проведеного дослідження встановлено, що традиційна дискретна автентифікація є критично вразливою до компрометації ідентифікаторів та АРТ-загроз через статичність оцінки безпеки. Показано, що лише синергія суворих криптографічних методів інфраструктури відкритих ключів та методів нелінійної динаміки (фрактального та ентропійного аналізу) дозволяє реалізувати концепцію безперервного контролю сесії. Використання інтегрального показника довіри з урахуванням коефіцієнта часового знецінення та аналізу антиперсистентності трафіку забезпечує проактивне виявлення аномалій у зашифрованих каналах зв'язку без необхідності дешифрування їхнього вмісту.

Література

1. NIST Special Publication 800-207. (2020). Zero Trust Architecture. National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-207.

2. Tsallis, C. (1988). Possible generalization of Boltzmann-Gibbs statistics. Journal of Statistical Physics, 52(1-2), 479-487.

3. Leland, W. E., Taqqu, M. S., Willinger, W., & Wilson, D. V. (1994). On the self-similar nature of Ethernet traffic (extended version). IEEE/ACM Transactions on Networking, 2(1), 1-15.

4. Adams, C., & Lloyd, S. (2003). Understanding PKI: Concepts, Standards, and Deployment Considerations. Addison-Wesley Professional.

5. Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2018). Attribute-Based Access Control. Artech House.

6. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.

ПІДВИЩЕННЯ ОСВІЧЕНОСТІ З ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В ПРОЦЕСІ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УНІВЕРСИТЕТУ

Національний технічний університет «Дніпровська політехніка»

tymofieiev.d.s@nmu.one, udovyk.i.m@nmu.one, kruchinin.o.v@nmu.one

Анотація. Обґрунтовано необхідність підвищення рівня освіченості з інформаційної та кібербезпеки серед співробітників і здобувачів вищої освіти в умовах впровадження системи управління інформаційною безпекою (СУІБ) за стандартом ДСТУ ISO/IEC 27001. Проаналізовано специфічні кіберризики та виклики людського фактора, характерні для сучасного освітнього середовища закладів вищої освіти. Запропоновано впровадження комплексної навчальної програми та розглянуто ефективність залучення сучасних інтерактивних інструментів навчання, таких як кіберполігони та платформ підвищення практичних навичок.

Ключові слова: СУІБ, ISO/IEC 27001, освіченість з кібербезпеки, кібергігієна, людський фактор, заклади вищої освіти, кіберполігон, архітектура нульової довіри.

Розвиток цифрового суспільства, впровадження новітніх хмарних рішень та тотальна цифровізація освітніх процесів суттєво змінили безпековий ландшафт сучасних закладів вищої освіти (ЗВО). Сучасний університет є складною екосистемою, яка оперує значними обсягами персональних даних, фінансовою інформацією, поточними наробками та результатами наукових досліджень, а також об'єктами інтелектуальної власності. Водночас науково-освітній сектор є однією з найбільш привабливих цілей для кібератак, оскільки характеризується значною відкритістю мережевої інфраструктури, гетерогенністю пристроїв та великою кількістю користувачів з різним рівнем цифрової грамотності. Характерною ознакою також є хронічне недофінансування інфраструктури та низький рівень оплати праці.

За даними аналітичних звітів з кібербезпеки та статистики Державної служби спеціального зв'язку та захисту інформації України, сфера науки та освіти входить до лідерів серед галузей, на які спрямовано найбільшу кількість методів реалізації кіберзагроз. Умови повномасштабного воєнного стану та тривалих надзвичайних ситуацій в Україні призвели до екстреного переходу ЗВО на дистанційні та асинхронні форми навчання, що критично підвищило ризиковий профіль установ. Персонал та здобувачі змушені підключатися до внутрішніх інформаційних ресурсів через незахищені канали зв'язку, використовувати домашні пристрої в межах концепції BYOD (Bring Your Own Device) та послуги сторонніх провайдерів. Це створює сприятливі умови для успішної реалізації атак з використанням методів соціальної інженерії, фішингу, розповсюдження шкідливого програмного забезпечення та деструктивної дезінформації.

У цьому контексті побудова надійної системи кіберзахисту ЗВО не може обмежуватися виключно технічними та програмно-апаратними засобами захисту (міжмережевими екранами, системами виявлення вторгнень тощо). Як показує практика, більшість успішних кіберінцидентів пов'язана з помилками користувачів або їхньою низькою освіченістю у сфері інформаційної безпеки. Провідним механізмом забезпечення стійкості ЗВО є впровадження системи управління інформаційною безпекою (СУІБ), проте її ефективне функціонування неможливе без безперервного підвищення рівня культури кібербезпеки, кібергігієни та освіченості всіх зацікавлених сторін.

Питання впровадження СУІБ регламентуються базовим міжнародним стандартом ISO/IEC 27001 (в Україні діє актуальна гармонізована версія ДСТУ ISO/IEC 27001:2023), який вимагає комплексного, ризик-орієнтованого підходу до управління інформаційними активами установи. У межах цього стандарту окрема увага приділяється людському чиннику. Зокрема, положення розділів 7.2 «Компетентність» та 7.3 «Поінформованість» зобов'язують організацію забезпечити необхідний рівень підготовки персоналу та його регулярне інформування про вимоги політики безпеки СУІБ. Додатково, у Додатку А до стандарту (захід контролю А.6.3) підкреслюється потреба у наданні регулярної освіти та навчання персоналу.

Теоретичні основи побудови комплексних навчальних програм з кібербезпеки викладені в керівництві Національного інституту стандартів і технологій США NIST SP 800-50r1 «Building a Cybersecurity and Privacy Learning Program» (вересень 2024 р.). Цей документ пропонує адаптивну модель розгортання програм навчання, орієнтовану на ролі, ризик-середовище та місію організації.

Специфіку впровадження СУІБ та управління ризиками, пов'язаними з персоналом в українських установах, детально розглянуто у працях Д.С. Тимофєєва та А.С. Совенка (2023). Автори наголошують на важливості процесного підходу для мінімізації інсайдерських загроз і наводять класифікацію порушників відповідно до вимог ISO/IEC 27001. Крім того, Д.С. Тимофєєв, О.В. Кручинін та В.О. Святошенко (2023) досліджували особливості реалізації архітектури нульової довіри (Zero Trust Architecture, ZTA) в інтеграції з СУІБ вітчизняних ЗВО, вказуючи на кадровий дефіцит та гетерогенність мережевого середовища як основні бар'єри.

Аналіз інформаційних ризиків в освіті в умовах надзвичайних ситуацій здійснено М. Пригарою, І. Опірським та М. Різаком (2023). Ними систематизовано ключові загрози дистанційного навчання та низької інформаційної компетентності працівників. У свою чергу, методи навчання студентів та залучення їх до

превентивної протидії дезінформації й перевірки цілісності даних описані в дослідженнях А. Давиденка, О. Висоцької та В. Щербини (2023).

Поведінкові аспекти кібербезпеки в організаціях часто базуються на використанні моделі КАВ (Knowledge-Attitude-Behavior), яка лежить в основі відомого опитувальника HAIS-Q (Human Aspects of Information Security Questionnaire), валідованого К. Парсонс та співавторами (2017). Відповідно до цієї моделі, системне накопичення знань (Knowledge) безпосередньо впливає на формування стійкого і позитивного внутрішнього ставлення (Attitude) до правил безпеки, що, у свою чергу, трансформується у безпечну повсякденну поведінку (Behavior) на робочому місці та мінімізує ймовірність успішного застосування проти персоналу методів соціальної інженерії.

Метою даної роботи є дослідження та обґрунтування комплексного науково-практичного підходу до підвищення рівня освіченості та обізнаності з інформаційної та кібербезпеки співробітників і здобувачів вищої освіти в ЗВО, що є критично необхідним етапом успішного впровадження системи управління інформаційною безпекою (СУІБ) та побудови надійної культури кібергігієни.

Аналіз ризиків інформаційної безпеки, проведений у ЗВО України за останні роки, показує, що екстрений перехід на дистанційне навчання призвів до появи специфічної групи вразливостей, безпосередньо пов'язаних із діяльністю персоналу. М. Пригара та ін. (2023) виділяють наступні ключові проблеми:

1) Низький рівень інформаційної компетентності працівників. Багато представників професорсько-викладацького складу та адміністративного персоналу не володіють базовими навичками кібергігієни, не розуміють принципів безпечної обробки та збереження конфіденційних даних.

2) Використання сторонніх хмарних ресурсів та сервісів сумнівного характеру для організації освітнього процесу, що призводить до неконтрольованої передачі персональних даних третім особам.

3) Зміна фактичного власника даних з навчального закладу на фізичну особу — працівника. Документи та дані починають зберігатися на особистих комп'ютерах викладачів, які часто позбавлені елементарного захисту (ліцензійного антивірусу, регулярного оновлення операційної системи).

4) Використання ненадійних або налаштованих за замовчуванням засобів ідентифікації та авторизації для внутрішніх інформаційно-комунікаційних систем (ІКС) університету, а також повторне використання слабких паролів.

5) Вразливість до атак соціальної інженерії та фішингу, спрямованих на викрадення корпоративних облікових записів.

Людський фактор в умовах ЗВО ускладнюється постійною ротацією здобувачів освітніх послуг, які щороку приходять до університету з різним початковим рівнем підготовки. Вони є надзвичайно активними споживачами контенту в соціальних мережах та месенджерах, що робить їх першочерговою цілью для маніпулятивних інформаційних операцій, кібершахрайства та поширення деструктивної дезінформації. Без систематичного навчання правилам безпечної поведінки в цифровому просторі, будь-який користувач мережі ЗВО стає потенційною точкою входу для зломисників.

Успішне впровадження СУІБ в університеті вимагає формалізації вимог до навчання персоналу відповідно до міжнародних і національних стандартів. ДСТУ ISO/IEC 27001:2023 чітко розмежовує два поняття: компетентність і поінформованість.

Положення пункту 7.2 «Компетентність» вимагає від ЗВО визначити необхідну кваліфікацію осіб, чия діяльність безпосередньо впливає на стан інформаційної безпеки організації. Це стосується як ІТ-фахівців, так і адміністраторів баз даних, керівників підрозділів та відповідальних осіб. Університет зобов'язаний забезпечити цю компетентність через навчання, наставництво або залучення аутсорсингових фахівців, а також обов'язково оцінювати ефективність проведених навчальних заходів і підтримувати відповідну задокументовану інформацію (сертифікати, звіти).

Пункт 7.3 «Поінформованість» (Awareness) стосується всіх працівників ЗВО та залучених сторін (зокрема здобувачів освіти). Співробітники мають бути поінформовані про чинну Політику інформаційної безпеки ЗВО, свій особистий внесок в ефективність функціонування СУІБ (включаючи вигоди від покращення показників безпеки) та наслідки, які можуть виникнути в результаті недотримання або порушення встановлених регламентів.

Фреймворк NIST SP 800-50r1 пропонує розглядати навчання з кібербезпеки як життєвий цикл, інтегрований у загальний процес управління ризиками організації. Згідно з NIST, програма підвищення обізнаності та навчання має бути гнучкою, динамічно адаптуватися до змін безпекового середовища (наприклад, появи нових загроз, пов'язаних із технологіями генеративного штучного інтелекту чи Інтернетом речей) та забезпечувати отримання якісного й кількісного зворотного зв'язку. Процес оцінки результатів тренінгів має відбуватися безперервно з метою постійного вдосконалення навчальних матеріалів.

Для систематичного та комплексного навчання співробітників і студентів університету в процесі впровадження СУІБ доцільно розробити уніфіковану навчальну програму, адаптовану до специфіки академічного середовища. Структура такої програми, має базуватися на кращих практиках кібергігієни та закривати основні виявлені ризики. За основу може бути взята типова програма, представлена у Додатку до Наказу Адміністрації Держспецзв'язку від 21.10.2025 № 661.

Основні модулі програми: основи кібергігієни, захист облікових записів, безпека мобільних пристроїв, електронна пошта, соціальна інженерія, безпечне користування мережею інтернет, захист персональних даних, соціальні мережі та месенджери, поведінка під час кіберінцидентів, робота з корпоративними системами,

віддалена робота та кібергігієна, профілактичні заходи та навчання, вплив технологій штучного інтелекту на конфіденційність, протидія дезінформації, безпека інтернету речей (IoT).

Запропонована структура програми охоплює основні виміри взаємодії користувача з інформаційним простором університету. Модульний характер дозволяє адаптувати тривалість та глибину викладання залежно від цільової аудиторії за ролями: здобувачів освітніх послуг технічних та нетехнічних спеціальностей, адміністрації університету, науково-педагогічного та педагогічного персоналу, фахівців служб університету, ІТ-фахівців, зовнішніх постачальників послуг.

Традиційні лекційні методи навчання часто демонструють низьку ефективність, оскільки не забезпечують перетворення теоретичних знань на стійкі поведінкові навички. Для досягнення максимального результату в процесі впровадження СУІБ необхідно поєднувати теоретичну підготовку з сучасними інтерактивними та практичними інструментами:

1) Використання спеціалізованих кіберполігонів (Cyber Ranges). Кіберполігони дозволяють моделювати реалістичні сценарії кібератак і захисту в безпечному, ізольованому середовищі. Наприклад, досвід Ужгородського національного університету довів високу ефективність проведення комплексних навчань у форматі хакатонів, під час яких учасники діляться на команду атаки (Red Team) та команду захисту (Blue Team). Такий підхід дозволяє системним адміністраторам, викладачам та студентам ІТ-спеціальностей відпрацьовувати навички виявлення, локалізації та ліквідації наслідків реальних кібератак у режимі реального часу (Малицький та ін., 2023).

2) Залучення відкритих та хмарних освітніх платформ з кібербезпеки. Для підвищення практичних навичок користувачів доцільно використовувати спеціалізовані онлайн-платформи, такі як HackTheBox, TryHackMe, RangeForce, Cybrary. В.О. Святошенко, О.В. Кручинін та Д.С. Тимофеев (2023) виділяє низку вимог, яким мають відповідати такі платформи під час інтеграції в освітній процес ЗВО: високий рівень доступності для користувачів різного рівня, підтримка індивідуальних траєкторій навчання, актуальність навчальних матеріалів, інтерактивність, підтримка гейміфікації (ігрового змагального процесу) та гнучкий контроль і оцінювання прогресу.

3) Симуляція атак соціальної інженерії. Проведення контрольованих фішингових розсилок департаментом кібербезпеки університету дозволяє оцінити реальну пильність персоналу. Співробітники, які переходять за посиланнями у тестових листах, автоматично перенаправляються на короткі навчальні курси з розпізнавання фішингу. Це дозволяє наочно продемонструвати наслідки недбалості без ризику для реальної інфраструктури.

4) Практичні лабораторні роботи з протидії дезінформації та аналізу джерел. А. Давиденко та ін. (2023) пропонують залучати студентів до фіксації деструктивної дезінформації в кіберпросторі. Навчання включає формування навичок пошуку першоджерела інформації, ручного та автоматизованого виявлення фейків, а також правильного копіювання інформації зі збереженням її автентичності (використання дзеркал веб-сайтів, фіксація дати, забезпечення цілісності копії за допомогою хешування та накладення цифрового підпису). Будь-яка освітня активність у рамках СУІБ є процесом, який підлягає регулярному аудиту, оцінюванню та покращенню згідно з принципами циклу Демінга (PDCA - Plan-Do-Check-Act), що відображено у вимогах ДСТУ ISO/IEC 27001 (пункт 10.1 «Постійне вдосконалення»). Оцінювання ефективності програми навчання за рекомендаціями NIST SP 800-50r1 та ISO 10015 має включати три основні рівні:

– рівень засвоєння знань (первинна оцінка): проведення тестувань, опитувань та виконання практичних завдань одразу після завершення навчального курсу або окремого модуля.

– поведінковий рівень (довгострокова оцінка): аналіз змін у щоденній поведінці персоналу. Показниками покращення є зменшення кількості успішно реалізованих фішингових атак під час симуляцій, підвищення швидкості повідомлення про підозрілі листи до служби підтримки, а також зменшення кількості інцидентів, пов'язаних із порушенням правил доступу.

– організаційний рівень (метрики СУІБ): оцінка загального впливу на стан кібербезпеки університету, зокрема скорочення часу виявлення та локалізації кіберінцидентів, зменшення фінансових та репутаційних втрат.

Зворотний зв'язок від слухачів та результати регулярних аудитів поведінки мають використовуватися для оновлення навчального контенту, адаптації складності модулів і впровадження нових рішень у програму.

Висновки. Підвищення рівня освіченості з інформаційної та кібербезпеки в процесі впровадження СУІБ університету є стратегічно важливим і безперервним процесом. Людський фактор залишається однією з найбільш критичних вразливостей будь-якої системи захисту, що особливо гостро відчувається в академічному середовищі в умовах воєнного стану та дистанційного навчання.

Інтеграція вимог стандартів ДСТУ ISO/IEC 27001 та NIST SP 800-50r1 дозволяє побудувати системну, ризик-орієнтовану модель навчання. Застосування модульної навчальної програми у поєднанні з поведінковою моделлю КАВ та сучасними практичними інструментами (кіберполігонами, симуляціями атак та освітніми платформами) дає змогу сформувати у викладачів, співробітників і студентів стійкі навички кібергігієни. Це суттєво знижує ймовірність виникнення кіберінцидентів, забезпечує цілісність, конфіденційність і доступність інформаційних активів ЗВО та створює надійне підґрунтя для сталого функціонування університету в сучасному динамічному кіберсередовищі.

Література

1. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист приватності. Системи управління інформаційною безпекою. Вимоги. — К. : ДП «УкрНДНЦ», 2023. — 21 с.
2. NIST Special Publication 800-50r1. Building a Cybersecurity and Privacy Learning Program. — National Institute of Standards and Technology, September 2024. — 42 p.
3. Тимофєєв Д. С., Совенко А. С. Мінімізація ризиків пов'язаних з персоналом в процесі впровадження системи управління інформаційною безпекою відповідно до вимог стандарту ISO/IEC 27001:2022 // Проблеми використання інформаційних технологій в освіті, науці та промисловості: XVIII міжнар. конф. (24 листопада 2023 р., м. Дніпро): зб. наук. пр. — Дніпро : Журфонд, 2025. — № 8. — С. 201–205.
4. Тимофєєв Д. С., Кручинін О. В., Святошенко В. О. Реалізація архітектури нульової довіри в процесі впровадження системи управління інформаційною безпекою закладів вищої освіти України // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). — К. : НАУ, 2023. — С. 56–58.
5. Пригара М., Опірський І., Різак М. Оцінка виявлених ризиків інформаційної безпеки в освіті в умовах надзвичайних ситуацій // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). — К. : НАУ, 2023. — С. 105–108.
6. Малицький Б., Черепов О., Буковецький В., Різак В. Полігон для проведення комплексних навчань з багаторівневого захисту від кібератак // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). — К. : НАУ, 2023. — С. 27–28.
7. Давиденко А., Висоцька О., Щербина В. Фіксація деструктивної дезінформації в кіберпросторі за участі студентів спеціальності «Кібербезпека» // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). — К. : НАУ, 2023. — С. 19–21.
8. Святошенко В. О., Кручинін О. В., Тимофєєв Д. С. Порівняльний аналіз відкритих платформ з кібербезпеки // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф. (м. Ужгород, 2-4 травня 2023 р.). — К. : НАУ, 2023. — С. 54–55.
9. Parsons K., Calic D., Pattinson M., Butavicius M., McCormac A., Zwaans T. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies // Computers & Security. — 2017. — Vol. 66. — P. 40–51.
10. Про затвердження Методичних рекомендацій щодо проведення інструктажів і тренінгів щодо кібергігієни на період призначення на посади державних службовців, працівників органів державної влади та інших державних органів, військовослужбовців, керівників та працівників державних підприємств, установ та організацій: Наказ Адміністрації Держспецзв'язку від 21.10.2025 № 661. URL: <https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-21-10-2025-661-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-provedennya-instrukтажiv-i-treningiv-shodo-kibergigiyeni-na-period-priznachennya-na-posadi-derzhavnikh-sluzhbovciv-pracivnikiv-organiv-derzhavnoyi-vladi-ta-inshikh-derzhavnikh-organiv-viiskovosluzhbovciv-kerivnikiv-ta-pracivnikiv-derzhavnikh-pidpriyemstv-ustanov-ta-organizacii> (дата звернення: 11.08.2026).

УДК 004.056.5

Гончаров М.О., Колованова Є.П., Малахов С.В.

ОСНОВНІ СКЛАДОВІ КОНЦЕПЦІЇ БАГАТОРІВНЕВОГО МУЛЬТИПЛЕКСУВАННЯ ДАНИХ ПРИ РЕАЛІЗАЦІЇ ГІБРИДНОГО СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ

Харківський національний університет імені В. Н. Каразіна
m.honcharov@student.karazin.ua (ORCID: 0000-0002-9790-7260)
e.kolovanova@karazin.ua (ORCID: 0000-0002-0326-2394)
malakhov@karazin.ua (ORCID: 0000-0001-8826-1616)

Анотація. Розглянуто концепцію багаторівневого мультимплексування відеоданих - контенту при реалізації гібридної схеми стеганоалгоритму. Характерні умови застосування – спорадичний дефіцит вільних ресурсів використовуваних апаратних (мобільних) платформ. Досліджено механізм дворівневого мультимплексування, де міжблоковий рівень забезпечує обфускацію поточних параметрів масиву довжин серій контенту, а внутрішньоблоковий - обфускацію його DC-коєфіцієнтів з координатами (0;0). Інкапсуляція даних контенту здійснено в низькочастотну область DCT матриць зображення контейнеру. Встановлено, що цілісність складеного ключа екстрактора даних, що визначає основні параметри обробки діючих пар в системі «контент-контейнер», є визначальною умовою для коректного вилучення прихованого контенту. Порушення (або невдалий підбір) поточних параметрів обробки призводить до руйнування контенту та неможливості його коректного відновлення. Проведене моделювання різних комбінацій діючих пар системи «контент-

контейнер» та різних варіантів підбору (атаки) контенту підтверджують можливість адаптивної обробки в умовах дефіциту обчислювальних ресурсів та високу стійкість до спроб нелегітимної екстракції контенту.

Ключові слова: кібербезпека, стеганографія, цифрові зображення, несанкціонований доступ, обчислювальна складність, просторова орієнтація, ресурсний консенсус, кодування довжин серій, ДКП.

Вступ. Розвиток інформаційно-комунікаційних систем (ІКС) і масштабне впровадження методів штучного інтелекту й машинного навчання (AI/ML), суттєвим чином трансформують звичні підходи до обробки, обміну та захисту цифрових даних. У цьому контексті забезпечення конфіденційності і прихованості інформації, яка циркулює в сучасних ІКС, є одним із пріоритетних завдань кібербезпеки. Цифрова стеганографія традиційно залишається надійним інструментом захисту, оскільки приховує сам факт наявності секретного повідомлення [1-3]. Проте еволюція технологій AI/ML та їх адаптація під специфіку завдань стеганографії, неминуче підвищує ефективність можливостей стеганографічного аналізу. Це, в свою чергу, створює нові виклики, вимагаючи від сучасних стеганографічних алгоритмів не лише високої стійкості до виявлення прихованого контенту, але й підтримці високої обчислювальної ефективності, що є критично важливим критерієм для мобільних платформ та/чи систем з обмеженими апаратними ресурсами. Для досягнення бажаного балансу між функціональною простотою, швидкістю обробки та стійкістю контенту до спроб його неавторизованого вилучення, перспективним напрямом є оптимізація базових процедур підготовки вихідних даних в межах діючої пари «контент-контейнер» [4]. Зокрема, до таких кроків належить використання методів попередньої обробки [5], специфічних схем вибірки (розгортки) даних вихідних зображень [6], зміни просторової орієнтації опорних блоків (ОБ) масиву довжин серій зображення-контенту та процедур багаторівневого мультимплексу даних [7]. Проведене моделювання показало, що послідовне застосування зазначених процедур, забезпечує необхідні механізми протидії спробам нелегітимної екстракції даних та дозволяє отримати бажаний ефект без надмірних обчислювальних витрат. Такі операції не погіршують візуальну якість контейнера, проте утворюють складні процедурні залежності, які роблять несанкціоновану екстракцію даних, енергетично обтяжливим завданням з високою невизначеністю витраченого (необхідного) на це часу.

Зважаючи на необхідність комплексної інтеграції зазначених вище механізмів обробки, головною метою даного матеріалу є стислий розгляд можливостей концепції багаторівневого мультимплексу даних в межах реалізації гібридного стеганоалгоритму [4]. Такий підхід спрямований на гнучке управління параметрами стегановставки та формування унікальної структури ключа екстрактора даних [7]. Складений ключ жорстко регламентує процеси інкапсуляції й вилучення даних на всіх основних етапах обробки [4] та передбачає гнучку структуру власних станів, залежно від поточних умов обробки й статистичних властивостей діючих пар «контент-контейнер». Надійність алгоритму досягається шляхом впровадження низки автономних процедур захисту, параметри яких визначаються поточним станом ключа екстрактора. Завдяки такій архітектурі, спроба неавторизованого втручання або невдалого підбору ключа руйнує прихований стеганографічний контент, забезпечуючи стійкість до його компрометації.

Основна частина. Побудова гібридного стеганографічного алгоритму за рахунок впровадження концепції багаторівневого мультимплексу даних, дає змогу позиціонувати його як гнучке та малоресурсне рішення для захисту даних у складі мобільних платформ [4]. У межах відпрацювання даної концепції проведено дослідження різних варіантів передобробки зображень, спрямованих на згладжування їх малоінформативних ділянок. За результатами моделювань отримано оцінки продуктивності окремих етапів алгоритму за часом виконання основних процедур [5-6,8-9], оцінено якість відновлення даних за показником PSNR (Peak Signal-to-Noise Ratio) та досліджено властивості отримуваних дисперитету, стосовно кількості сформованих ОБ, в системі «контент-контейнер» для різних типів зображень. Дослідний прототип алгоритму побудований на комплексному використанні різноманітних властивостей, ефектів і методів кодування відеоданих [4,10]. Синтез цих параметрів (як для контейнера, так і для контенту) забезпечує широкий простір комбінаторики можливих станів структури складеного ключа екстрактора даних [7]. Саме висока варіативність параметрів кодування на різних рівнях захисту, зумовлює унікальну структуру ключа екстрактора даних [7], що жорстко регламентує процеси стегановставки й легітимного вилучення інформації. Будь-яке порушення цілісності ключа призводить до незворотної втрати або суттєвого викривлення прихованих даних, що підвищує загальну стійкість контенту до спроб його неавторизованого вилучення. З метою наочної демонстрації базових принципів роботи алгоритму [4], спрощену концептуальну структуру складеного ключа наведено на рис. 1. На даному етапі схема відображає лише загальну логіку взаємодії основних модулів без надмірної деталізації.

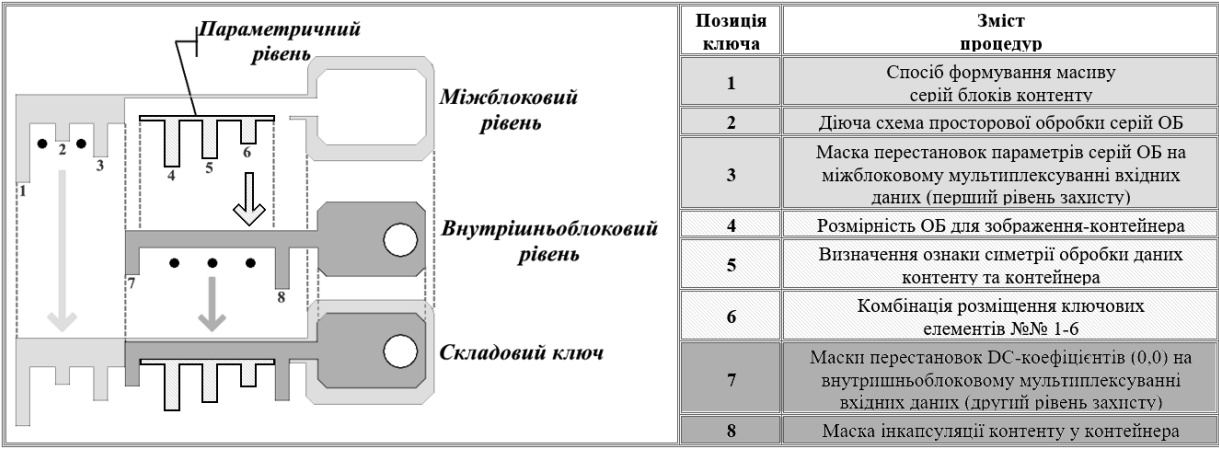


Рис. 1. Тестова структура ключа екстрактора даних гібридного стеганоалгоритму

Ключовим завданням для створення сучасних стеганографічних алгоритмів є забезпечення компромісу між низкою суперечливих чинників й вимог: забезпечення високої скритності факту передачі даних, стійкістю вбудованого контенту, а також мінімальною обчислювальною складністю та енергоємністю використовуваних процедур обробки [4-8]. Вирішення цієї проблеми досягається шляхом адаптивної оптимізації алгоритмічних процесів, що безпосередньо спирається на статистичні та просторові властивості цифрового середовища. В спрощеному вигляді, структура запропонованого алгоритму складається з 4-х основних функціональних модулів [4]:

1. Попередня підготовка вихідних даних. На цьому етапі виконується глибокий аналіз структури зображення з метою виявлення малоінформативних областей, які піддаються процедурі контрольованого фоновому згладжування текстури [5]. Процес реалізується через два послідовні аспекти. Суть першого аспекту полягає в оцінці ймовірності перепаду яскравості/кольору між сусідніми пікселями [8], що дозволяє детально проаналізувати зображення та визначити загальну текстурну складність. На основі отриманих даних користувач має можливість оцінити тип зображення та вручну визначити доцільні параметри для наступного етапу [6]. Другий аспект реалізується як окрема процедура згладжування самих блоків [5], що працює за власним критерієм порівняння блоків зображення. Результати розрахованих градієнтних карт та оцінки текстурної складності дозволяють визначати оптимальні параметри значення порогу закруглення (P_{Z1}). Відповідно, якщо цей перепад виявляється меншим за заздалегідь встановлений поріг закруглення, алгоритм штучно вирівнює значення пікселів на цій ділянці, при цьому різкі контури та важливі деталі залишаються недоторканими. Таке згладжування дозволяє ефективно усунути надлишковий флуктуаційний шум та зменшити кількість візуально непомітних перепадів яскравості, що створює оптимальні стартові умови для наступного етапу функціонального модулю [4-5,8-9]. Завдяки усуненню надлишкової інформації на старті, значно знижується обчислювальне навантаження на наступні модулі алгоритму, оскільки зменшується загальна кількість сформованих ОБ, що потребують складних математичних перетворень (наприклад, на етапі ДКП (DCT) [10]). Важливою перевагою цього етапу є можливість гнучкої адаптації параметру згладжування під різні типи зображень та/чи поточні апаратні обмеження базового пристрою. Усе це дозволяє знаходити необхідний компроміс між високою швидкістю обробки, економією обчислювальних ресурсів та збереженням потрібної візуальної якості контейнера-переносника [4-5].

2. Формування масиву довжин серій ОБ. На цьому етапі здійснюється формування масиву довжин серій ОБ [4,10], що є критично важливим для створення потрібних умов для подальшої інкапсуляції контенту та зменшення загальної обчислювальної складності алгоритму. Залежно від отриманих статистичних співвідношень системи «контент-контейнер», згладжені масиви вихідних даних поділяються на блоки відповідної розмірності, після чого виконується їх послідовний обхід за обраною схемою розгортки [6,10]. Застосована схема розгортки, формує окремий рівень захисту [6], стан налаштувань якого, визначає відповідний елемент в структурі ключа екстрактора даних [7]. Схеми розгортки умовно поділяються на прості лінійні, нелінійні, багатопрохідні (кратні) та випадкові. Якщо прості лінійні схеми забезпечують мінімальні часові витрати, то складні, зигзагоподібні чи двопрохідні розгортки суттєво ускладнюють аналіз статистичних залежностей для атакуючого і формують окремий дієвий рівень захисту при помірному зростанні обчислювальних витрат [6]. **Формування масиву довжин серій ОБ** контенту, базується на аналізі подібності сусідніх блоків за критерієм «порога закруглення» - P_{Z2} [6,8], який оцінює різницю між max та min значеннями яскравості елементів сусідніх (за розгорткою) блоків. Так, якщо ця різниця є несуттєвою, блоки вважаються подібними і групуються в одну серію, а при перевищенні значення « P_{Z2} », цій блок маркується, як початок нової серії. Проведене моделювання показало, що процес формування масиву серій ОБ контенту, є базовою процедурою для покращення енергоефективності всіх наступних перетворень. Водночас додатковим шаром захисту на цьому етапі є **зміна просторової орієнтації** ОБ контенту [7,11], що передбачає їх геометричні перетворення, такі як обертання, горизонтальне та/чи вертикальне віддзеркалення або їх комбінації. Ці оборотні просторові маніпуляції є обчислювально простими, проте кардинально змінюють порядок відновлення блоків,

навіть якщо зломисник вірно підбере схему розгортки та розмір блоків, помилка у просторовій орієнтації ОБ призведе до критичної втрати цілісності відновленого зображення [11]. Широка варіативність діючих станів розгортки та просторової орієнтації ОБ, утворює незалежну багатoshарову систему захисту, яка передбачає величезну кількість комбінацій станів ключа екстрактора даних, роблячи несанкціоноване вилучення контенту вкрай ресурсомістким. Баланс між припустимим ступенем викривлень отриманого масиву ОБ та середньої кількістю сформованих серій (дилема «якість – швидкість»), зумовлюється встановленими параметрами обробки, а саме: розмірністю маски згладжування (n), значеннями P_{Z1} та P_{Z2} й розмірністю блоків (N) [4]. Зазначена логіка процесу дозволяє створити оптимальні для поточних обмежень, умови обробки та інкапсуляції контенту. Така модель дій, спрямована на максимальне використання наявного диспаритету поточних статистичних властивостей елементів системи «контент-контейнер».

3. Мультиплексування даних контенту. Механізм мультиплексування даних забезпечує основний механізм протидії спробам несанкціонованого вилучення прихованої інформації [4,7,9]. Суть мультиплексування полягає у перетворенні та взаємній перестановці вихідних даних згідно із заданою маскою. Це ускладнює встановлення взаємозв'язків між елементами прихованої інформації та їхнім початковим розташуванням. Кожен рівень такої обробки формує власну незалежну позицію в структурі складеного ключа екстрактора [7], що суттєво розширює комбінаторику алгоритму та підвищує його захищеність. Першим процедурним рівнем виступає **міжблокове мультиплексування**, під час якого відбувається перемішування двох основних параметрів: самих ОБ та відповідних їм значень довжин серій. Глибина та складність цього перемішування залежать від обраної маски [9], яка моделюється у двох варіантах (для діючого релізу прототипу). Наступним важливим кроком, що передує другому рівню мультиплексування є кодування з перетворенням ОБ масивів серій. Реалізується як для контенту, так і для контейнеру. В обох випадках для першого блоку кожної серії ОБ, виконується дискретне косинусне перетворення (ДКП, або DCT) з подальшою селекцією та квантуванням для найбільш значущих коефіцієнтів [9]. Після виконання зазначеного кодування алгоритм переходить до другого рівня захисту - **внутрішньоблокового мультиплексування** даних [9]. Цей рівень працює виключно з DC-коефіцієнтами трансформант з координатами (0,0), які відповідають за середню яскравість кожного ОБ контенту. Діючий алгоритм передбачає роздільну обробку окремих елементів вихідного масиву, що дозволяє досягти високого ступеня структурної дефрагментації контенту без значних обчислювальних витрат. Одночасне застосування обох рівнів захисту забезпечує режим дворівневого мультиплексування даних контенту [9]. Саме цей режим є ключовим для максимального посилення стійкості прихованої інформації до спроб її неавторизованого вилучення. Перший рівень змінює просторове розташування ОБ та модифікує наявну структуру масиву довжин серій ОБ контенту, а другий рівень оперує з кутовими коефіцієнтами DCT перетворення [9-10]. Синергія різних рівнів призводить до контрольованого руйнування кореляційних зв'язків елементів вихідного масиву контенту. Навіть у разі одночасної компрометації міжблокового і параметричного рівнів захисту, наявність додаткового незалежного рівня [8-9] призведе до руйнування даних при неавторизованому відновленні [6]. При цьому вибір діючої комбінації рівнів є результатом оперативного вирішення завдання [5-6,8], щодо забезпечення поточного ресурсного консенсусу для виконання головної задачі – стегановставки даних.

4. Інкапсуляція даних. Після етапу внутрішньоблокового мультиплексування застосовуються методи інкапсуляції, під час яких у матриці ДКП записуються біти секретного повідомлення. Після цього виконуються зворотні операції (ЗДКП), демультимплексування, блоки повертаються на свої початкові місця, і відновлюється фінальне зображення із вбудованою інформацією. Слід зазначити, що повноцінну роботу запропонованого алгоритму й виконання всіх необхідних умов безпеки демонструють усі алгоритми інкапсуляції, які пов'язані з роботою в низько- та середньо- частотній області спектральних коефіцієнтів DCT трансформант. Процедура декодування реалізована, як окремий програмний модуль, на вхід якого подається сформований стегоконтейнер. При цьому повністю зберігається принцип «сліпого витягнення» даних. Для коректного відновлення прихованого повідомлення необхідний точний набір налаштувань, формалізований у вигляді складеного ключа екстрактора. Якщо хоча б один його елемент введено некоректно, система видасть лише набір шуму та помилок. Наразі точність відновлення приховуваного контенту коливається в межах 95-100%. Поодинокі помилки пов'язані з особливостями математичного округлення коефіцієнтів після виконання зворотного DCT [10]. Тому для збереження візуальної якості контейнера доцільно використовувати методи завадостійкого кодування, які дозволять гарантовано відновити вихідне повідомлення та виправити появу «битих бітів» після етапу екстракції.

Висновки. Розглянуто основні складові концепції багаторівневого мультиплексу даних гібридного стеганоалгоритму [4,7]. Представлена реалізація може розглядатися, як гнучке, малоресурсне рішення для стеганографічного захисту чутливої інформації в сучасних мультисервісних ІКС. Запропонована парадигма логіки дій спирається на адаптивну модифікацію базових процедур (Етапів) підготовки і обробки приховуваного контенту [4-9]. Початкове згладжування текстури зображення-контенту дозволяє усунути присутній флуктуаційний шум, забезпечуючи потрібні умови для подальшого формування масиву довжин серій ОБ контенту та посилення диспаритету статистичних властивостей даних в системі взаємодіючих пар - «контент-контейнер». Виконання цих процедур зменшує загальну кількість ОБ, які потребують проведення DCT, що в свою чергу, дозволяє забезпечити підтримку ресурсного консенсусу в умовах спорадичного дефіциту вільних ресурсів [4-5]. Своєю чергою, простота і широка варіативність застосовуваних схем розгортки, способів просторової орієнтації ОБ контенту та варіантів дворівневого мультиплексування, загалом

створюють простий але потужний механізм з протидії спробам несанкціонованій екстракції даних [4-7,9]. Цей захисний механізм жорстко прив'язаний до конфігурації й параметрів окремих елементів складеного ключа екстрактора даних. Їх порушення гарантує незворотне руйнування кореляційних зв'язків у прихованих даних [7] і, як наслідок, хибне відновлення даних [6,9]. Реалізована багаторівнева схема обробки найбільш сумісна з механізмом інкапсуляції даних в низькочастотній області матриць DCT [10], оскільки вони спільно оперують DC-коефіцієнтами [4,9]. Практична апробація модуля «сліпого» витягнення даних, підтвердила широкий потенціал розглянутої концепції, проте виявила прояви випадків поодиноких втрат інформації через процеси математичного округлення й фільтрації коефіцієнтів при зворотному DCT [10]. При цьому нарощування «потужності» вбудовування для компенсації цих втрат неминуче провокує появу демаскуючих візуальних артефактів контейнеру-переноснику. Тому, в даному випадку, пошук можливих рішень слід шукати в удосконаленні механізму збереження/компенсації енергії для виключених DCT коефіцієнтів. Подальший розвиток розглянутої концепції базується на інтеграції методів завадостійкого кодування для гарантованого відновлення цілісності повідомлення при збереженні початкової візуальної якості контейнера-переносника. В цілому, за сукупністю отримуваних властивостей й якостей, розглянуті механізми обробки виявляють потрібний потенціал й свідчать про необхідність подальшого аналізу їх характеристик та уточнення граничних умов застосування.

Література

1. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge : Cambridge University Press, 2009. 448 p.
2. Кузнецов О. О., Євсеев С. П., Король О. Г. Стеганографія : навч. посіб. Харків : Вид-во ХНЕУ, 2011. 264 с. URL: <http://www.repository.hneu.edu.ua/jspui/handle/123456789/2289>
3. Коначович Г., Прогонов Д., Пузиренко О. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. Київ : Центр навчальної літератури, 2018. 336 с.
4. Гончаров М., Лесная Ю., Малахов С. Дослідження властивостей прототипу гібридного стеганоалгоритму. Комп'ютерні науки та кібербезпека. 2021. № 2. С. 45–56. DOI: <https://doi.org/10.26565/2519-2310-2021-2-05>
5. Honcharov M. O., Nariezhnii O. P., Malakhov S. V. Analysis of prerequisites for ensuring resource consensus when performing steganographic data insertion procedures. Сучасний захист інформації. 2025. № 3. С. 37–47. DOI: <https://doi.org/10.31673/2409-7292.2025.030518>
6. Гончаров М. О., Малахов С. В., Жіленков Д. В. Дослідження складності та властивостей різних схем розгортки вихідних даних стеганоконтента, в умовах зміни сценаріїв атак. Сучасний захист інформації. 2025. № 4. С. 44–58. DOI: <https://doi.org/10.31673/2409-7292.2025.041205>
7. Honcharov M., Malakhov S. Modeling attempts of unauthorized extraction of steganoccontent under different combinations of data key-extractor. Collection of Scientific Papers «ЛОГОС» (Paris, France, March 1, 2024). P. 234–245. DOI: <https://doi.org/10.36074/logos-01.03.2024.053>
8. Гончаров М., Малахов С. Застосування ймовірнісних карт градієнтів яскравості цифрових зображень для коригування параметрів стеганографічної вставки даних. Кібербезпека: освіта, наука, техніка. 2026. № 1(33). С. 255–273. DOI: <https://doi.org/10.28925/2663-4023.2026.33.1163>
9. Лесная Ю., Гончаров М., Малахов С. Результати моделювання спроб несанкціонованого вилучення стеганоконтенту для різних комбінацій атаки дослідного стегоалгоритму. Scientific Collection «InterConf». 2023. № 141. С. 338–345. URL: <https://archive.interconf.center/index.php/conference-proceeding/article/view/2319>
10. Pratt W. K. Digital image processing. New York : John Wiley & Sons, 1978.
11. Гончаров М., Малахов С. Оцінка результатів просторових перетворень опорних блоків контенту як окремого етапу гібридного стеганоалгоритму. Комп'ютерні науки та кібербезпека. 2025. № 2. С. 6–20. URL: <https://periodicals.karazin.ua/cscs/article/view/2519-2310-2025-2-01>

UDC 004.056.53

Iurii Zhurov

BASELINE CONTROL COVERAGE IN RESOURCE-CONSTRAINED ORGANIZATIONS:
STRUCTURAL CAUSES OF CYBERSECURITY UNDERINVESTMENT IN SMALL BUSINESS

SMB Cybersecurity Advisors LLC, Palm Harbor, Florida, USA
iurii.zhurov@smbsecurityadvisors.com

Abstract. *The small-business segment shows the widest gap between the effectiveness of baseline security controls and the extent of their implementation. Two models are proposed. The first shows the efficient frontier of coverage against implementation effort to be concave by construction, so marginal cost is necessarily non-decreasing;*

what is empirical is the dispersion of control efficiency, estimated at four orders of magnitude. The second treats the cost of interpreting a control framework as indivisible, yielding a per-employee burden hyperbolic in headcount with a crossover near 67 employees. Underimplementation is attributed to five structural mechanisms not reducible to budget constraint.

Keywords: *SMB cybersecurity, baseline controls, essential cyber hygiene, NIST CSF 2.0, CIS Controls IGI, initial access vectors, third-party risk, security investment.*

Problem statement. Small and medium-sized organizations carry a disproportionate share of the cyber-threat burden. The Verizon 2026 Data Breach Investigations Report [1] records 7,152 confirmed breaches at organizations fewer than 1,000 employees and finds that approximately 96 percent of ransomware victims whose organizational size was known fell within that group.

A note on the segment boundary is required. The publisher classifies as small and medium-sized any organization with fewer than 1,000 employees, whereas the present work addresses organizations under 100 employees and in particular under 10. Segment-level figures below are stated with that boundary in view and are not transferred to micro-enterprises without corresponding narrowing.

The set of controls addressing the prevailing compromise scenarios is known, standardized and operable without a dedicated security function. That the resulting gap is systematic rather than incidental — that it follows from organizational characteristics rather than from negligence — has been established empirically [2]. The subject of this work is the mechanism by which the gap is reproduced: why the baseline is not implemented precisely where it is most effective, and what follows from this for implementation methodology.

Baseline controls and coverage of initial access vectors. By baseline is meant the set of organizational and technical controls satisfying two conditions: they address the prevailing initial access vectors, and they do not require staff dedicated to the security function in order to operate.

CIS Controls v8.1 [3] defines Implementation Group 1 as essential cyber hygiene — 56 safeguards out of 153, intended for small and medium-sized organizations with limited IT and security expertise [4]. NIST CSF 2.0 [5] provides the functional frame onto which the composition of IG1 is natively mapped.

On segment-level data from DBIR 2026, the known initial access vectors in organizations of the size under consideration are distributed as follows: exploitation of unremediated vulnerabilities — 26 percent, abuse of stolen credentials — 13 percent, phishing — 9 percent. Together these three account for approximately 48 percent of cases in which the initial vector was known. The baseline addresses all three.

A distinction must be drawn here. That a control addresses a vector is not the same as its preventing every attack along that vector: multi-factor authentication is bypassed by adversary-in-the-middle phishing and session-token theft, and patch discipline does not reach a vulnerability for which no fix has been published. The figure of 48 percent is therefore an upper bound on the addressable share, not the share of incidents prevented. The argument below does not depend on the difference, since it concerns the ordering of controls by efficiency rather than their absolute efficacy.

Victim selection is opportunistic: compromise follows neither industry nor revenue, but the compromise of credentials (38 percent of cases) or unremediated vulnerabilities in perimeter devices (29 percent).

Table 1 — Baseline controls mapped to control frameworks and initial access vectors

Baseline control	NIST CSF 2.0 function	CIS IG1 area	Vector addressed
Multi-factor authentication; password discipline	Protect	Account and access management	Credential abuse (13%)
Patch management; perimeter device control	Identify / Protect	Vulnerability management; asset inventory	Exploitation of vulnerabilities (26%)
Email authentication (SPF/DKIM/DMARC); phishing awareness	Protect	Email and web protections	Phishing (9%)
Backup with tested restoration	Recover	Data recovery	Consequence mitigation
Least privilege; access review	Protect / Govern	Access control	Limits lateral movement

Model 1: concavity of the efficient frontier. Let the available controls be indexed $i = 1..N$, each with implementation effort $c_i > 0$ and risk reduction $r_i \geq 0$, and let efficiency be $e_i = r_i / c_i$. Order the controls by non-increasing efficiency and let C_k and K_k denote cumulative effort and cumulative coverage after the first k of them. The piecewise-linear function $K(C)$ through the points (C_k, K_k) has non-increasing slopes by construction and is therefore concave; the marginal cost $m(C) = 1/e(C)$ is correspondingly non-decreasing.

This is not an empirical finding but a consequence of rational ordering, and it holds for any control set whatever. What is empirical is the magnitude: the dispersion of efficiency across the set determines how steeply marginal cost rises. Estimating effort in hours of owner or administrator time, and coverage in percentage points of addressable initial access vectors, the dispersion between the most and least efficient control spans approximately four

orders of magnitude (Fig. 1). Three controls costing some 36 hours in aggregate address the vectors identified above; monitored round-the-clock operations, costing four orders of magnitude more, address the residual.

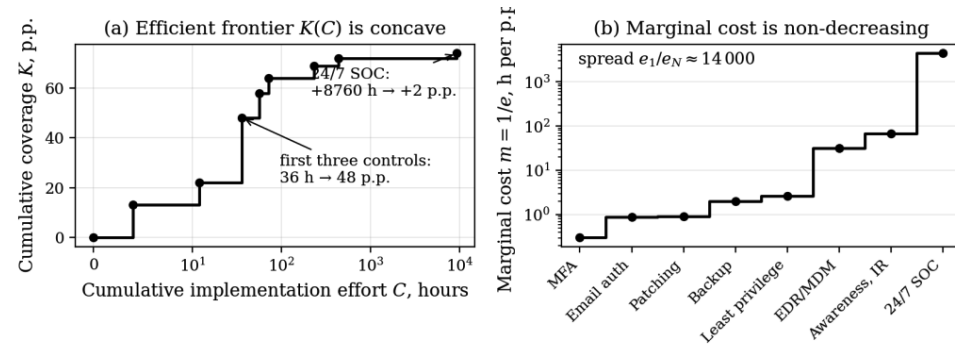


Fig. 1. Efficient frontier of coverage against implementation effort (a) and the corresponding marginal cost (b). Effort estimates are order-of-magnitude; coverage is expressed in percentage points of addressable initial access vectors per DBIR 2026.

Two consequences follow. The commonly cited pattern in which a small fraction of controls yields the greater part of the reduction is not a property of cybersecurity but a necessary feature of any efficiently ordered set, and requires no explanation. Less obviously, the point at which an organization should stop is set not by its budget but by where marginal cost exceeds the capacity available to operate the control — a constraint in hours, not in currency.

Model 2: indivisibility of the interpretation cost. Let the effort of implementing a control framework be $C(n) = F + v \cdot n$, where F is the one-off cost of interpreting the framework, deriving policy from it and documenting the result — a cost that does not depend on organizational size — and v is the recurring per-employee cost of enrolment, training and review. The per-employee burden is then

$$c(n) = C(n)/n = F/n + v,$$

a hyperbola asymptotic to v . The fixed component ceases to dominate at $n^* = F/v$. Taking F as the effort of working through the 56 safeguards of CIS IG1 — interpretation, policy drafting and documentation, of the order of 100 to 400 hours — and v of the order of 2 to 6 hours per employee per year, the crossover falls between 17 and 200 employees, with a central estimate of 67 (Fig. 2). The segment addressed by this work lies entirely below that crossover: at ten employees, some 87 percent of the per-employee burden is the fixed cost of interpretation, and at five employees, 93 percent.

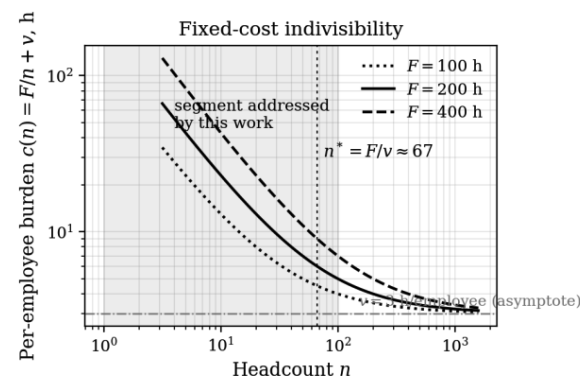


Fig. 2. Per-employee implementation burden as a function of headcount, for three estimates of the fixed interpretation cost F .

The model makes the first mechanism precise. What burdens the small organization is not the price of controls — the most efficient of them are free — but the indivisible cost of determining which controls apply to it and in what form. Reducing the number of required safeguards, as the separation of IG1 does, lowers F but does not alter the shape of the curve; the same holds for condensed guidance addressed directly to the segment [6]. Only a reduction of F to near zero, by supplying the interpretation already performed, moves an organization of ten employees onto the flat part of it.

The paradox of underimplementation and its structural causes. The segment for which the return on the baseline is greatest exhibits the lowest level of its implementation. This observation is not explained by budget constraint: the cost of the first tier is not commensurable with the median cost of an incident in the same segment. Five structural mechanisms are proposed.

1) Indivisibility of the fixed cost of implementation. Formalized above as Model 2. NIST CSF 2.0, ISO/IEC 27001 [7] and CIS Controls in full are designed on the assumption that a dedicated security function exists, and the labour of interpreting them depends only weakly on organizational size. For an organization of under ten employees the resulting per-employee burden reaches magnitudes incommensurable with the scale of its activity.

2) Absence of a receiving function. Methodological guidance presupposes an addressee within the organization. In the segment under fifty employees such a role generally does not exist, and the IT-support function and the security function are identical neither in competence nor in incentive. Per CyberSeek [8], against 514,359 open cybersecurity positions and an employed workforce of 1,337,400, available specialists cover only 74 percent of employer demand; the shortfall is distributed unevenly and falls first on the segment least able to compete for staff. Where the function is absent it is frequently displaced onto the external IT provider, whose incentives differ from the client's [9].

This mechanism admits direct empirical testing. Per DBIR 2026, only 26 percent of vulnerabilities listed in the CISA Known Exploited Vulnerabilities catalog were fully remediated, down from 38 percent the previous year, while the median time to full remediation rose from 32 to 43 days. Applying a patch carries no acquisition cost; the observed deterioration is therefore explained not by budget constraint but by the absence of an executing function. This is independent confirmation that what is scarce is capacity, not funds.

3) Informational asymmetry with respect to own risk. The magnitude of the return on the baseline is not observable from within the organization. Estimating it requires an apparatus the owner of a small enterprise does not possess and incident data to which they do not turn. A high calculated return therefore fails to translate into a management decision — not through irrationality, but through the unavailability of the quantity on which the decision would rest. The finding is consistent with protection motivation research on micro-business owners, in which every construct of the model predicted protective behaviour except perceived susceptibility to the threat [10], and with studies of adoption intention among small-firm managers [11, 12]. Instruments intended to make the estimate accessible have been proposed [13], but their use presupposes the very engagement whose absence is at issue.

4) Discontinuity of the loss function. Loss is not proportional to organizational size. For a large enterprise an incident of the magnitude in question is a line item; for a micro-enterprise it is an event bearing on solvency. Valuation through the ratio of loss avoided to expenditure systematically understates the incentive precisely in the lower segment, since it does not account for the discontinuous character of the consequence.

5) Externalization of the perimeter. Third parties are involved in 55 percent of breaches in the segment, against 48 percent across the full sample. Supplier risk management presupposes a function able to formulate requirements for a counterparty, verify their fulfilment and respond to an incident on the supplier side. Where no such role exists, more than half of the segment's incidents arrive through a perimeter the organization cannot control. This mechanism differs from the preceding four in that no internal implementation removes it: it requires market pressure from customers or regulatory intervention.

A supply-side constraint operates in addition: the economics of serving an organization with a security budget of this order sustains neither an enterprise sales channel nor a project-based consulting model.

Requirements for a methodology scalable by resource. From mechanisms 1 and 2 it follows that the solution lies not in reducing the volume of an enterprise programme but in a methodology designed for the resource constraint from the outset. Its requirements are:

- 1) priority of process-based organizational controls over controls requiring continuous operational capacity;
- 2) a fixed minimum periodic routine in place of project-based implementation;
- 3) expression in the language of business operations rather than in the terms of control frameworks, while retaining traceable correspondence to those frameworks;
- 4) reproducibility without the participation of an external consultant after initial implementation;
- 5) inclusion of a minimal supplier-facing routine executable without a dedicated function — as a partial answer to mechanism 5.

A practical realization of these requirements is the SMB Cybersecurity Framework — a methodology adapting NIST CSF 2.0, ISO/IEC 27001 and CIS Controls for resource-constrained organizations, the baseline mapping of which is given in Table 1 [14–16].

Conclusions.

1. The efficient frontier of coverage against implementation effort is concave by construction, and marginal cost is therefore necessarily non-decreasing; the widely cited concentration of benefit in a small fraction of controls requires no separate explanation. What is empirical is the dispersion of efficiency across the control set, estimated here at approximately four orders of magnitude.

2. Treating the cost of interpreting a control framework as indivisible yields a per-employee burden $c(n) = F/n + v$, hyperbolic in headcount, with the fixed component ceasing to dominate at $n^* = F/v$. For plausible values of F and v that crossover falls between 17 and 200 employees, centrally near 67 — that is, above the entire segment under study. At ten employees some 87 percent of the burden is the fixed cost of interpretation, which no reduction in the price of controls affects.

3. The baseline addresses initial access vectors accounting for approximately 48 percent of known cases in the segment per DBIR 2026, this being an upper bound on the addressable share rather than the share of incidents prevented. Underimplementation is reproduced by five structural mechanisms and does not reduce to budget constraint; in particular, the fall in the share of remediated KEV vulnerabilities, where the remedy has no acquisition cost, indicates a deficit of executing capacity rather than of funds. Reducing the price of existing solutions therefore does not by itself close the gap.

4. The mechanism of perimeter externalization — 55 percent of segment incidents involving third parties — is not removed by internal implementation and requires separate treatment at the level of market or regulatory mechanisms.
5. The direction following from this result is methodologies designed for the resource constraint, with priority given to process-based controls and with traceable correspondence to the operative frameworks.

References

1. Verizon. 2026 Data Breach Investigations Report. Verizon Business, 2026.

2. Heidt M., Gerlach J. P., Buxmann P. Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments // Information Systems Frontiers. 2019. Vol. 21. P. 1285–1305. DOI: 10.1007/s10796-019-09959-1

3. Center for Internet Security. CIS Critical Security Controls, Version 8.1. East Greenbush, NY, 2024.

4. Center for Internet Security. CIS Controls Implementation Groups: IG1 — Essential Cyber Hygiene. URL: cisecurity.org/controls/implementation-groups (accessed 31 July 2026).

5. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD, 2024.

6. NIST. Small Business Information Security: The Fundamentals. NISTIR 7621 Rev. 1. Gaithersburg, MD, 2016.

7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva, 2022.

8. CyberSeek. Cybersecurity Supply/Demand Heat Map, national data. URL: cyberseek.org (accessed 31 July 2026).

9. Cartwright A., Cartwright E., Edun E. S. Cascading information on best practice: cyber security risk management in UK micro and small businesses and the role of IT companies // Computers and Security. 2023. Vol. 131, 103288. DOI: 10.1016/j.cose.2023.103288

10. Whitty M. T., D’Alessandro S. et al. Human-centric cyber security: applying protection motivation theory to analyse micro business owners’ security behaviours // Information and Computer Security. 2025. Vol. 33, No. 1. P. 49–70. DOI: 10.1108/ICS-10-2023-0176

11. Peter M. K., Zobair K. M., Lindeque J. P., Mändli Lerch K., Houghton L. How much more will it need? Determinants of risk-driven cybersecurity adoption in Swiss SMEs: a structural equation modelling approach // Journal of Cybersecurity. 2025. Vol. 11, No. 1, tyaf027. DOI: 10.1093/cybsec/tyaf027

12. Barlette Y., Gundolf K., Jaouen A. CEOs’ information security behavior in SMEs: does ownership matter? // Systèmes d’Information et Management. 2017. Vol. 22, No. 3. P. 7–45.

13. Benz M., Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs // Business Horizons. 2020. Vol. 63, No. 4. P. 531–540.

14. Korchenko A. O., Davydenko K. O., Askerov M. H., Zhurov Yu. S. A method for formalizing a multidimensional reference sub-environment for detecting phishing URLs // Modern Information Security. 2026. No. 2(66). P. 70–87. DOI: 10.31673/2409-7292.2026.021105

15. Zhurov I. Cybersecurity for small and medium-sized businesses: a practical framework for organizations with limited resources // XV International Scientific and Technical Conference “ITSec: Information Technology Security”, Ternopil Ivan Puluj National Technical University, 27–29 May 2026. P. 182–184.

16. Zhurov I. S. SMB Cybersecurity Framework — Practitioner Edition. Version 1.3. SMB Cybersecurity Advisors LLC. Zenodo, 2026. DOI: 10.5281/zenodo.21687186

УДК 004.056:004.7

¹Зубін С.В.

²Прокопович-Ткаченко Д.І.

³Хохлячова Ю.Є.

ПІДВИЩЕННЯ ЖИВУЧОСТІ МЕРЕЖІ В УМОВАХ ДЕФІЦИТУ
ЕЛЕКТРОЕНЕРГІЇ ТА КІБЕРАТАК

¹Державний університет інформаційно-комунікаційних технологій
zysv@ukr.net

²Університет митної справи та фінансів
omega2417@gmail.com

³Державний торговельно-економічний університет
yuliiahohlachova@gmail.com

Анотація. Мета роботи полягає у розробленні методу підвищення рівня живучості мережі в умовах гібридних кібератак під час відключень електроенергії. Модель живучості поєднує енергетичний контур резервування (оцінювання автономності ДБЖ), доступність активного ланцюга та ймовірнісну модель ризику компрометації керуючих площин, включно з *firmware*-атаками, пов’язаними з уразливостями *SNMP* та *SSL/TLS* у вбудованому програмному забезпеченні. Методика моніторингу інтегрує *IDS* і *SIEM* з моделями глибинного навчання: *AE+LSTM* для часових рядів телеметрії та *CNN+LSTM* для аналізу перетворених за *Byte2Image*

дамнів прошивок. За результати проведених досліджень показано, що архітектура *mini OLT GPON* з пасивним оптичним розгалуженням зменшує кількість критичних активних вузлів у ланцюгу доступу, підвищує доступність та спрощує резервування.

Ключові слова: кібербезпека, *SOHO*, *блекаут*, *GPON*, *IDS*, *SIEM*, *Zero Trust*

SOHO-середовище (Small Office / Home Office) охоплює невеликі офіси, приватні будинки, майстерні, малі житлові комплекси, а також змішані об’єкти, де одночасно присутні бізнес-процеси, побутова інфраструктура та охоронні сервіси. Для таких мереж електронних комунікацій історично були типовими прості рішення на базі *Ethernet* та *Wi-Fi*, однак у сучасних умовах експлуатації ключовими стають два взаємопов’язані критерії: живучість під час *блекаутів* і кіберстійкість до гібридних атак.

По-перше, при *блекауті* деградація мережі *SOHO* часто відбувається не через нестачу пропускну здатності, а через каскадну відмову дрібних залежностей: проміжний комутатор без резервного живлення, *PoE*-інжектор поза ДБЖ, точка доступу, що живиться від вузла, який знеструмлено, тощо. Внаслідок цього відмова набуває системного характеру, а не локального. У цьому сенсі *SOHO* є мережею з непропорційно високою чутливістю до структурних слабких ланок, що потребує архітектурних рішень зі зменшенням кількості активних елементів у полі доступу та кращою централізацією контролю.

По-друге, *SOHO* дедалі частіше стає мішенню гібридних кібератак, у яких поєднуються і технічні, і організаційні вектори, такі як слабкі облікові дані, надмірні привілеї, некеровані зміни конфігурацій, відсутність інвентаризації активів, спрощене журналювання та неузгоджені політики доступу. Для структурування таких загроз застосовують підходи моделювання загроз, які поєднують опис активів, векторів атаки й можливих наслідків та створюють основу для обґрунтованого відбору захисних контрольних заходів [1]. Ці заходи мають бути узгоджені з процесами управлінням ризиком, зокрема методиками оцінювання ймовірностей та впливів і формуванням планів оброблення ризику [2], а також із загальноприйнятими вимогами системи управління інформаційною безпекою, де критичними є інвентаризація, політики доступу, керування інцидентами й контроль змін [3].

Особливе місце в гібридних атаках *SOHO* посідають *firmware*-атаки (атаки на прошивки), оскільки вони здатні забезпечувати довготривалу присутність і "переживати" перезавантаження. У практичному контексті критичними є два типові канали компрометації керування. Перший пов’язаний із *SSL/TLS* (Secure Sockets Layer / Transport Layer Security), з яким пов’язано використання застарілих версій, невірна валідація сертифікатів, слабкі криптопараметри або допущення *downgrade*-сценаріїв підвищують ризик перехоплення чи підміни керуючих сесій [4,5]. Другий пов’язаний із *SNMP* (Simple Network Management Protocol), який у *SOHO* часто використовується зі спрощеними політиками доступу та типовими *community*-рядками, що створює умови для несанкціонованої модифікації параметрів пристроїв і опосередкованої компрометації прошивок [5]. Загальні принципи мережної та комп’ютерної безпеки додатково підкреслюють, що в малих середовищах ризики керування й "зручних" конфігурацій часто домінують над ризиками, пов’язаними з пропускну здатністю чи топологічною складністю [6].

У відповідь на таку динаміку загроз модель *Zero Trust* розглядається як базовий принцип побудови доступу й керування [7]. Для *SOHO* це означає потребу в керованому розмежуванні доступів, обов’язковості журналювання подій і можливості кореляції інцидентів у реальному часі, зокрема через використання *IDS* (Intrusion Detection System) та *SIEM* (Security Information and Event Management).

Водночас практика показує, що моніторинг за правилами (лише сигнатури та кореляційні правила) у *SOHO* стикається з двома обмеженнями. Перше – "закритий світ" навчальних і тестових припущень. Машинне навчання в безпеці часто погано переноситься на реальні мережі без належної процедури валідації, контролю дрейфу та оновлення моделей [8]. Друге – висока варіативність трафіку й подій навіть у невеликих середовищах, що потребує комбінації статистичних підходів, ознак та моделей, а також чіткої методології збору й підготовки даних [9]. Додатково, у сучасних мережах з елементами програмно-керованих підходів і централізованого керування ризику площини керування та помилки політик стають настільки ж критичними, як і класичні ризики площини даних [8].

Окремим каталізатором інцидентів у *SOHO* є людський фактор. Теорія людських помилок показує, що більшість "фатальних" збоїв виникає не через одну дію, а через накопичення латентних умов і компромісів у процесах [10]. Паралельно дослідження *usable security* підкреслюють, що надмірна складність політик і засобів безпеки породжує небезпечні обходи. Тобто, слабкою ланкою стає не користувач як такий, а дизайн процесів і інтерфейсів, що підштовхує до неправильних рішень [11]. Тому для *SOHO* важливо поєднати архітектуру доступу з операційно здійсненням режимом керування, діагностики й моніторингу.

У роботі розглядається пасивна оптична архітектура у компактному форматі. Архітектура складається з *mini OLT* (mini Optical Line Terminal) технології *GPON* (Gigabit-capable Passive Optical Network) з одним *PON*-портом і пасивним оптичним сплітером (типово 1:32) до абонентських *ONU/ONT* (Optical Network Unit / Optical Network Terminal). Пасивність сплітера знижує кількість активних елементів у полі доступу та, як наслідок, скорочує кількість вузлів, що потребують резервування живлення під час *блекаутів*. Паралельно централізація керування та телеметрії дозволяє формувати більш узгоджену картину стану доступу й підсилити дисципліну змін конфігурацій відповідно до *Zero Trust* [7].

Для підсилення виявлення гібридних атак і зменшення часу до виявлення інцидентів у роботі обґрунтовується інтегрований підхід *IDS+SIEM* із додаванням моделей машинного навчання двох типів.

Перший тип – моделі виявлення аномалій на телеметрії подій і потоків, зокрема автоенкодеру як засіб навчання компактного представлення "нормальної" поведінки та виявлення відхилень [12], а також гібридні схеми, що комбінують ознаки та класифікатори для зниження хибнопозитивів [13]. Другий тип – глибокі моделі, здатні працювати з високорозмірними даними та складними залежностями, що є типовим для трафіку та послідовностей подій у мережах доступу [14]. Методологічно ці підходи узгоджуються із сучасними уявленнями про оцінювання ризиків і невизначеностей, де необхідно явно враховувати ймовірнісну природу подій і неповноту спостережень [15,17].

Окремо для аналізу артефактів прошивок доцільною є репрезентація Byte2Image, коли байтові послідовності перетворюються у зображення з подальшим застосуванням методів класифікації та виявлення структурних змін. Підхід "malware images" як клас ідей був продемонстрований як працездатний для візуалізації та автоматичної класифікації шкідливих зразків [13], а подальші роботи показали можливість застосування глибокого навчання для таких репрезентацій, зокрема у задачах класифікації та виявлення шкідливого програмного забезпечення [18]. У SOHO-контексті це важливо саме для firmware-атак, де традиційна мережна телеметрія може бути недостатньою, а аналіз структурних змін у прошивках додає незалежну "модальність" сигналів для SIEM.

Референтна архітектура GPON-доступу для SOHO побудована за принципом "mini OLT → пасивний PLC-сплітер 1:32 → 32 абонентські ONU". Схема фіксує повний шлях передачі трафіку від зовнішнього підключення (Інтернет) через гігабітний комутатор до mini OLT, після чого дані транспортуються оптичним каналом і пасивно розгалужуються на абонентські відгалуження. Така побудова є показовою для методичного аналізу, оскільки вона чітко відокремлює активні вузли, що потребують живлення, від пасивного елемента розподілу, який живлення не потребує. Також задаються інженерні точки, які використовуються в подальших розрахунках і порівняннях: де формується "ядро" доступу (гігабітний комутатор і mini OLT), де відбувається пасивне розгалуження (PLC-сплітер), і де розташовані кінцеві термінали (ONU) як точки підключення абонентських сегментів.

Компонентний склад архітектури визначається так, щоб забезпечити коректне моделювання двох взаємопов'язаних контурів: енергетичної живучості під час блекаутів та кіберстійкості до гібридних атак. З методичної точки зору компоненти доцільно розділяти на активні вузли, які потребують живлення для підтримки сервісу (маршрутизатор, комутатори, OLT, ONU, точки доступу за потреби), та пасивні елементи, які живлення не потребують (кабельні лінії, оптичні сплітери, пасивні кроси, роз'ємні з'єднання). Такий поділ є критичним саме для SOHO, оскільки пасивні елементи можуть відмовляти через монтажні помилки, але не створюють додаткового навантаження на ДБЖ-резервування, що принципово змінює інженерну логіку підбору "ядра живучості" та масштабу резервування. У межах дослідження цей поділ використовується як базис для порівняння двох сценаріїв доступу: "Ethernet всюди" та "mini OLT + пасивний сплітер + ONU", де в GPON-варіанті розгалуження оптики не потребує живлення.

Ethernet-сценарій (Ethernet всюди): магістральний маршрутизатор, один або кілька комутаторів доступу, додаткові проміжні комутатори/РоЕ-інжектори залежно від планування приміщень. Активні елементи рознесені просторово.

GPON-сценарій (mini OLT + пасивний сплітер): mini OLT як централізований вузол GPON, пасивний оптичний сплітер, ONU у точках абонентів. Розгалуження оптики не потребує живлення.

Сценарії аналізуються з позицій (і) живучості під час блекауту, (ii) керованості та діагностики, (iii) стійкості до гібридних кібератак. Формально виділяються множини:

V_a – активні вузли: маршрутизатор, комутатори, OLT, ONU, точки доступу (за потреби).

V_p – пасивні елементи: кабельні лінії, оптичні сплітери, пасивні кроси, роз'ємні з'єднання.

Пасивні елементи можуть відмовляти (наприклад, через помилки монтажу), однак не створюють додаткового навантаження на ДБЖ-резервування. Це є принциповою відмінністю GPON-сценарію.

Енергетичний контур резервування та автономність

"Ядро живучості" визначається як набір вузлів, які мають бути гарантовано резервовані для утримання скелета мережі: mini OLT та магістральний маршрутизатор, а за потреби – один ключовий ONU (наприклад, сегмент охорони/VoIP). Оцінка автономності резервування здійснюється формулою:

$$T = \frac{C \cdot U \cdot \eta}{P}, \quad (1)$$

де T – час автономної роботи (год), C – ємність акумулятора (А·год), U – напруга (В), η – коефіцієнт корисної дії, P – сумарна активна потужність навантаження (Вт). Підхід відповідає практиці попереднього підбору ДБЖ та батарейних модулів, після чого виконується уточнення за паспортними характеристиками [4].

Модель доступності активного ланцюга

Кожен активний вузол $i \in V_a$ характеризується середнім часом між відмовами $MTBF_i$ і середнім часом відновлення $MTTR_i$. Доступність вузла:

$$A_i = \frac{MTBF_i}{MTBF_i + MTTR_i}.$$

За припущенням серійної критичності активного ланцюга (відмова будь-якого з критичних вузлів припиняє сервіс доступу) інтегральна доступність:

$$A_{series} = \prod_{i \in V_a} A_i, \quad (2)$$

де $V_a \subseteq V_a$ – підмножина вузлів, без яких сервіс недоступний. Для Ethernet-сценарію $V_a \setminus V$ зазвичай більше через проміжні активні елементи; для GPON-сценарію критичними є mini OLT, магістральний маршрутизатор та, залежно від сервісу, окремі ONU [7].

Ймовірнісна модель гібридного ризику з акцентом на прошивки

Гібридну подію деградації сервісу D трактуємо як комбінацію енергетичної події E (відсутність живлення поза ДБЖ) та кіберподії C (компрометація керуючої площини або прошивки). Ймовірність:

$$P(D) = 1 - (1 - P(E))(1 - P(C \vee E)). \quad (3)$$

Термін $P(C \vee E)$ підкреслює, що під час блекауту часто спостерігаються тимчасові зміни політик, спрощення доступу для відновлення сервісів та деградація моніторингу, що може підвищувати кіберризик [10, 16]. Для SOHO важливо виділити саме firmware-атаки як підклас C , де зловмисник (або шкідливий оновлювальний пакет) модифікує прошивку ONU, маршрутизатора чи допоміжного пристрою. Основними векторами є наступні:

SNMP-вектор: слабкі community-рядки, некоректні ACL до SNMP-агента [2].

SSL/TLS-вектор: застарілі протокольні версії, слабкі набори шифрів, проблеми з валідацією сертифікатів у вебінтерфейсах керування та в механізмах оновлення [19].

Ланцюг оновлень: підміна файлів оновлення, відсутність перевірки підпису, компрометація джерела [12].

Оптимізація резервування та пріоритизація критичних сегментів

Для формалізації вибору, які вузли резервувати в першу чергу, вводиться бінарна змінна $x_i \in \{0,1\}$, що означає підключення вузла i до ДБЖ або локального резервного живлення. Нехай P_i – потужність вузла. Для обмеження за доступною потужністю ДБЖ P_{max} ставиться задача:

$$\max_{\{x_i\}} E[A] \text{ за умов } \sum_{i \in V_a} x_i P_i \leq P_{max}. \quad (4)$$

Інтерпретація у SOHO наступна: у GPON-сценарії базове рішення завжди включає $x_{OLT} = 1$ та $x_R = 1$ (маршрутизатор), далі додаються лише критичні ONU, тоді як у Ethernet-сценарії часто доводиться резервувати одразу кілька проміжних комутаторів, інакше топологія фрагментується.

Інтегрований контур IDS+SIEM з AE+LSTM та CNN+LSTM (Byte2Image)

Для підсилення виявлення гібридних атак застосовується багаторівневий контур, у якому:

IDS фіксує аномалії трафіку, сканування, спроби експлуатації та підозрілі шаблони на мережевому рівні.

SIEM збирає журнали подій (маршрутизатор, mini OLT, ONU, сервери, Wi-Fi контролери), корелює їх правилами та додає аналітичні ознаки.

Моделі машинного навчання оцінюють нетиповість подій для двох класів даних: телеметрії та прошивок.

AE+LSTM (Autoencoder + Long Short-Term Memory) застосовується до часових рядів x_t ознак (наприклад, кількість помилок, NetFlow-агрегати, частота перереєстрацій ONU, коливання Rx/Tx, показники втрат пакетів). Автоенкодер стискає ознаки в латентний простір, а LSTM моделює динаміку латентних представлень для виявлення "повільних" атак і деградацій [5,6].

CNN+LSTM (Convolutional Neural Network + LSTM) застосовується до Byte2Image-репрезентації прошивки: байтовий дамп перетворюється у двовимірну матрицю яскравостей фіксованої ширини (Byte2Image), CNN витягує структурні ознаки, LSTM відстежує послідовність оновлень (версії/час) [5,15]. Для одночасного навчання/оцінювання вводиться комбінована функція втрат:

$$L = \lambda_1 \cdot L_{cls}(y, \hat{y}) + \lambda_2 \cdot \|x - \hat{x}\|_2^2, \quad (5)$$

де L_{cls} – класифікаційна втрата (наприклад, крос-ентропія) для CNN+LSTM, $\|x - \hat{x}\|_2^2$ – похибка реконструкції автоенкодера для AE+LSTM, λ_1, λ_2 – ваги. Вихідні оцінки (anomaly score, firmware drift score) передаються в SIEM як збагачені поля подій, після чого виконуються кореляційні правила та сценарні перевірки за ATT&CK [11].

Висновки. У роботі розроблено та апробовано метод підвищення рівня живучості мережі в умовах гібридних кібератак під час відключень електроенергії. Показано, що архітектура mini OLT GPON з пасивним оптичним розгалуженням до 32 абонентських терміналів ONU зменшує кількість критичних активних вузлів у ланцюгу доступу, підвищує доступність та спрощує резервування.

Література

1. National Institute of Standards and Technology (NIST). The NIST cybersecurity framework (CSF) 2.0. NIST CSWP 29. Gaithersburg (MD): NIST. 2024. <https://doi.org/10.6028/NIST.CSWP.29>.
2. US-CERT (CISA). SNMP vulnerabilities in networked devices: common misconfigurations and exploitation patterns. 2019. Alert/Note.

3. Harrington D., Presuhn R., Wijnen B. An architecture for describing SNMP management frameworks // *RFC 3411: Internet Standard*. December 2002. <https://doi.org/10.17487/RFC3411>.

4. Malhotra P., Ramakrishnan A., Anand G., Vig L., Agarwal P., et al. LSTM-based encoder–decoder for multi-sensor anomaly detection // *ICML 2016 Anomaly Detection Workshop*. 2016. <https://doi.org/10.48550/arXiv.1607.00148>.

5. Ring M., Wunderlich S., Scheuring D., Landes D., Hotho A. A survey of network-based intrusion detection datasets // *Computers & Security*. 2019. Vol. 86. P. 147–167. <https://doi.org/10.1016/j.cose.2019.06.005>.

6. IEEE Standards Association. IEEE Standard for Ethernet: IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018). New York: IEEE, 2022. <https://doi.org/10.1109/IEEESTD.2022.9844436>.

7. Trivedi K. S. Probability and statistics with reliability, queuing and computer science applications. 2-nd ed. Hoboken (NJ): John Wiley & Sons, 2016. <https://doi.org/10.1002/9781119285441>.

8. Möller S., Thomson M. RFC 8996: Deprecating TLS 1.0 and TLS 1.1. IETF, 2021. <https://doi.org/10.17487/RFC8996>.

9. Case B., Harrington D. RFC 3411: An architecture for describing SNMP management frameworks. IETF, 2002. <https://doi.org/10.17487/RFC3411>.

10. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg, MD: National Institute of Standards and Technology, 2024. <https://doi.org/10.6028/NIST.CSWP.29>.

11. MITRE ATT&CK® Team. Enterprise Matrix and Techniques: Updates – April 2023 (version 13). MITRE Corporation, 2023. Доступ 11 серпня 2026 р.: attack.mitre.org/resources/updates/updates-april-2023/.

12. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture (NIST Special Publication 800-207). Gaithersburg, MD: National Institute of Standards and Technology, 2020. <https://doi.org/10.6028/NIST.SP.800-207>.

13. Moriarty K., Farrell S. Deprecating TLS 1.0 and TLS 1.1 // *RFC 8996: Best Current Practice*. March 2021. <https://doi.org/10.17487/RFC8996>.

14. Durumeric Z., Ma Z., Springall D. The security impact of HTTPS interception // *Proceedings of the 2017 Network and Distributed System Security Symposium (NDSS 2017)*. 2017. San Diego, CA. <https://doi.org/10.14722/ndss.2017.23456>.

15. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. S. Malware images: visualization and automatic classification // *Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec 2011)*. 2011. Pittsburgh, USA. P. 1–7. <https://doi.org/10.1145/2016904.2016908>.

16. NIST. Zero Trust Architecture: NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology, 2020. P. 59. <https://doi.org/10.6028/NIST.SP.800-207>.

17. US-CERT (CISA). SNMP vulnerabilities in networked devices: common misconfigurations and exploitation patterns. Alert/Note. 2019.

18. Malhotra P., Ramakrishnan A., Anand G., Vig L., Agarwal P., Shroff G. LSTM-based encoder–decoder for multi-sensor anomaly detection // *arXiv*. 2016. <https://doi.org/10.48550/arXiv.1607.00148>.

19. Harrington D., Presuhn R., Wijnen B. An architecture for describing SNMP management frameworks // *RFC 3411: Internet Standard*. December 2002. <https://doi.org/10.17487/RFC3411>.

передбачуваності сигнальних конструкцій, зниження взаємної кореляції та підвищення їх структурної прихованості порівняно з традиційними позиційними сигналами.

Ключові слова: таймерні сигнальні конструкції, шумоподібний сигнал, кореляційний аналіз, пряме розширення спектра, послідовності Уолша, прихованість сигналів, захищений зв'язок.

Одним із пріоритетних напрямів розвитку сучасних систем захищеного зв'язку є забезпечення високого рівня прихованості передавання інформації в умовах впливу засобів радіоелектронної боротьби [1]. Класичні методи розширення спектра [2, 3], зокрема пряме розширення спектра псевдовипадковими послідовностями (DSSS) та псевдовипадковий перескок робочої частоти (FHSS), ефективно знижують спектральну густину енергії сигналу. Водночас сучасні засоби радіотехнічної розвідки здатні здійснювати кореляційний і спектральний аналіз широкосмугових сигналів, що обмежує ефективність класичних підходів. Перспективним напрямом підвищення прихованості є використання таймерних сигнальних конструкцій (ТСК), які дозволяють формувати додаткову часову невизначеність шляхом зміни тривалостей імпульсів та їх взаємного розташування [4]. Поєднання ТСК із методом прямого розширення спектра створює шумоподібні сигнали зі складнішою структурою, що суттєво ускладнює їх виявлення засобами радіоелектронної розвідки.

Широкосмуговий сигнал, сформований методом прямого розширення спектра ТСК, можна подати як розклад у базисі ортогональних функцій

$$s(t) = \sum_{i=1}^N a_i \varphi_i(t), \tag{1}$$

де a_i – вагові коефіцієнти випадкових або псевдовипадкових послідовностей; $\varphi_i(t)$ – ортогональні або квазіортогональні базисні функції; N – розмірність простору сигналу.

На відміну від позиційних сигналів, структура яких після розширення спектра залишається відносно передбачуваною, часові параметри ТСК створюють додатковий рівень структурної невизначеності. Це знижує ефективність кореляційного аналізу та статистичного спектрального моніторингу.

Для оцінювання впливу часової структури ТСК було розглянуто три різні сигнальні конструкції, сформовані на однаковому часовому інтервалі $T_c = mt_0$, але з різними параметрами побудови:

- 1) ТСК-1: $t_{c1} = 4\Delta, t_{c2} = 7\Delta, t_{c3} = 5\Delta$;
- 2) ТСК-2: $t_{c1} = 5\Delta, t_{c2} = 5\Delta, t_{c3} = 6\Delta$;
- 3) ТСК-3: $t_{c1} = 6\Delta, t_{c2} = 4\Delta, t_{c3} = 6\Delta$.

Розширення спектра здійснювалося за допомогою послідовностей Уолша з базою $B_{t_0} = 16$. Кількість імпульсів ПВП, що використовуються для розширення спектра комбінації ТСК, визначається як:

$$N_{\tau\text{ТСК}} = B_{t_0} \times m, \tag{2}$$

де m – кількість елементарних інтервалів у межах T_c . Як критерій оцінювання використано коефіцієнт взаємної кореляції між різними реалізаціями широкосмугових сигналів. В табл. 1 за допомогою коефіцієнту кореляції K_{cy} надана оцінка впливу ТСК на структуру широкосмугового сигналу.

Таблиця 1

Оцінка впливу ТСК на структуру широкосмугового сигналу за допомогою коефіцієнту кореляції K_{cy}						
N	K_{cy}					
	C_{17}	C_{37}	C_{47}	C_{07}	C_{55}	C_{62}
ТСК-1	0,125	0,135	0,126	0,125	0,135	0,126
ТСК-2	0,375	0,387	0,387	0,375	0,387	-0,250
ТСК-3	0,500	0,516	0,516	0,500	0,516	0,516

Отримані результати свідчать, що навіть при використанні однакової послідовності Уолша, наприклад C_{62} , зміна часової структури ТСК суттєво впливає на взаємну кореляцію сигналів. Для ТСК-1 коефіцієнт кореляції становить близько 0,126, для ТСК-2 спостерігається зниження до -0,250, тоді як для ТСК-3 він досягає 0,516. Це підтверджує, що часові параметри ТСК формують ансамбль шумоподібних сигналів зі змінною структурою.

Особливістю запропонованого методу формування шумоподібних сигналів є те, що зсуви тривалостей імпульсів ТСК змінюють часову структуру послідовності Уолша після розширення спектра. У результаті навіть за умови знання базового коду потенційний противник отримує додаткову невизначеність щодо фактичної структури передаваного сигналу. Це суттєво ускладнює визначення тривалості імпульсів, їхнього взаємного розташування та відновлення сигнальної конструкції засобами радіотехнічної розвідки.

Відновлення структури імпульсів ТСК здійснюється після демодуляції широкосмугового сигналу за допомогою кореляційного приймача. На виході інтегратора формується залежність напруги, екстремуми якої відповідають моментам зміни структури сигналу (рис. 1).

УДК 004.056.5:368

Гавель С.М.,
Степанов В.О.,
Корчинський В.В.,
Богданюк І.А.,
Мар'ян М.О.,
Славич В.О.

АНАЛІЗ КОРЕЛЯЦІЙНИХ ВЛАСТИВОСТЕЙ ШУМОПОДІБНИХ ТАЙМЕРНИХ СИГНАЛІВ

Державний університет інтелектуальних технологій і зв'язку
arkominer@gmail.com, stepanovvadym333@gmail.com, vladkorchin@ukr.net, igor.bogdanuke@gmail.com,
maryannickikay61@gmail.com, kanra512@gmail.com

Анотація. Для забезпечення захищеного зв'язку в умовах активного радіоелектронного протиборства необхідним є підвищення структурної та енергетичної прихованості передаваних сигналів, що ускладнює їх виявлення, перехоплення та аналіз засобами радіотехнічної розвідки. Одним із перспективних напрямів розв'язання цього завдання є використання шумоподібних таймерних сигналів, сформованих методом прямого розширення спектра таймерних сигнальних конструкцій із застосуванням псевдовипадкових послідовностей Уолша. У роботі досліджено кореляційні властивості таких сигналів та проаналізовано вплив параметрів побудови таймерних сигнальних конструкцій на значення взаємної кореляції між різними реалізаціями широкосмугових сигналів. Показано, що зміна часової структури імпульсів призводить до зменшення

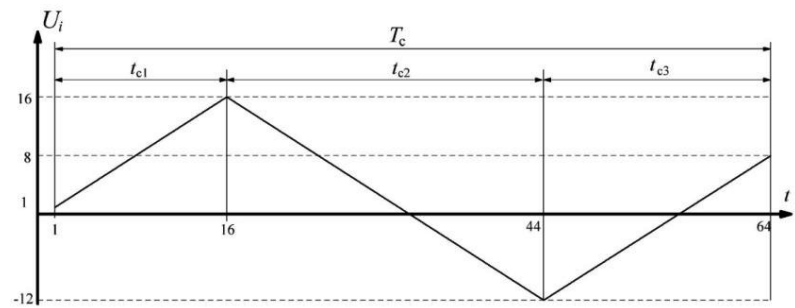


Рис. 1. Рівень напруги U_i на виході інтегратора кореляційного приймача для визначення тривалостей t_{c1} , t_{c2} , t_{c3} комбінації ТСК-1

На відміну від класичних систем прямого розширення спектра, де аналіз виконується для імпульсів фіксованої тривалості t_0 , запропонований метод враховує непозиційну структуру всієї сигнальної конструкції T_c . Це забезпечує коректне визначення передніх і задніх фронтів імпульсів навіть після широкосмугового перетворення сигналу. Проведений аналіз підтверджує доцільність використання адаптивного підходу до вибору параметрів ТСК залежно від характеристик каналу зв'язку, рівня завад та вимог до прихованості передавання інформації. Застосування різних множин сигнальних конструкцій у різних сеансах зв'язку дозволяє додатково підвищити стійкість системи до засобів радіоелектронної розвідки.

Висновки. Проведений аналіз показав, що використання таймерних сигнальних конструкцій у поєднанні з методом прямого розширення спектра суттєво впливає на кореляційні властивості широкосмугових сигналів. Зниження взаємної кореляції між різними реалізаціями ТСК підвищує структурну прихованість сигналів і ускладнює їх виявлення засобами радіотехнічної розвідки. Запропонований метод кореляційного прийому забезпечує відновлення часової структури непозиційних сигналів та створює передумови для розроблення адаптивних методів захисту інформації в умовах радіоелектронного протидію.

Література

1. Зайцев Д. В., Яфонкін А. О., Ярема В. В. Основи зв'язку та радіоелектронна боротьба як вид бойового забезпечення : навчальний посібник : *Університет державної фіскальної служби України*. Ірпінь, 2021. 280 с.
2. Крижний А. В., Гурський Т. Г., Климович С. О. Аналіз характеристик систем радіозв'язку з використанням кодового розділення каналів. *Збірник наукових праць Національної академії державної прикордонної служби України. Серія: військові та технічні науки*. 2014. № 1(61). С. 342–356.
3. Сталий розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б.В. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. Одеса : ДУ «ІРЕД НАНУ», 2024. С. 543.
4. Korchynskyi, V. V., Kildishev, V. Y., Al-Faiyumi, K., Smazhenko, K. A., Valihurskyi, Y. P., & Polishchuk, K. V. (2021). *Method of forming parameters for chaos generators based on hash functions. Proceedings of O. S. Popov ONAT*, (2), 65–69. <https://doi.org/10.33243/2518-7139-2020-1-2>

УДК 004.056.53:004.75

Сіренко О. І.

ОСОБЛИВОСТІ ВИЯВЛЕННЯ АТАК У КОНТЕЙНЕРИЗОВАНИХ СЕРЕДОВИЩАХ

Державний університет інтелектуальних технологій і зв'язку
olexandr.sirenko@gmail.com

Анотація. Розглянуто особливості виявлення атак у контейнеризованих середовищах як окремого класу задач кібербезпеки. Показано, що специфічні характеристики контейнерів - спільне ядро операційної системи, короткий життєвий цикл екземплярів та динамічна оркестрація - суттєво ускладнюють застосування традиційних систем виявлення вторгнень на основі хоста. Виконано порівняльний аналіз правил (rule-based), поведінкових (anomaly-based, ML-based) та гібридних підходів до виявлення аномалій на рівні системних викликів (syscalls) з використанням технології eBPF, а також промислових інструментів runtime-безпеки. Визначено ключові невирішені проблеми: відсутність стандартизованих наборів даних для контейнерних атак, нестабільність поведінкового базового профілю при частому перерозгортанні контейнерів та розрив між метриками, досягнутими в лабораторних умовах, та реальною ефективністю у виробничих середовищах. Визначено перспективи гібридних методів, що поєднують правила виявлення (Falco) з поведінковими та replica-based моделями машинного навчання, як засіб підвищення повноти виявлення атак з прийнятним рівнем хибнопозитивних результатів.

Ключові слова: контейнеризація, Kubernetes, виявлення вторгнень, eBPF, системні виклики, машинне навчання, аномалії.

Швидке поширення контейнерних технологій та платформ оркестрації, зокрема Kubernetes, призвело до появи нового класу проблем кібербезпеки, пов'язаних з виявленням атак у контейнеризованих середовищах. На відміну від традиційних серверних та віртуалізованих інфраструктур, контейнери характеризуються спільним використанням ядра операційної системи, коротким життєвим циклом окремих екземплярів та високим ступенем динаміки масштабування, що суттєво ускладнює формування стабільного профілю нормальної поведінки системи. Класичні підходи до виявлення вторгнень, розроблені для статичних середовищ на основі хостів, демонструють обмежену ефективність у контексті контейнерів, що обґрунтовує актуальність дослідження конкретних методів та інструментів для виявлення атак у цьому класі систем.

Ключовою відмінною рисою контейнеризованого середовища як об'єкта моніторингу є спільне використання ядра операційної системи всіма контейнерами на вузлі, що робить рівень системних викликів (syscall) одним із ключових джерел низькорівневої телеметрії під час виконання, що дозволяє спостерігати за поведінкою процесів усередині контейнерів незалежно від їх короткого життєвого циклу; водночас, повна картина безпеки контейнеризованого середовища вимагає співвіднесення цієї телеметрії з подіями Kubernetes API, журналами аудиту, мережевою та файловою активністю. Ефемерність контейнерів - короткий час життя окремого екземпляра при частому повторному розгортанні - ускладнює накопичення достатньої кількості даних для побудови стабільного базового профілю поведінки. Динаміка оркестрації (автоматичне масштабування, міграція подів, роллінгові оновлення) додатково створює семантичний розрив між подією на рівні ядра та її інтерпретацією на рівні логічної сутності - контейнера, поду або мікросервісу. Окремою проблемою є природна подібність поведінки серед реплік одного й того ж мікросервісу: оскільки репліки виконують аналогічні завдання, відхилення в поведінці однієї репліки відносно інших може служити індикатором компрометації без необхідності попереднього навчання моделі на великих обсягах даних [1].

Атаки на контейнеризовані середовища можна обґрунтовано класифікувати за трьома векторами: атаки на рівні додатків (експлуатація вразливостей у веб-додатках та сервісах, що працюють усередині контейнера), атаки на рівні інфраструктури контейнерів (вихід за межі контейнера, ескаляція привілеїв через вразливості ядра або надмірні можливості) та атаки на рівні оркестрації Kubernetes (небезпечна конфігурація робочого навантаження, надмірні дозволи доступу, відсутність сегментації мережі та витік секретних даних). Окремої згадки заслуговують загрози ланцюга постачання, зокрема компрометація образів контейнерів у публічних реєстрах, таких як Docker Hub, на етапі збірки: ці загрози формуються до запуску контейнера та вимагають різних контрзаходів (сканування образів, підписання, контроль походження (provenance)), проте їхні наслідки можуть проявлятися в поведінці під час виконання та виявлятися інструментами моніторингу під час виконання, що є предметом цієї роботи. Кожен із трьох векторів середовища виконання вимагає власного набору джерел телеметрії: тоді як атаки на рівні програм та контейнерів переважно спостерігаються на рівні системних викликів та файлової системи, атаки на рівні оркестрації вимагають аналізу подій Kubernetes API та журналів аудиту, що виходить за рамки класичного моніторингу на основі хоста. Емпіричні дослідження наборів даних LID-DS та Container Breakout Dataset (CB-DS) показують, що лід-тайм виявлення (час від першого виявленого прояву атаки до її завершення) критичних атак, особливо тих, що пов'язані з ескалацією привілеїв, суттєво варіюється залежно від сценарію атаки, що накладає високі вимоги до швидкості реагування детекторів [2].

Академічні підходи до виявлення атак на рівні системних викликів умовно поділяються на графові, частотні та автоенкодерні методи. Графові методи моделюють послідовність системних викликів як зв'язаний орієнтований граф, що дозволяє враховувати контекстні залежності між викликами та їхніми аргументами; цей підхід використовується в рішенні CHIDS, яке додатково розрізняє раніше не бачені виклики та їхні аргументи як окремі вузли графа [2], а також у методі, заснованому на ансамблі випадкових та ізоляційних лісів, який використовує анонімні випадкові блукання для компактного представлення графів поведінки контейнерів [4]. Частотні методи, зокрема Ab-HIDS, використовують частоту N-грам системних викликів як ознаки для ансамблевих класифікаторів (на основі голосування та XGBoost), що забезпечує підвищення точності порівняно з окремими моделями [3]. Окремий та концептуально важливий клас утворюють методи без навчання, які взагалі не потребують попереднього навчання. Замість традиційного темпорального baseline (профілю нормальної поведінки, накопиченого з часом), рішення ReplicaWatcher спирається на просторовий принцип: репліки одного й того ж мікросервісу виконують аналогічні завдання та зазвичай демонструють подібну поведінку, тому відхилення в поведінці однієї репліки відносно інших може служити індикатором компрометації без побудови довготривалого baseline. Цей підхід досягає точності 91,08% та повноти 98,35% і, на відміну від класичних моделей машинного навчання, залишається стійким до змін у профілі нормальної поведінки - саме тієї нестабільності baseline, яка виникає внаслідок динамічного перерозподілу та масштабування контейнерів [1]. Це робить методи на основі реплік природним доповненням до підходів на основі правил та класичних підходів на основі аномалій у динамічних середовищах Kubernetes. Гібридні рішення eBPF поєднують рівень хоста (послідовності системних викликів) та рівень мережі (метадані потоку) у межах однієї моделі класифікації. За результатами одного такого дослідження, виявлення на основі системних викликів досягає точності 98,39%, тоді як виявлення на основі мережевого трафіку досягає 87,49%, що у межах експерименту, проведеного авторами, демонструє вищу інформативність телеметрії на рівні хоста для класифікації досліджуваних контейнерних атак [5].

Промислові рішення середовища виконання, такі як Falco, Tracex та Tetragon, використовують телеметрію подій ядра eBPF у поєднанні з механізмами правил та політик для виявлення визначених класів небезпечної поведінки, але вони не ідентичні один одному за архітектурою та призначенням. Найбільш чітким підходом, заснованим на правилах, серед них є Falco: інструмент зіставляє події ядра, збагачені метаданими контейнера та Kubernetes, з набором декларативних правил у режимі реального часу; створений та відкритий Sysdig, а пізніше переданий CNCF, він у 2024 році отримав статус Graduated-проєкту CNCF [8], що підтверджує зрілість технології для виробничого використання, та підтримує розширення за допомогою системи плагінів. Перевагами підходу на основі правил є низька затримка виявлення та інтерпретованість рішень; недоліками є обмежена здатність виявляти раніше невідомі (нові) атаки та необхідність постійного оновлення бази правил. На відміну від інструментів на основі правил, методи на основі поведінкових аномалій можуть виявляти відхилення без апріорних визначень правил, але вони стикаються з проблемами високого рівня хибнопозитивних результатів та «холодного старту» за нестабільного baseline. Гібридні підходи, що поєднують правила швидкого реагування з класифікаторами машинного навчання для глибшого аналізу аномальної поведінки, вважаються компромісом між повнотою виявлення та обчислювальними витратами.

Серед невирішених проблем виявлення атак у контейнеризованих середовищах визначено наступні. По-перше, відсутність стандартизованих та репрезентативних наборів даних, які відтворюють реалістичні сценарії атак у кластерах Kubernetes: розроблена методологія бенчмаркінгу та ін'єкцій атак для мікросервісних додатків демонструє, що без єдиного підходу до генерації наборів даних коректне порівняння різних рішень IDS стає суттєво складнішим [6]. По-друге, нестабільність базового поведінкового профілю через часте перерозгортання та масштабування контейнерів, що знижує ефективність статичних моделей виявлення аномалій. По-третє, розрив між метриками ефективності, отриманими в лабораторних умовах, та реальною продуктивністю рішень у виробничих середовищах, де характер робочих навантажень та атак суттєво відрізняється від тестових сценаріїв. Перспективним напрямом є розроблення гібридних методів виявлення на основі телеметрії eBPF у поєднанні з класифікаторами машинного навчання, а також емпірична перевірка підходів на сценаріях, що відповідають списку ризиків OWASP Kubernetes Top 10, видання 2025 року (зокрема, небезпечна конфігурація робочого навантаження, надмірні дозволи авторизації та недостатнє логування і моніторинг) [7]. Особливу увагу слід приділити методологічній коректності оцінки запропонованих рішень: порівняння різних систем виявлення вторгнень (IDS) за єдиним протоколом ін'єкції атак та узгодженим набором метрик (точність, повнота, лід-тайм виявлення, накладні витрати на продуктивність) допомагає уникнути ситуацій, коли заявлена висока ефективність методу пояснюється особливостями конкретного тестового стенду, а не фактичною якістю детектора [6]. Це особливо актуально при порівнянні підходів без навчання, які не потребують фази навчання та є стійкими до зміщення baseline, з класичними моделями машинного навчання, які демонструють вищу точність на статичних тестових наборах, але менш стійкі до дрейфу нормальної поведінки в динамічних кластерах Kubernetes.

Висновки. Виявлення атак у контейнеризованих середовищах є самостійним класом задач кібербезпеки, що вимагає врахування специфіки спільного ядра, ефемерності контейнерів та динаміки оркестрації. Проведений аналіз показав, що жоден з розглянутих підходів - на основі правил, на основі аномалій (на основі графів, частоти, автоенкодерні моделі) або на основі реплік без навчання - повністю не вирішує проблему: рішення на основі правил (Falco, Tracex, Tetragon) забезпечують низьку затримку та інтерпретованість, але обмежені у виявленні нових атак, тоді як поведінкові моделі машинного навчання здатні виявляти відхилення, не описані заздалегідь визначеними правилами, хоча їхня ефективність суттєво залежить від якості навчальних даних та стабільності базового профілю. Ключова суперечність полягає в тому, що динаміка оркестрації Kubernetes ускладнює формування та підтримку стабільного темпорального baseline, на якому базується більшість підходів машинного навчання; просторовий (spatial) baseline, заснований на порівнянні поведінки реплік одного й того ж мікросервісу одна з одною, як це реалізовано в підході ReplicaWatcher без навчання, може служити альтернативою. Це формує логічну основу для подальших досліджень: поєднання методів швидкого реагування на основі правил з моделями машинного навчання та реплік для аналізу аномальної поведінки у межах єдиної гібридної архітектури. На основі проведеного аналізу гібридні методи виявлення на основі eBPF-телеметрії системних викликів визначено як перспективний напрям подальших досліджень. Такі методи потребують емпіричної верифікації на реалістичних сценаріях атак, що відповідають переліку ризиків OWASP Kubernetes Top 10 (редакція 2025 р.).

Література

1. El Khairi A., Caselli M., Peter A., Continella A. REPLICAWATCHER: Training-less Anomaly Detection in Containerized Microservices // Proceedings of the Network and Distributed System Security Symposium (NDSS 2024). San Diego, CA, USA, 2024. DOI: 10.14722/ndss.2024.24286.
2. El Khairi A., Caselli M., Knierim C., Peter A., Continella A. Contextualizing System Calls in Containers for Anomaly-Based Intrusion Detection // Proceedings of the 2022 Cloud Computing Security Workshop (CCSW'22). Los Angeles, CA, USA, 2022. P. 9-21. DOI: 10.1145/3560810.3564266.
3. Joraviya N., Gohil B. N., Rao U. P. Ab-HIDS: An anomaly-based host intrusion detection system using frequency of N-gram system call features and ensemble learning for containerized environment // Concurrency and Computation: Practice and Experience. 2024. Vol. 36, Issue 23. Art. e8249. DOI: 10.1002/cpe.8249.

4. Iacovazzi A., Raza S. Ensemble of Random and Isolation Forests for Graph-Based Intrusion Detection in Containers // 2022 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2022. P. 30-37. DOI: 10.1109/CSR54599.2022.9850307.
5. Ryu J., Kim R., Lee S., Kim S., Choi H., Kim S. Hybrid Runtime Detection of Malicious Containers Using eBPF // Computers, Materials & Continua. 2026. Vol. 86, No. 3. DOI: 10.32604/cmc.2025.074871.
6. Flora J., Antunes N. Evaluating intrusion detection for microservice applications: Benchmark, dataset, and case studies // Journal of Systems and Software. 2024. Vol. 216. Art. 112142. DOI: 10.1016/j.jss.2024.112142.
7. OWASP Kubernetes Top 10 (2025 edition) [Electronic resource] / OWASP Foundation. URL: <https://owasp.org/www-project-kubernetes-top-ten/> (accessed: 14.08.2026).
8. Falco: Cloud Native Runtime Security [Electronic resource] / The Cloud Native Computing Foundation. URL: <https://falco.org/> (accessed: 14.08.2026).

УДК 004.056.5:368

¹Бектурсунов Д.Н.,
²Копитін Ю.В.,
²Копитіна М.В.,
³Корчинський В.В.,
³Мартінова О.М.,
³Дунаєва В.В.

МОДЕЛЬ ПРОЦЕСУ КІБЕРСТРАХУВАННЯ ДЛЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

¹АТ Казахтелеком

dbektursun@gmail.com

²Академія електронного управління

y.v.kopytin@gmail.com, myr19@i.ua

³Державний університет інтелектуальних технологій і зв'язку

vladkorchin@ukr.net, elena_martynova@ukr.net, lvlada.dunaeva@gmail.com

Анотація. Розглянуто модель процесу кіберстрахування як інструменту управління ризиками інформаційної безпеки підприємства. Визначено основні етапи взаємодії підприємства зі страховою компанією, що охоплюють надання інформації про інформаційну інфраструктуру, оцінювання кіберризиків, визначення страхового покриття, укладання договору, сплату страхових внесків, здійснення страхового відшкодування та використання отриманих коштів для відновлення інформаційної системи. Запропоновано математичне представлення основних етапів процесу кіберстрахування, що дає змогу формалізувати параметри інформаційної безпеки, очікувані збитки, страхову премію, страхове покриття та страхове відшкодування. Визначено основні складові витрат підприємства, які можуть компенсуватися внаслідок реалізації кіберінциденту.

Ключові слова: кіберстрахування, інформаційна безпека, кіберризик, кібербезпека, страхове покриття, страхова премія, кіберінцидент, страхове відшкодування

Цифровізація діяльності підприємств та зростання залежності від інформаційних систем супроводжуються збільшенням кількості кіберінцидентів, пов'язаних із несанкціонованим доступом, витоком інформації, шкідливим програмним забезпеченням, порушенням доступності інформаційних ресурсів та іншими кіберзагрозами [1, 2]. Реалізація таких загроз може призводити не лише до порушення функціонування інформаційних систем, але й до значних фінансових, юридичних та репутаційних втрат [3]. У таких умовах забезпечення інформаційної безпеки потребує комплексного управління кіберризиками, яке має передбачати не лише застосування технічних та організаційних засобів захисту, а й використання економічних механізмів компенсації можливих збитків. Одним із таких механізмів є кіберстрахування [4, 5], що дає змогу підприємству передати страховій компанії частину фінансових ризиків, пов'язаних із реалізацією кіберзагроз. Водночас ефективність кіберстрахування [6] залежить від достовірності інформації про стан інформаційної інфраструктури підприємства, обґрунтованості оцінювання кіберризиків, правильності визначення страхового покриття та чіткого встановлення умов договору.

Метою дослідження є розроблення моделі процесу кіберстрахування для управління ризиками інформаційної безпеки підприємства та формалізація основних етапів взаємодії між підприємством і страховою компанією.

Для досягнення поставленої мети необхідно вирішити такі завдання: визначити сутність кіберстрахування; встановити основні етапи процесу кіберстрахування; формалізувати інформацію про інформаційну інфраструктуру та рівень захищеності підприємства; визначити порядок оцінювання кіберризиків та очікуваного збитку; формалізувати процес визначення страхової премії, страхового покриття та умов

договору; визначити порядок розрахунку страхового відшкодування та основні напрями використання отриманих коштів.

Кіберстрахування є формою організаційних, правових та економічних відносин між підприємством і страховою компанією, яка бере на себе частину фінансових ризиків, пов'язаних із реалізацією кіберзагроз, в обмін на сплату страхових внесків. Модель процесу кіберстрахування передбачає послідовне виконання взаємопов'язаних етапів, на кожному з яких визначаються відповідні інформаційні, економічні та організаційні складові.

1. Надання підприємством інформації страховій компанії

Першим етапом процесу кіберстрахування є встановлення відносин зі страховою компанією. Підприємство надає інформацію про свою інформаційну інфраструктуру, рівень захищеності інформаційних ресурсів, наявні засоби кіберзахисту та статистику кіберінцидентів за визначений період. Надану підприємством інформацію можна представити у вигляді множини:

$$I = \{A, S, T, H\}, \tag{1}$$

де A – інформаційні активи підприємства; S – рівень захищеності інформації; T – технічні засоби захисту інформації; H – статистика кіберінцидентів за попередній період. Отримана інформація використовується страховою компанією для оцінювання рівня кіберризиків та визначення основних умов майбутнього страхування.

2. Оцінювання кіберризиків

На другому етапі страхова компанія на основі отриманих даних проводить оцінювання кіберризиків та визначає його інтегральний рівень:

$$R = f(P, C) \tag{2}$$

де R – рівень кіберризиків; P – імовірність виникнення кіберінциденту; C – розмір можливих фінансових збитків.

На основі значень P та C визначається очікуваний збиток:

$$L = P \times C. \tag{3}$$

Розмір очікуваного збитку є одним із основних параметрів для визначення розміру страхової премії:

$$Pr = k \times L, \tag{4}$$

де Pr – страхова премія, EUR; k – страховий коефіцієнт; L – очікуваний збиток, EUR.

Отже, на другому етапі встановлюється взаємозв'язок між імовірністю виникнення кіберінциденту, можливими фінансовими збитками та розміром страхової премії.

3. Визначення страхового покриття

На третьому етапі, з урахуванням результатів оцінювання кіберризиків, страхова компанія визначає основні параметри страхового покриття, зокрема максимальний розмір фінансової відповідальності, величину франшизи, перелік страхових випадків та умови здійснення страхового відшкодування. Основні параметри страхового покриття можна представити у вигляді множини:

$$Ic = \{L_c, F, D\}, \tag{5}$$

де L_c – ліміт страхового покриття; F – франшиза, EUR; D – перелік страхових випадків.

Ліміт страхового покриття визначає максимальну суму збитків, яку страхова компанія зобов'язується компенсувати відповідно до умов договору. Франшиза визначає частину збитків, яка не компенсується страховою компанією та залишається відповідальністю підприємства. Перелік страхових випадків визначає види кіберінцидентів, за настання яких підприємство має право на отримання страхового відшкодування.

4. Укладання договору кіберстрахування

На четвертому етапі, після оцінювання кіберризиків та визначення параметрів страхового покриття, підприємство і страхова компанія узгоджують умови кіберстрахування. Основні параметри договору можна представити у вигляді множини:

$$C = \{Pr, Ic, T\}, \tag{6}$$

де C – договір кіберстрахування; Pr – страхова премія або страховий внесок; Ic – страхове покриття, яке визначає умови страхового відшкодування; T – строк дії договору кіберстрахування. Договір визначає взаємні права та обов'язки сторін, розмір страхових платежів, обсяг відповідальності страхової компанії, перелік страхових випадків та умови отримання страхового відшкодування.

5. Сплата страхових внесків та підтримання рівня інформаційної безпеки

На п'ятому етапі підприємство здійснює сплату страхових внесків відповідно до умов договору – одноразово або частинами:

$$Pr = \sum_{i=1}^n P r_i, \tag{7}$$

де Pr – загальна страхова премія, EUR; Pr_i – i -й страховий внесок, EUR; n – кількість платежів.

Паралельно підприємство зобов'язане підтримувати належний рівень інформаційної безпеки:

$$S \geq S_{min}, \tag{8}$$

де S – поточний рівень захищеності, S_{min} – мінімально допустимий рівень. Дотримання цієї умови є ключовим елементом кіберстрахування, оскільки підприємство відповідає за підтримання належного рівня захисту інформаційної системи.

6. Виникнення кіберінциденту та страхове відшкодування

На шостому етапі, у разі виникнення кіберінциденту, що відповідає умовам договору кіберстрахування, страхова компанія здійснює оцінювання завданих збитків та виплату страхового відшкодування в межах визначеного покриття. Факт настання страхового випадку фіксується умовою:

$$Incident = 1.$$

Сума відшкодування визначається як::

$$Comp = \min(L_f, L_c) - F, \tag{9}$$

де $Comp$ – страхове відшкодування, EUR; L_f – фактичні фінансові збитки, EUR; L_c – ліміт страхового покриття, EUR; F – франшиза, EUR. Отже, компенсація здійснюється лише в межах ліміту, а збитки у межах франшизи покриває підприємство самостійно.

7. Використання страхового відшкодування

На сьомому етапі отримані від страхової компанії кошти підприємство використовує для відновлення інформаційної системи, компенсації фінансових, юридичних та інших витрат, передбачених договором. Загальну структуру витрат, які можуть компенсуватися в межах страхового відшкодування, можна представити:

$$Comp = C_{rec} + C_{law} + C_{pr} + C_{loss}, \tag{10}$$

де C_{rec} – витрати на відновлення інформаційної інфраструктури; C_{law} – юридичні витрати; C_{pr} – витрати на управління репутаційними ризиками; C_{loss} – компенсація втрати прибутку.

При формуванні страхової суми страхова компанія враховує масштаби потенційних збитків, кількість та тип обладнання, яке може бути пошкоджено, витрати на відновлення або заміну програмного та апаратного забезпечення, витрати на залучення зовнішніх ІТ-фахівців для відновлення та стабілізації інформаційної інфраструктури.

Крім того, враховуються витрати на юридичний супровід, які можуть охоплювати правові консультації, судові провадження та врегулювання претензій, а також можливі витрати на компенсацію штрафів і санкцій за порушення законодавства. Слід зазначити, що можливість страхового покриття фінансових санкцій за порушення вимог щодо захисту персональних даних визначається нормативно-правовими актами відповідної країни. Для країн Європейського Союзу одним із ключових нормативних документів у цій сфері є Загальний регламент про захист даних (GDPR), відповідно до якого максимальний розмір адміністративного штрафу може становити до 4 % річного обороту підприємства [8]. Крім того, договір кіберстрахування може передбачати покриття витрат на PR (Public Relations) та управління репутаційними ризиками, необхідних для залучення медіа-консультантів та проведення відповідних комунікаційних кампаній [9]. Законодавство України передбачає адміністративну, цивільну або кримінальну відповідальність за окремі порушення вимог щодо захисту інформації та персональних даних. Зокрема, Кодекс України про адміністративні правопорушення містить положення щодо відповідальності за порушення законодавства про захист персональних даних, а Кримінальний кодекс України передбачає відповідальність за несанкціоноване втручання в роботу інформаційно-комунікаційних систем [2]. Отже, модель процесу кіберстрахування охоплює послідовність взаємопов'язаних організаційних, економічних та правових процедур, що забезпечують передачу частини фінансових наслідків кіберризиків від підприємства до страхової компанії.

Висновки

Розроблено модель процесу кіберстрахування для управління ризиками інформаційної безпеки підприємства. Визначено сім основних етапів її реалізації: надання підприємством інформації про інформаційну інфраструктуру та рівень захищеності; оцінювання кіберризиків; визначення страхового покриття; укладання договору кіберстрахування; сплата страхових внесків та підтримання належного рівня інформаційної безпеки; визначення страхового відшкодування у разі кіберінциденту; використання отриманих коштів для відновлення інформаційної системи та компенсації передбачених договором витрат. Виконано математичну формалізацію основних параметрів моделі, зокрема інформаційних характеристик підприємства, рівня кіберризиків, очікуваного збитку, страхової премії, страхового покриття, умов договору та страхового відшкодування. Запропонована модель дає змогу систематизувати взаємодію підприємства та страхової компанії й забезпечує формальну основу для визначення фінансових наслідків реалізації кіберзагроз. Подальший розвиток моделі доцільно пов'язати з її адаптацією до зміни рівня кіберризиків на основі періодичного моніторингу стану інформаційної безпеки підприємства.

Література

1. Revenko, D., Romanenkov, Y., Polozova, T., Lebedchenko, V., & Molchanova, K. (2024). The impact of digitalization on the economic growth of the European Union: an empirical study. *Eastern-European Journal of Enterprise Technologies*, 3(13 (129), 46–56. <https://doi.org/10.15587/1729-4061.2024.304256>

2. Верховна Рада України. (2018). *Про основні засади забезпечення кібербезпеки України* (Закон України № 2163-VIII від 5 жовтня 2017 року, зі змінами). <https://zakon.rada.gov.ua/laws/show/2163-19>

3. Adriko, R., & Nurse, J. R. C. (2024). *Cybersecurity, cyber insurance, and small-to-medium-sized enterprises: A systematic review. Information & Computer Security*, 32(5), 691–710.

4. Нагайчук, Н. Г., Третяк, Н. М., & Ткаленко, О. О. (2019). Страхування в системі управління кіберризиками підприємства в умовах цифрової економіки. *Фінансовий простір*, 1(33), 97–111. [https://doi.org/10.18371/fp.1\(33\).2019.177102](https://doi.org/10.18371/fp.1(33).2019.177102)

5. Cybersecurity and Infrastructure Security Agency. (2023). *Cyber insurance and risk management*. U.S. Department of Homeland Security. <https://www.cisa.gov/resources-tools/resources/cyber-insurance-and-risk-management>

6. Marotta, A., Martinelli, F., Nanni, S., & Yautsiukhin, A. (2015). *A survey on cyber-insurance*. Unipol Gruppo Finanziario. <https://publications.cnr.it/api/v1/documents/download/185921>

7. Корчинський, В. В., Аль Файюмі, Х., Копитін, Ю. В., & Копитіна, М. В. (2019). Ризики інсайдерських загроз у системах захисту інформації підприємств. *Наукові праці ОНАЗ ім. О. С. Попова*, (2), 112–116. <https://doi.org/10.33243/2518-7139-2019-1-2-112-116>

8. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

9. Peters, G. W., Shevchenko, P. V., & Cohen, R. D. (2021). *Understanding cyber-risk and cyber-insurance*. Centre for Financial Risk, Faculty of Business and Economics. <https://doi.org/10.2139/ssrn.3200166>

УДК 004.056.53:004.8

¹Царьов Р.Ю.,
¹Стайкуца С.В.,
²Царьова Г.А.

ЗАСОБИ ШТУЧНОГО ІНТЕЛЕКТУ, ЯК ПЕРСПЕКТИВНА МОДЕЛЬ ЗАГРОЗИ СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

¹Державний університет інтелектуальних технологій і зв’язку
²Одеська філія ПАТ «Укртелеком»
r-y.tsarov@suitt.edu.ua

Анотація. Досліджено проблему використання штучного інтелекту у контексті загрози системі інформаційної безпеки. Розглянуто задокументовані інциденти безпеки, у яких великі мовні моделі застосовано для реалізації атак на систему інформаційної безпеки. Визначено, що більшість із них посилює вже відомі вектори загроз, але деякі з них здатні впливати на припущення, покладені в основу побудови систем захисту. Виокремлено два такі припущення: розділення каналу інструкцій і каналу даних та зв’язок між обсягом дій нападника і кількістю залучених виконавців. Запропоновано таксономію з трьох площин за роллю моделі в інциденті, виділено сім векторів загроз і зіставлено їх із вимогами ДСТУ ISO/IEC 27002:2023 та НД ТЗІ 2.5-004-99. Визначено, що для трьох векторів відсутні механізми протидії.

Ключові слова: штучний інтелект, велика мовна модель, ін'єкція інструкцій, отруєння навчальних даних, вектор загрози, модель загроз, динфейк, НД ТЗІ, ISO/IEC 27002.

Донедавна застосування штучного інтелекту в кібератаках зводилося до допоміжної ролі на етапі підготовки, коли модель допомагала скласти фішинговий лист або фрагмент коду. Два інциденти 2025 року цю картину змінили. У липні CERT-UA задокументувала LAMENUG – шкідливу програму, яка отримувала команди від великої мовної моделі безпосередньо під час виконання, а не була заздалегідь запрограмована [1]. У вересні Anthropic описала операцію GTG-1002, де модель у агентному режимі вела розвідку, писала експлойти й збирала облікові дані приблизно у 30 організаціях [2]; цей інцидент відомий лише із самозвіту постачальника без незалежної верифікації, тому далі слугує ілюстрацією, а не доказом.

Спільна риса обох випадків у тому, що вони погано лягають на чинні моделі захисту. НД ТЗІ 2.5-004-99 описує порушника через рівень його можливостей, ДСТУ ISO/IEC 27002:2023 подає перелік заходів, і жоден із документів не передбачає обробника, вихід якого не визначається однозначно входом і станом. Через це виникає питання, яке й становить предмет роботи: поява таких загроз потребує лише доповнення переліку відомих загроз чи перегляду самих засад, на яких будується захист. Різниця тут не термінологічна. Якщо це новий пункт у переліку, достатньо додати ще один механізм захисту. Якщо ж перестало виконуватися базове припущення, жоден додатковий механізм захисту не допоможе, бо він працює всередині архітектури, яка вже не відповідає вимогам.

Мета роботи полягає в тому, щоб установити, щодо яких саме припущень загрози від великих мовних моделей мають системоутворюючий характер, і зіставити відповідні вектори з чинними нормативними вимогами. Під вектором загрози тут розуміється спосіб її реалізації, що задається точкою входу, послідовністю дій нападника та компонентом-ціллю; два вектори вважаються різними, коли їм відповідають різні точки

прикладення захисного заходу. Загрозу називаємо системоутворюючою, якщо її реалізація не додає нового елемента до переліку загроз, а робить хибним припущення, покладене в основу побудови захисту; практичною ознакою є те, що такий вектор не усувається доданням окремого механізму захисту в межах наявної архітектури.

Метод складається з трьох кроків. Спершу зібрано публічно задокументовані інциденти наступального застосування моделей і для кожного зазначено рівень підтвердження джерела. Далі за явною процедурою відбору з класифікацій NIST AI 100-2e2025 та OWASP Top 10 for LLM Applications 2025 виділено вектори, придатні для аналізу. Нарешті кожен відібраний вектор перевірено за ознакою системоутворюваності й зіставлено із заходами ДСТУ ISO/IEC 27002:2023 та функціональними послугами НД ТЗІ 2.5-004-99.

Роль моделі в інциденті задає природний поділ загроз на три площини (рис. 1): модель як засіб атаки, як об'єкт атаки і як компонент контуру захисту. Площини різняться рівнем підтвердження. Перші дві спираються на задокументовані інциденти та відтворені експерименти, тоді як третя публічно зафіксованих випадків не має і залишається гіпотезою, тому до подальшого зіставлення з нормативами не залучається.

Для першої площини зібрано сім публічно задокументованих інцидентів 2024–2026 років (табл. 1). Їх джерела різняться за надійністю, від матеріалів правоохоронних органів до самозвітів постачальників, і колонка рівня підтвердження дає читачеві бачити цю різницю без звертання до першоджерел.

Спільним для цих інцидентів є перенесення частини логіки з бінарного файлу на зовнішній сервіс. Так PROMPTFLUX щогодини запитує в моделі нові техніки обфускації і переписує власний код, через що сигнатурне виявлення втрачає сенс, а точка контролю зміщується з файлової системи на мережевий периметр. Це дає окремий вектор, що описує дію проти захищеної системи, а не проти самої моделі.



Рисунок 1 – Таксономія загроз за роллю моделі в інциденті

Таблиця 1 – Публічно задокументовані інциденти із застосуванням мовних моделей			
Позначення	Роль моделі в операції	Рівень підтвердження	Дж.
Відеонарада, Гонконг	Синтез відео і голосу; 15 переказів на суму близько 25 млн дол.	Матеріали поліції	[3]
LAMENUG, UAC-0001	Генерація команд збирання даних через Qwen 2.5-Coder-32B	CERT-UA; зразок доступний	[1]
PROMPTLOCK	Генерація і виконання Lua-скриптів шифрування	Звіт постачальника	[4]
GTG-1002	Розвідка, експлойти, збирання облікових даних	Самозвіт; індикаторів немає	[2]
PROMPTFLUX	Запит до Gemini на обфускацію, перезапис власного коду	Звіт постачальника	[4]
QUIETVAULT	Викрадення токенів GitHub і NPM III-інструментами	Звіт постачальника	[4]
Дистиляція моделей	Масові запити до API для відтворення логіки	Звіт постачальника	[5]

Класифікації NIST і OWASP укладені для різних цілей і напряму не зіставні, тому до них застосовано процедуру відбору. Вектор потрапляє до аналізу, якщо для нього існує задокументований інцидент або відтворений експеримент у рецензованому джерелі і він реалізується проти системи в експлуатації, а не лише в лабораторії. За цим правилом відсіяно позиції, що покриваються іншими заходами, описують наслідок замість способу реалізації або стосуються гіпотетичної третьої площини. Так, компрометацію ланцюга постачання моделей до аналізу не включено через відсутність задокументованих інцидентів, хоча саме її вважаємо найімовірнішим кандидатом на появу найближчим часом, оскільки перевірити цілісність ваг попередньо навченої моделі наявними засобами неможливо. Разом із вектором із таблиці 1 відбір дає сім векторів.

Серед відібраних векторів найпоказовіший результат стосується отруєння навчальних даних. Довгий час цю атаку вважали такою, що потребує контролю над помітною часткою вибірки, проте виявилось, що для стійкого бекдору достатньо близько 250 шкідливих документів, і ця кількість майже не залежить від розміру

моделі [6]. Для моделі з 13 млрд параметрів це відповідає приблизно 0,00016 % обсягу навчальних токенів. Практичний наслідок полягає в тому, що збільшення масштабу моделі захисту не додає, а вартість атаки при цьому не зростає.

Перевірка відібраних векторів за ознакою системоутворюваності показує, що вони роблять хибними два припущення. Перше – розділення каналу інструкцій і каналу даних. Мовна модель приймає системну інструкцію, ввід користувача та зовнішній контент одним потоком токенів, і механізму примусового розділення, порівнянного за рівнем дії з апаратним бітом NX класичної архітектури, для неї не запропоновано. Аналогія тут точна: фон-нейманівська архітектура такого розділення теж не забезпечувала, і переповнення буфера свого часу зробило відповідне припущення хибним, проте механізм примусу виявився досяжним на апаратному рівні. Для мовної моделі досяжного механізму того самого рівня поки немає, і заходи стандарту лише знижують імовірність реалізації, не усуваючи вектора. Особливо гостро це виявляється в непрямій ін'єкції, коли інструкція для моделі приходить не від користувача, а з документа чи вебсторінки, які модель читає в межах штатного сценарію, і формально нічим не відрізняється від легітимних даних.

Друге припущення – зв'язок між обсягом дій нападника і кількістю залучених виконавців, на якому неявно тримається практика ранжування порушника за рівнем можливостей. Зразки LAMENUG, PROMPTFLUX і PROMPTLOCK показують, що частину роботи, яка раніше вимагала кваліфікованого оператора, виконує програмний компонент. Оскільки наявні свідчення стосуються окремих операцій, а не кампаній загалом, коректним висновком є послаблення цього зв'язку, а не його зникнення. Окремо зазначимо, що втрата розпізнавання людини за голосом і обличчям, попри серйозність наслідків, системоутворюючою загрозою не є: така автентифікація була організаційною практикою, а не припущенням формальної моделі, і засоби протидії тут відомі.

Зіставлення семи векторів із нормативними вимогами зведено в таблиці 2. Основою обрано ДСТУ ISO/IEC 27002:2023 як каталог заходів; НД ТЗІ 2.5-004-99 наведено допоміжно, оскільки він задає критерії оцінювання захищеності, а не перелік заходів, тому колонки оцінюються кожна у власних межах, а не одна проти одної. Оцінка виставлялася за шкалою від 3 (вимога описує вектор безпосередньо) до 0 (відповідника немає).

Таблиця 2 – Матриця відповідності відібраних векторів нормативним вимогам				
Вектор загрози	ДСТУ ISO/IEC 27002	Оц.	НД ТЗІ 2.5-004-99	Оц.
Пряма ін'єкція інструкцій	8.26, 8.28	2	Відповідника немає	0
Непряма ін'єкція	5.14, 8.26	1	Відповідника немає	0
Отруєння навчальних даних	5.21, 8.25	2	Відповідника немає	0
Вилучення моделі, витік вибірки	8.12, 5.15	2	КД-2, КА-2	2
Надмірні повноваження агента	8.2, 5.15	2	КА-2 (частково)	1
Автентифікація за синтезом медіа	5.17, 6.3	2	НИ-2 (частково)	1
Модель у складі шкідливого коду	5.7, 8.16	3	НР-2	2

Розподіл оцінок показує розрив між двома документами. Заходи ДСТУ ISO/IEC 27002:2023 у п'яти випадках із семи застосовні після інтерпретації, тоді як у НД ТЗІ 2.5-004-99 відповідника не мають три вектори, і всі три стосуються самої моделі, а не її оточення. Нулі в українському документі не є хобою його укладачів: він писався 1999 року для систем із детермінованою обробкою, де поняття інструкції, вбудованої у вхідні дані, не мало сенсу. Саме ці три позиції визначають першочерговий предмет перегляду вітчизняної нормативної бази технічного захисту інформації.

Отриманий розрив між документами варто розглядати на тлі регуляторної динаміки. Європейський Regulation (EU) 2024/1689 набув чинності в серпні 2024 року, проте застосування його вимог до високоризикових систем відтерміновано до 2027–2028 років, тож поява гармонізованих стандартів, на які могла б спиратися українська нормативна база, відсувається. Водночас профільне українське законодавство окремих вимог до систем штучного інтелекту поки не містить, і побудована матриця показує, для яких саме векторів ці вимоги доведеться формулювати насамперед.

Висновки.

Загрози, пов'язані з великими мовними моделями, окремого класу атак не утворюють, але щодо двох припущень мають системоутворюючий характер. Розділення каналу інструкцій і каналу даних не має технічного вирішення рівня апаратних механізмів класичної архітектури, а зв'язок між обсягом дій нападника і кількістю виконавців послаблюється, коли частину роботи бере на себе програмний компонент. Побудована матриця відповідності придатна як робочий інструмент для двох задач: попереднього оцінювання захищеності систем із вбудованими мовними моделями та формування переліку заходів, яких бракує чинним українським документам. Напрямом подальших досліджень є контрольована перевірка гіпотези щодо третьої площини, тобто випробування засобу захисту з вбудованою моделлю на вибірці непрямих ін'єкцій.

Література

1. Кібератаки UAC-0001 із застосуванням LAMENUG, що використовує LLM : CERT-UA#16039. Держспецзв'язку України, 17.07.2025. URL: <https://cert.gov.ua/article/6284730>.

2. Disrupting the first reported AI-orchestrated cyber espionage campaign / Anthropic, 2025. URL: <https://www.anthropic.com/news/disrupting-AI-espionage>.

3. Deepfake CFO tricks Hong Kong biz out of \$25 million. The Register, 05.02.2024. URL: https://www.theregister.com/2024/02/05/hong_kong_deepfaked_cfo.

4. GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools / Google Threat Intelligence Group, 05.11.2025.

5. GTIG AI Threat Tracker: Distillation, Experimentation and Integration of AI for Adversarial Use / Google Threat Intelligence Group, 12.02.2026.

6. A small number of samples can poison LLMs of any size / Anthropic, UK AI Security Institute, The Alan Turing Institute, 09.10.2025.

УДК 621.39

Яневич О. К., Трифонова К. В., Лозовий О. О.

ІНТЕРФЕРЕНЦІЙНІ ЗАВАДИ У СИСТЕМАХ ШИРОКОСМУГОВОГО ДОСТУПУ
МЕРЕЖАМИ БУДИНКОВОЇ ЕЛЕКТРОПРОВОДКИ, ПОБУДОВАНИМИ З ВИКОРИСТАННЯМ
ПРОВОДІВ ТИПУ ШВВП ТА ВВГ-П

Державний університет інтелектуальних технологій і зв’язку
nevych.science@gmail.com, tryfksenia@gmail.com, director.fbp.kyiv@ukr.net

Анотація. Робота присвячена дослідженню інтерференційних завад у системах передачі Broadband Power Line Communications, розроблених відповідно до стандарту G.hn, що працюють мережами будинкової електропроводки, побудованими з використанням електричних проводів типу ШВВП та ВВГ-П.

Ключові слова: broadband power line communications, інтерференційні завади, мережа будинкової електропроводки.

Мережі широкосмугового доступу (ШД), побудовані на основі технології Broadband Power Line Communication (BPLC), дедалі активніше застосовуються як альтернатива традиційним провідним та безпроводовим рішенням для організації мереж Smart Home та Smart Grid. Особливістю таких систем є використання вже наявної мережі будинкової електропроводки (МБЕ) як фізичного середовища передавання високочастотних сигналів, що дозволяє суттєво знизити витрати на розгортання інфраструктури [1]. Водночас домінуючим чинником, що обмежує пропускну здатність та надійність каналу BPLC, є інтерференційні завади, спричинені неоднорідностями структури МБЕ, типом, конструкцією і довжиною електричного проводу та типом навантажень, підключених до електричних розеток МБЕ.

Одним із ключових факторів, що впливають на параметри передачі МБЕ, є тип та конструктивні особливості електричного проводу, з якого побудована МБЕ. Проводи типу ШВВП [2] та ВВГ-П [3] мають подібну конструкцію – це плоский провід з мідними жилами, вкритими полівінілхлоридною ізоляцією. Основна відмінність полягає у конструкції жил. У проводу ВВГ-П вони є суцільними, а у ШВВП – багатожильними. Ця особливість чинить суттєвий вплив на первинні та вторинні параметри проводу і, як наслідок, на інтерференційні завади у системі передачі (СП), яка працює МБЕ, побудованою за допомогою даних проводів. Це, своєю чергою, впливає на вибір оптимальної довжини захисного інтервалу символу OFDM та швидкість передавання даних.

У даній роботі з використанням відомого методу [4] було проведено дослідження інтерференційних завад у СП BPLC при роботі по двохжильному проводам типу ШВВП та ВВГ-П з площею поперечного перетину струмопровідних жил 1,5 мм² довжиною 50 м, 100 м, і 200 м. Співвідношення *h* ефективних значень інтерференційних завад і сигналу на вході приймача було розраховано для наступних параметрів СП BPLC:

- частотний план 25 МГц-PB [5];
- тип сигналу: класичний ОГС;
- кількість відліків на інтервалі ортогональності, *N* = 2048 [5];
- кількість інформаційних каналів, *n* = 942 [5];
- номер першого інформаційного каналу, *m* = 82 [5];
- довжина захисного інтервалу, *L* = 32 [5];
- маска спектральної густини потужності (СГП) на виході передавача СП BPLC [5];
- дискретні імпульсні реакції двохжильних проводів типу ШВВП та ВВГ-П з площею поперечного перетину струмопровідних жил 1,5 мм² довжиною 50 м, 100 м, 200 м і 300 м.

Результати розрахунків наведено на графіках (рис. 1), що ілюструють залежність h від номеру l інформаційного каналу і номеру відліку початку інтегрування k_T у приймачі СП BPL.

Висновки.

Аналіз результатів розрахунків показав, що зі збільшенням довжини проводу від 50 до 200 м спостерігається перерозподіл максимумів співвідношення h : перший максимум (при малих значеннях k_T) послаблюється, а другий (при великих k_T) посилюється, зрівнюючись за амплітудою на довжині 200 м, тоді як базовий рівень завади на плато залишається практично незмінним. Це пояснюється зростанням затримки відбитого сигналу пропорційно довжині лінії – для коротких ліній він накладається на початок вікна інтегрування, а для довгих формує окремий пік ближче до його кінця. Якщо ж порівнювати між собою результати розрахунку інтерференційних завад для проводу ШВВП та ВВГ-П 2х1,5, можна зробити висновок, що значення величини співвідношення h для всіх довжин проводу в усіх каналах СП BPLC відрізняються несуттєво – не більше 1%. Це пов'язано із тим, що конструкція проводів є подібною і відрізняється тільки виконанням струмопровідної жили – у проводу ВВГ-П вона є суцільною, а у ШВВП – утворена великою кількістю дрітків з малою площею поперечного перерізу. Це впливає на кілометричний опір проводу і, як наслідок, на кілометричне загасання.

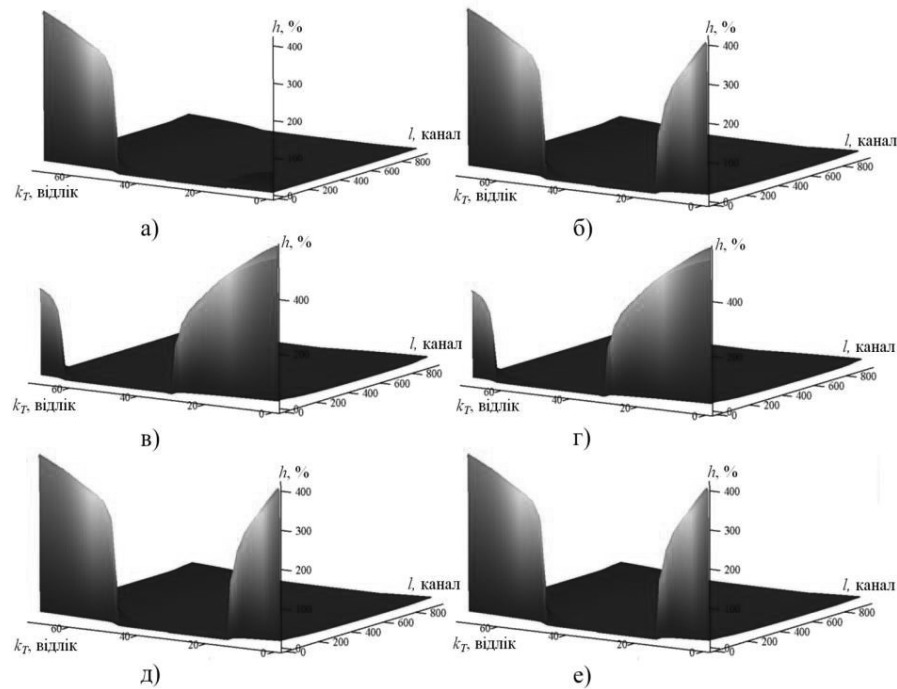


Рисунок 1 Залежність співвідношення h від l та k_T у приймачі СП BPL (середовище поширення сигналів: провід ШВВП 2х1,5 довжиною а) 50 м, в) 100 м, д) 200 м; провід ВВГ-П 2х1,5 довжиною а) 50 м, в) 100 м, д) 200 м).

Література

1. Ляховецький Л.М., Яневич О.К. PLC – технологія передавання даних мережами електропостачання // *Наукові праці Sworld*. 2016. Випуск 45. Том 1, С. 87 – 91.
2. ШВВП. URL: <https://www.zbcm.com.ua/catalog/kabel-silovij-midnij/provoda-ta-shnuri/shvvp> (дата доступу: 08.07.2026)
3. ВВГ-П, ВВГнг-П, ВВГнгд-П. Кабелі силові з мідними струмопровідними жилами (в плоскому виконанні) URL: https://www.zbcm.com.ua/wp-content/uploads/2023/09/zzkm_new24_vvg-p-vvgng-p-vvgngd-p.pdf (дата доступу: 08.07.2026)
4. Яневич О.К. Моделі та методи розрахунку характеристик систем передачі мережами електропроводки: дис. канд. тех. наук : 05.12.02 / Одеська державна академія зв'язку ім. О.С. Попова. Одеса, 2019. 195 с.
5. ITU-T Recommendation G.9964: Unified high-speed wireline-based home networking transceivers – Power spectral density specification.

ІНТЕРФЕРЕНЦІЙНІ ЗАВАДИ У СИСТЕМІ ПЕРЕДАЧІ BPLC ПРИ ВПЛИВІ ІМПУЛЬСНИХ БЛОКІВ ЖИВЛЕННЯ

Державний університет інтелектуальних технологій і зв'язку
nevych.science@gmail.com, tryfksenia@gmail.com, olegchubarev1991@ukr.net

Анотація. Досліджено характер інтерференційних завад у системі передачі Broadband Power Line Communications, що застосовують класичні ортогональні гармонічні сигнали та ортогональні гармонічні сигнали узагальненого класу при підключенні до мережі будинкової електропроводки імпульсних блоків живлення різної номінальної потужності.

Ключові слова: broadband power line communications, імпульсні блоки живлення, інтерференційні завади.

Широке застосування імпульсних блоків живлення (ІБЖ) у складі побутових електроприладів зумовлює необхідність дослідження їхнього впливу на характеристики систем передачі (СП) технології ширококугової передачі даних лініями електроживлення – Broadband Power Line Communication (BPLC). Актуальність цього питання обумовлена тим, що ІБЖ, будучи неузгодженим навантаженням мережі будинкової електропроводки (МБЕ), є причиною спотворення амплітудно-частотної та фазо-частотної характеристик МБЕ, що призводить до росту рівня інтерференційних завад і зменшення максимальної досяжної швидкості передавання даних СП BPLC.

Як показано у [1, 2], застосування ортогональних гармонічних сигналів узагальненого класу (ОГС УК) замість класичних ОГС дозволяє зменшити інтерференційні завади на вході приймача СП BPLC (яка використовує МБЕ як середовище поширення сигналу), коли навантаження на відгалуженнях МБЕ має індуктивний та ємнісний характер, представлено високоомним (в ідеальному випадку холостим ходом – ХХ) або низькоомним (в ідеальному випадку коротким замиканням – КЗ) навантаженням. У даній роботі надано результати дослідження ефективності застосування ОГС УК порівняно з класичними ОГС в СП BPLC, реалізований відповідно до стандарту G.hn, за умови підключення до МБЕ ІБЖ.

Принципова відмінність ОГС УК від класичних ОГС полягає у способі протидії виникненню інтерференції. Замість введення циклічного префікса (захисного інтервалу, що розширює інтервал ортогональності сигналів і застосовується в класичних OFDM-системах), в ОГС УК використовується обвідна спеціальної форми з косинус-квадратичними фронтами, яка забезпечує максимальну концентрацію енергії синтезованих сигналів у частотній області, тобто мінімальну ефективну спектральну ширину. Кількісною характеристикою такого підходу є коефіцієнт розширення сигналу, який відображає відносне збільшення тривалості сигналу порівняно з початковим значенням і замінює поняття захисного інтервалу, традиційно вживане для класичних ОГС.

Дослідження проведено для фрагмента МБЕ з одним відгалуженням, утвореного відрізками електричного проводу ШВВП 2х1,5 (мідні струмопровідні жили з площею поперечного перетину 1,5 мм² довжиною $l = 5$ м) (рис. 1), до полюсів якого підключено модеми BPLC (полюс 1 та 2) та навантаження у вигляді ІБЖ номіналом 65 Вт. Як відомо основним джерелом неоднорідності в ІБЖ є вхідний фільтр, параметри компонентів якого для розглядуваного у даній роботі ІБЖ є такими: $C = 100$ нФ; $L = 5,0$ мГн; $R = 814$ Ом.

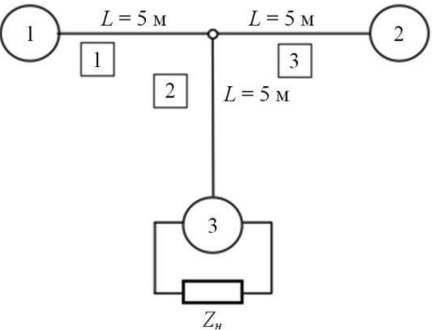


Рисунок 1 – Схема фрагменту МБЕ з одним відгалуженням

Розрахунок інтерференції виконано з використанням методу, описаного в [3] для наступних параметрів СП BPLC:

- частотний план 25 MHz-PB [4];
- кількість відліків на інтервалі ортогональності, $N = 2048$ [4];
- кількість інформаційних каналів, $n = 942$ [4];
- номер першого інформаційного каналу, $m = 82$ [4];

- коефіцієнт розширення сигналу (для ОГС УК), $\alpha = 0,0625$;
- маска спектральної густини потужності (СПП) на виході передавача СП BPLC [4];
- дискретні імпульсні реакції, визначені у [5].

Даний метод дозволяє визначити співвідношення ефективних значень інтерференційної завади та сигналу h для кожного окремого інформаційного каналу l , де сигнал представлено у вигляді маски СПП на виході передавача СП BPLC згідно з Рекомендацією ITU-T G.9964 [4] та визначити залежність даних величин від номера відліку початку обробки сигналу в приймачі k_T . Результати розрахунку наведено на рис. 2.

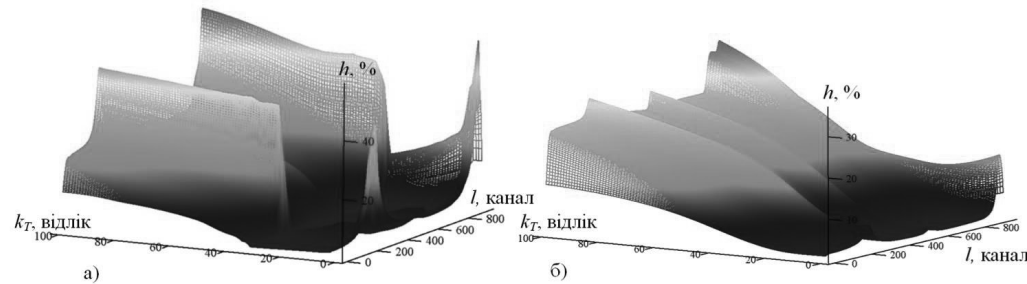


Рисунок 2 □ Залежність співвідношення h від l та k_T за умови, що у СП BPLC використовуються: а) класичні ОГС [5]; б) ОГС УК.

Висновки.

Аналіз отриманих результатів розрахунку інтерференційних завад при підключенні до МБЕ ІБЖ потужністю 65,0 Вт дозволяють зробити висновок, що застосування ОГС УК забезпечує суттєве зниження співвідношення h порівняно з класичними ОГС. Крім того, ОГС УК усувають вузькосмугові піки співвідношення h , характерні для класичних ОГС при розгляданому номіналі потужності, які роблять окремі канали практично непридатними для передавання через критично високий рівень міжканальної інтерференції.

Залежність рівня інтерференції від k_T при використанні ОГС УК має плавний характер без різких розривів, тоді як для класичних ОГС спостерігається стрибкоподібна зміна даного рівня, що свідчить про вищу передбачуваність поведінки ОГС УК щодо обрання оптимального k_T для розглядуваного навантаження.

Література

- Лашко А.Г., Ляховецький Л.М., Орешков В.І., Яневич О.К. Дослідження ефективності застосування ортогональних гармонічних сигналів узагальненого класу в системах передачі BPL. *Науковий погляд в майбутнє*. 2018. Випуск 10. Том 1, С. 13 – 19.
- Lashko A., Liakhovetskyi L., Oreshkov V., Yanevych O., Barba I. and Iegupova O. Research of the Generalized Class Orthogonal Harmonic Signals Application Efficiency in BPL Transmission Systems. *2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine. PP. 1 – 5.
- Яневич О.К. Моделі та методи розрахунку характеристик систем передачі мережами електропроводки: дис. канд. тех. наук : 05.12.02 / *Одеська державна академія зв'язку ім. О.С. Попова*. 2019. 195 с.
- ITU-T Recommendation G.9964: Unified high-speed wireline-based home networking transceivers – Power spectral density specification.
- Yanevych O. Tryfonova K. Research on Switched-mode Power Supplies Influence on a Data Rate Over Home Electrical Wiring Networks. *Security of Infocommunication Systems and Internet of Things*. 2025. Vol 3, No 2, 02013(8).

UDC 004.056.53:004.382.4

Karpenko Y.V., Dubrovin V.I.

DETECT NETWORK ATTACKS: Quantum Implementation
National University “Zaporizhzhia Polytechnic”

Abstract. Modern cyberthreats require new approaches to protecting infrastructure – from embedded microcontrollers to high-traffic networks. This paper proposes a comprehensive anomaly detection method that combines the mathematical precision of Daubechies wavelets (D4) with the power of quantum computing. Since classical systems are physically unable to handle gigabit data flows, the transition to a quantum wavelet transform (QWT) dramatically reduces computational complexity. This enables the immediate detection of hidden network attacks

and sensor data corruption. The presented approach solves the scalability problem of traditional systems, providing reliable protection in real time.

Keywords: Quantum wavelet transform, Daubechies D4 wavelet, network intrusion detection, anomaly detection, quantum signal processing, multiresolution analysis, quantum parallelism, network traffic analysis, cybersecurity, IDS.

Introduction

The rapid growth of global network infrastructure and the shift toward Big Data processing have made the speed of traffic analysis a decisive factor in cybersecurity. Modern network traffic behaves as a non-stationary signal in which legitimate activity is closely intertwined with the anomalous bursts that mark the early stages of an attack. Conventional monitoring tools frequently struggle to combine high analytical resolution with near-instant response, which leaves a window of opportunity for intruder[1, 2, 3].

Wavelet transform is one of the most effective tools for analyzing such dynamic processes, as it provides simultaneous localization in both time and frequency. Unlike classical spectral analysis, it not only detects the existence of an anomaly, but also precisely determines when it began and how long it lasted. Among the available wavelet families, the fourth-order Daubechie wavelet (D4) performs best in intrusion detection, as it has two vanishing points that allow it to suppress smooth background trends while responding sharply to true singularities[4, 5, 6].

However, the use of successive convolution in classical wavelet decomposition limits its scalability on von Neumann architectures, especially when traffic volumes reach gigabit or terabit levels. This report presents an approach that replaces the sequential classical processing with a quantum wavelet transform (QWT) based on D4 Daubechie, using superposition and quantum parallelism to achieve polylogarithmic computational complexity[7].

Problem Statement and Research Objective

Modern cyber threats are non-stationary and often hide inside regular traffic patterns at scales too small for classical spectral methods. Although the use of wavelet transform effectively overcomes the problem of spatiotemporal localization of such anomalies, its classical implementation reaches a computational ceiling when applied to large-volume real-time traffic.

The aim of this work is to develop an information technology for detecting network attacks based on the quantum Daubechie wavelet transform, aimed at increasing the accuracy of anomaly detection while radically reducing the traffic processing time. To achieve this goal, it is planned to develop a mathematical model of a quantum decomposition scheme, optimize the parameters of the applied wavelet, and conduct a comparative analysis of the developed method with traditional wavelet-oriented intrusion detection systems (IDS).

Signal Model and Quantum Amplitude Encoding

Network traffic is modeled as a time series $X(t)$ representing the intensity of packets or bytes during uniform intervals Δt . Such traffic exhibits self-similarity and range dependence; the Hurst parameter $H = 0.8$ creates a characteristic "pulse" clustering, within which low-intensity attacks (LDoS) are usually hidden and which simple thresholding methods do not capture.

To transfer the signal to quantum computing, the discretized vector $\mathbf{X} = \{x_0, x_1, \dots, x_{N-1}\}$, where $N = 2^n$, is mapped to a quantum state in a Hilbert space of dimension 2^n using amplitude encoding: $|x\rangle = \sum_{i=0}^{N-1} c_i |i\rangle$, with the amplitudes normalized such that $\sum_{i=0}^{N-1} c_i^2 = 1$, where $c_i = \frac{x_i}{|x|_V}$. This preserves the relative proportions of the traffic pulses, which is important for subsequent wavelet analysis.

The main advantage of the proposed representation is the logarithmic compression of the state space. For example, to process a traffic window of 2^{30} samples (which exceeds a billion records), only 30 qubits are needed, compared to about eight gigabytes of RAM for the equivalent classical double-precision representation. This is not a small efficiency gain, but a qualitative shift in what becomes computationally feasible for real-time, gigabit-scale analysis.

Daubechies D4 Wavelet and Multiresolution Analysis

After preparing the quantum state, multi-resolution analysis (MRA) operators decompose it into nested subspaces of increasing resolution, separating low-frequency background trends from high-frequency spikes associated with unauthorized activity. The method is implemented using a 4th-order Daubech wavelet. It outperforms the Haar wavelet due to its smoothness property, and is a more rational choice than higher-order basis sets that burden the computation with additional gates without significantly improving detection results.

For the D4 wavelet, the order of the vanishing moment is $p = 2$, which means that the transform nulls out signal components that vary linearly or remain constant. Since legitimate traffic often exhibits smooth short-term trends, D4 filters out this natural noise and focuses attention on sharp changes that mark the beginning of a DDoS attack or port scan. The transform is implemented using four filter coefficients h_0, h_1, h_2, h_3 , obtained from orthogonality conditions that guarantee unitarity[8, 9].

Table 1. Comparison of Wavelet Basis Properties for IDS Applications

Property	Haar Wavelet (D2)	Daubechies Wavelet (D4)	Fourier Transform (DFT)
Localization	Time only	Time-frequency	Frequency only
Smoothness	None (discontinuous)	Continuous	Infinite
Vanishing moments	1	2	None
Response to anomalies	High noise sensitivity	Sensitive to trend changes	Low (temporal smearing)
False positive rate	High	Low	Medium

Quantum Circuit Architecture (QWT)

The transition from classical wavelet decomposition to quantum computing requires replacing linear convolution with unitary transforms. The QWT architecture implements the orthogonal Daubechie D4 matrix as a cascade of Y-axis rotation gates ($R_y(\theta)$) and controlled NOT (CNOT) operations. Each rotation angle is analytically derived from the wavelet filter coefficients, so the sequence of gates encodes the exact D4 transform without approximation, preserving energy conservation, perfect reconstruction, and the vanishing moment property. The basis architecture relies on a lifting scheme: after the initial separation of the data into even and odd indices, the prediction and update stages are implemented through controlled quantum gates. This approach guarantees strict reversibility of the system, which is critical for preserving its unitary nature. A symmetric inverse quantum wavelet transform (QWT) is provided for the recovery and verification of the output signal. The decomposition procedure itself is performed using the Mull pyramid algorithm, generating detailing coefficients for each scale level. Anomalous amplitude spikes of these coefficients serve as precise markers of the time of occurrence of network attacks, allowing to reliably identify even subtle and complex targeted threats (APTs) that are deployed in different time dimensions.

Table 2. Gate Complexity for QWT Based on Daubechies Wavelets

Gate Type	Count for D4	Functional Role in IDS
$R_y(\theta)$	$2n - 2$	Computing wavelet coefficient values
CNOT	$2n$	Entangling temporal samples
SWAP	$n/2$	Reordering data for MRA steps
Hadamard (H)	n	Preparing superposition for parallel analysis

Comparison with Classical Wavelet-Based IDS

Classical wavelet/ARX-based approaches, evaluated on the DARPA 1999 dataset, achieved 1-9% attack type detection and approximately 95% unique cases on the best-performing test day, but fell to only 30% on a comparable day when the training data was less representative. A comparison of the parent wavelets confirmed that the Daubech method outperformed Coiflets1, Symlets2, and Discrete Meyer, detecting all 20 attack types present in the test traffic.

In real Wi-Fi traffic, the wavelet/ARX method detected five out of six attack types with zero false positives, significantly outperforming CUSUM and I-means [10]. However, its structural weakness is that the sequential convolution on von Neumann hardware becomes a bottleneck as the data volume increases, forcing systems to selectively aggregate or delay analysis, creating windows suitable for low-slow denial-of-service (LDoS) attacks. The hardware limitations of classical architectures are also clearly evident in embedded systems. For example, the implementation of DWT using the Haar basis on the STM32F411CEU microcontroller provided an anomaly detection accuracy of 93% versus 96% for the support vector method (SVM) [11]. However, such a comparison is devoid of practical meaning, since SVM algorithms are too resource-intensive for such hardware. Insufficient computing power of the controller made it impossible to use the more accurate Daubech wavelet in real time, forcing a compromise and choosing the simpler Haar basis. The developed quantum architecture completely solves this problem: due to parallel processing of the entire state vector, rather than its individual elements, the full D4 transformation is performed with polylogarithmic complexity.

Discussion: Practical Implementation Considerations

Although the theoretical complexity advantages of quantum wavelet transform (QWT) are compelling, several practical limitations must be considered before real-world deployment. Current noisy intermediate-scale quantum devices (NISQ) exhibit gate error rates and decoherence times that limit the effective circuit depth achievable before the wavelet coefficients lose accuracy. For a traffic window encoded in n qubits, the cascade of R_y rotations and CNOT

gates described in Table 2 must be completed within the hardware coherence window, which limits both the window size N and the number of decomposition levels that can be reliably extracted in a single run. Another important aspect is the bottleneck problem in the readout step. Although amplitude coding provides efficient logarithmic compression of the input data, the procedure for extracting the full spectrum of detail coefficients requires multiple measurements and quantum tomography of the states. This process scales extremely inefficiently and can nullify the computational gain obtained at the preparation and quantum transformation stages. To solve this problem, selective (targeted) readout strategies are used in applied architectures. Instead of a full reconstruction of the multi-level decomposition, measurements focus exclusively on the subspaces with the highest resolution, where the probability of capturing anomalous bursts from attacks is maximum.

Successful integration of the developed technology into the existing network infrastructure will require the creation of a hybrid interface layer. Stages such as classical packet capture and their preliminary preparation (windowing, normalization, buffering) are integral steps before the start of amplitude coding. On the other hand, converting the detected anomalies of the detail ratios into real notifications or commands to block threats also requires classical decision-making logic. Accordingly, in the near future, the latest solutions will not completely replace traditional IDS pipelines. Instead, the quantum coprocessor will play the role of an integrated hardware accelerator inside the classical monitoring stack, which is fully consistent with the concept of a hybrid architecture proposed in the conclusions.

Conclusions

Quantum signal processing based on the Daubechie D4 wavelet transform offers a practical way to overcome the computational barrier that limits classical intrusion detection systems in gigabit- and terabit-scale networks. By encoding traffic into quantum amplitudes of states and implementing the D4 filter as a cascade of unitary gates (R_y and CNOT flips), the proposed QWT preserves all the mathematical properties of the classical transform, including its two vanishing points and correspondingly low false positive rate, while achieving polylogarithmic computational complexity with respect to the size of the input data. This eliminates the trade-off between accuracy and performance that limits classical implementations, especially on resource-constrained embedded hardware, where the choice of a lighter wavelet basis (Haar) currently comes at the expense of a direct loss of detection accuracy.

Further research should be directed towards the creation of hybrid quantum-classical architectures. In such systems, the quantum coprocessor will take on the ultra-fast preprocessing – trend filtering and anomaly isolation, while the classical machine learning algorithm will perform the final threat classification. In addition, the development of optimized amplitude coding methods and measurement protocols is critically important to avoid the emergence of new classical “bottlenecks” at the data readout stage. Given the rapid development of error correction technologies on modern quantum devices (NISQ), the practical implementation of the developed hybrid IDS is quite achievable by the end of the current decade.

References

- Wavelets and Matrix Transformations. Misl Technical Reports. Retrieved from http://bearcave.com/misl/misl_tech/wavelets/matrix/index.html.
- Kaliuha, B., & Zaderei, N. (2018). Zastosuvannia veivlet-peretvorennia v suchasni nautsi ta tekhnitsi. Tezy dopovidi (National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"). (in Ukrainian)
- Rawat, S., & Sastry, C. S. Network intrusion detection using wavelet analysis. In Proceedings of the 7th International Conference on Information Technology (CIT '04), vol. 3356 of Lecture Notes in Computer Science, pp. 224–232, Hyderabad, India, December 2004.
- Chemerys, K. M., & Deineha, L. Yu. (2022). Zastosuvannia metodu veivlet-analizu dlia vyiavlennia atak v merezhakh. Nauka i tekhnika PS ZSU, 1(46), 99–107. (in Ukrainian)
- Petryk, B. V., & Dubrovin, V. I. (2021). Vyiavlennia atak typu DoS v merezhovomu trafiku za dopomohoiu veivlet-peretvorennia. Prykladni pytannia mat. modeliuvannia, 4(1), 186–196. (in Ukrainian)
- Kwon, D., Ko, K., Vannucci, M., Reddy, A. N., & Kim, S. (2006). Wavelet methods for the detection of anomalies and their application to network traffic analysis. Quality and Reliability Engineering International, 22(8), 953–969. <https://doi.org/10.1002/qre.781>
- Karpenko, Ya., & Dubrovin, V. (2026). Doslidzhennia kvantovoho veivlet-peretvorennia Dobeshi dlia vyiavlennia merezhovykh atak. Kombinatorni konfihuratsii ta yikhni zastosuvannia: materialy XXVIII Mizhnar. nauk.-prakt. seminaru, 127–132. (in Ukrainian)
- The Daubechies Wavelet Transform. Bear Cave Software Resources. Retrieved from <http://bearcave.com/software/java/wavelets/daubechies/index.html>.
- Tverdokhlib, Yu. V., & Dubrovin, V. I. (2015). Kompiuterna prohrama «Analiz chastotnykh skladovykh veivlet-bazysu»: Svidotstvo pro reiestratsiiu avtorskoho prava na tvir No 60630. Derzhavna sluzhba intelektualnoi vlasnosti Ukrainy. (in Ukrainian)
- Dainotti, A., Pescape, A., & Ventre, G. (2006). Wavelet-based detection of DoS attacks. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '06), pp. 1–6, San Francisco, Calif, USA, November 2006.
- Pacheco, Benitez, Pérez, & Brau. (2024). Wavelet-Based Computational Intelligence for Real-Time Anomaly Detection and Fault Isolation in Embedded Systems. Machines.

ПРОФІЛЮВАННЯ СОЦІОТЕХНІКА ЗА ОЗНАКАМИ ВИЯВЛЕНОЇ ФІШИНГ-АТАКИ

¹Національний технічний університет «Дніпровська політехніка»,
²Державний університет інформаційно-комунікаційних технологій
¹annakor@ukr.net, ²marinapetcenko@gmail.com, ¹kirilldavy@gmail.com

Анотація. Аналіз існуючих підходів до виявлення фішингових атак показав недостатню формалізацію зв’язку між технічними параметрами виявленої атаки та характеристиками її виконавця. Це зумовлює необхідність розроблення методів, що забезпечують формування профілю соціотехніка за результатами аналізу виявленої фішинг-атаки. Запропоновано метод профілювання соціотехніка, що передбачає розширення узагальненого кортежу множиною ознак профілю (Feature Set). Метод передбачає реалізацію чотирьох етапів: формалізоване представлення виявленої фішинг-атаки, визначення характеристик соціотехніка за п’ятнадцятьма класифікаційними ознаками, формування узагальненого профілю та його візуалізацію. Отримані результати можуть використовуватися для підтримки атрибуції кібератак, кіберрозвідки та реагування на інциденти.

Ключові слова: фішинг, профіль соціотехніка, соціальна інженерія, кіберрозвідка, інформаційна безпека.

Фішингові атаки залишаються одним із поширених видів соціотехнічних атак, що поєднують технічні засоби впливу на інформаційні системи з методами соціальної інженерії. Їх реалізація передбачає використання спеціально підготовленої доменної та мережевої інфраструктури, URL-адрес, засобів маскування та сценаріїв взаємодії з потенційною жертвою. Тому параметри виявленої фішинг-атаки можуть характеризувати не лише сам факт фішингової активності, а й окремі особливості її виконавця, що зумовлює актуальність формування профілю соціотехніка за результатами аналізу виявленої атаки.

Існуючі дослідження у цій сфері переважно розвиваються у двох напрямках. Перший охоплює методи виявлення фішингових атак за параметрами URL-адрес, DNS та доменної інфраструктури і спрямований переважно на детекцію та класифікацію фішингових ресурсів. Другий пов’язаний із класифікацією соціотехнічних атак та визначенням характеристик їх виконавців. Водночас недостатньо формалізованим залишається зв’язок між технічними параметрами конкретної виявленої фішинг-атаки та характеристиками соціотехніка, які можуть бути визначені на їх основі. Отже, актуальним науковим завданням є розроблення методу, що забезпечує формалізований перехід від параметрів виявленої фішинг-атаки до формування профілю її виконавця.

Метою дослідження є розроблення методу профілювання соціотехніка за результатами аналізу параметрів виявленої фішинг-атаки на інформаційну систему.

Для досягнення поставленої мети пропонується розширити функціональні можливості узагальненого кортежу шляхом введення нового компонента – множини ознак профілю соціотехніка **FS_{ph}**. Зазначена множина формується відповідно до класифікаційної моделі соціотехнічних атак на основі аналізу параметрів виявленої фішинг-атаки DA, FC DNS, NSD, UL, SSL/Cert Age, SC, DR, TE та TLD [1].

Запропонований метод реалізується у чотири взаємопов’язані етапи: формування формалізованого представлення виявленої фішинг-атаки, визначення характеристик профілю соціотехніка, формування його узагальненого профілю та візуалізація отриманих результатів.

На **першому етапі** здійснюється формування формалізованого представлення виявленої фішинг-атаки на основі її параметрів. Вихідною основою є розширений узагальнений кортеж [2], до структури якого поряд із параметрами атаки P_{ph} , нечіткими еталонами T_{ph}^e , поточними значеннями $P_{ph}^{\tau f}$, патернами детекції DP_{ph} вводиться множина ознак профілю соціотехніка **FS_{ph}**. Вона формується за п’ятнадцятьма класифікаційними ознаками **S_i** відповідно до моделі сучасних підходів реалізації соціотехнічних атак [3-4].

Таким чином, формалізоване представлення виявленої фішинг-атаки можна подати у вигляді розширеного кортежу

$$CA_{ph}^{\tau f} = \langle CA_{ph}, P_{ph}, T_{ph}^e, P_{ph}^{\tau f}, DP_{ph}, FS_{ph} \rangle,$$

де: $CA_{ph}^{\tau f}$ – фішингове атакуюче субдовкілля, а CA_{ph} – ідентифікатор фішинг-атаки.

Введення компонента **FS_{ph}** розширює функціональні можливості формалізованого представлення атаки, оскільки результати її детекції використовуються не лише для встановлення факту фішингової активності, а й як вихідні дані для подальшого визначення характеристик виконавця.м

На **другому етапі** на основі сформованого формалізованого представлення виявленої фішинг-атаки визначаються характеристики соціотехніка, результатом якого є множина характеристик профілю соціотехніка (табл. 1).

Таблиця 1. Основні характеристики сформованого профілю соціотехніка

Ознака	Клас	Ключова підстава
S₁ – часовий аспект	ППЛ-атака	Молодий домен, швидка ротація <i>fast-flux DNS</i>
S₂ – галузева афіліація	КС/ГУ-атаки	Орієнтація на інформаційну систему організації
S₃ – політика безпеки	ДП-методи	Імітація довірених ресурсів, малий вік SSL
S₄ – ініціалізація	УА-атака	Активація після переходу за фішинговим URL
S₅ – тип звернення	АВ-методи	Пряме звернення до жертви
S₆ – інструментарій	ПМ-методи	Автоматизація доменів, DNS, URL і вебресурсів
S₇ – порушення безпеки	К/Ц-дієві	Порушення конфіденційності та цілісності
S₈ – ступінь важкості	С-атаки	Складна багатокomпонентна інфраструктура атаки
S₉ – реляційні ознаки	ПМ-атаки	Масштабований вплив на множину жертв
S₁₀ – тип джерела	ЛГ/КН-джерельні	Орієнтація на неухважних користувачів і персонал
S₁₁ – тип доступу	КН/СК-доступ	Націленість на конфіденційні/секретні дані
S₁₂ – дистанційність	МТ-віддалені	Віддалена реалізація через Інтернет
S₁₃ – маніпулювання	АВ/ОБ-маніп.	Авторитетність і терміновість
S₁₄ – тип соціотехніка	ХК/ШХ-виконавчі	Поєднання профілю хакера і шахрая
S₁₅ – масштаб	ГБ-атаки	Глобальний характер кампанії

На **третьому етапі** визначені характеристики інтегруються в єдиний профіль соціотехніка. Множина ознак профілю **FS_{ph}**, сформована відповідно до класифікаційної моделі [3-4], набуває такого вигляду:

$$FS_{ph} = \{ППЛ; КС/ГУ; ДП; УА; АВ; ПМ; К/Ц; С; ПМ; ЛГ/КН; КН/СК; МТ; АВ/ОБ; ХК/ШХ; ГБ\}.$$

Сформована множина **FS_{ph}** визначає профіль соціотехніка та включається до узагальненого кортежу фішингової атаки:

$$CA_{ph}^{\tau f} = \langle CA_{ph}, \{P_{phDA}, P_{phFCDNS}, P_{phNSD}, P_{phUL}, P_{phSSL}, P_{phSC}, P_{phDR}, P_{phTE}, P_{phTLD}\}, \\ \{\{T_{phDA}^e, T_{phDA}^e, T_{phDA}^e\}, \{T_{phFCDNS}^e, T_{phFCDNS}^e, T_{phFCDNS}^e\}, \dots, \{T_{phTLD}^e, T_{phTLD}^e, T_{phTLD}^e\}\}, \\ \{P_{phDA}^{\tau f}, P_{phFCDNS}^{\tau f}, \dots, P_{phTLD}^{\tau f}\}, \\ \{DP_{phDA}, DP_{phFCDNS}, \dots, DP_{phTLD}\}, \\ \{ППЛ; КС/ГУ; ДП; УА; АВ; ПМ; К/Ц; С; ПМ; ЛГ/КН; КН/СК; МТ; АВ/ОБ; ХК/ШХ; ГБ\} \rangle.$$

На **четвертому етапі** здійснюється візуалізація сформованого профілю соціотехніка. Множина **FS_{ph}** представляється у вигляді кругової діаграми, кожний сектор якої відповідає одній із п’ятнадцяти класифікаційних ознак **S_i** і відображає визначений для неї клас відповідно до моделі [3-4]. Таке представлення дає змогу комплексно відобразити структуру профілю соціотехніка, виокремити його основні характеристики та спростити подальший аналіз технічних і поведінкових ознак.

Висновки. Запропоновано метод профілювання соціотехніка, що забезпечує формалізований перехід від параметрів виявленої фішинг-атаки до визначення характеристик її виконавця. На основі аналізу параметрів атаки сформовано узагальнений профіль соціотехніка за п’ятнадцятьма класифікаційними ознаками. Отримані результати можуть використовуватися для підтримки атрибуції фішингових атак, кіберрозвідки та реагування на інциденти.

Література

1. Корченко А. О., Давиденко К. О., Аскеров М. Г., Журов Ю. С. Метод формалізації багатовимірною еталонного субдовкілля для виявлення фішингових URL-адрес // *Сучасний захист інформації*. 2026. № 2(66). С. 70-87. <https://doi.org/10.31673/2409-7292.2026.021105>

2. Корченко А. А. Кортёжная модель формирования набора базовых компонент для выявления кибератак // *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2014. Вип. 2(28). С. 29-36.

3. Korchenko O., Korchenko A., Zybin S., Davydenko K. An Approach for Classifying Socio-Technical Attacks // *Radioelectronic and Computer Systems*. 2025. № 2. Р. 230-252. <https://doi.org/10.32620/reks.2025.2.15>

4. Корченко О., Корченко А., Зибін С., Давиденко К. Сучасні підходи реалізації соціотехнічних атак // *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. № 2. С. 48-71. <https://doi.org/10.32782/IT/2025-2-6>

МЕТОД ДЕТЕКТУВАННЯ МУЛЬТИВЕКТОРНИХ АРТ-АТАК ІЗ ВИКОРИСТАННЯМ АНСАМБЛІВ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

Державний університет інформаційно-комунікаційних технологій
o.shkurchenko@stud.duikt.edu.ua, iaverichev19@gmail.com, petja9186@gmail.com

Анотація. Запропоновано метод детектування мультимекторних АРТ-атак на основі ансамблю алгоритмів машинного навчання. Метод поєднує класифікатори Random Forest, XGBoost, SVM та неймережеву модель з механізмом динамічного зважування голосів. Для навчання використано ознаки мережевого трафіку, системних логів і поведінкових характеристик процесів, витягнуті з наборів даних CIC-IDS2018 та SCVIC-APT-2021. Експериментально показано підвищення точності виявлення на 3–5 % порівняно з окремими класифікаторами та зниження рівня хибних спрацьовувань. Отримані результати підтверджують ефективність ансамблевого підходу для раннього виявлення складних цільових атак.

Ключові слова: АРТ-атаки, мультимекторні атаки, ансамблі машинного навчання, детектування вторгнень, Random Forest, XGBoost, кібербезпека.

Сучасні цільові атаки типу Advanced Persistent Threat (APT) характеризуються тривалістю, прихованістю та використанням кількох векторів одночасно: фішинг, експлуатація вразливостей, латеральне переміщення, командно-контрольні канали та експільтрація даних [1, 4]. Традиційні системи виявлення вторгнень, що базуються на сигнатурах або простих евристичках, виявляються недостатньо ефективними проти таких багатоетапних загроз [2, 6]. Тому актуальною є розробка методів, здатних комплексно аналізувати гетерогенні джерела даних і виявляти аномальні патерни на ранніх стадіях атаки.

У роботі запропоновано метод детектування мультимекторних АРТ-атак, що ґрунтується на ансамблі алгоритмів машинного навчання. Ансамбль складається з чотирьох базових моделей: Random Forest (RF), XGBoost, Support Vector Machine (SVM) з RBF-ядром та двошарової нейронної мережі (MLP). Для агрегації прогнозів застосовано схему зваженого голосування, де ваги моделей динамічно перераховуються на основі їхньої точності на валідаційній вибірці та каліброваної ймовірності (temperature scaling).

Остаточне рішення ансамблю визначається за формулою:

$$\hat{y} = \arg \max_{c \in C} \sum_{m=1}^M w_m \rho_m(c | x) \quad (1)$$

де: $\hat{y}$ – прогнозований клас (АРТ-атака або нормальний трафік);

C – множина можливих класів;

M – кількість базових моделей в ансамблі ($M = 4$);

w_m – вага m -ї моделі;

$\rho_m(c | x)$ – апостеріорна ймовірність класу c , оцінена m -ю моделлю для вхідного вектора ознак x .

Ваги моделей обчислюються на основі їхньої точності на валідаційній вибірці:

$$w_m = \frac{\text{Acc}_m}{\sum_{k=1}^M \text{Acc}_k} \quad (2)$$

де: Acc_m – точність (акурасу) m -ї моделі на валідаційній вибірці;

$\sum_k \text{Acc}_k$ – сума точностей усіх моделей ансамблю. Такий підхід забезпечує більший вплив моделей з кращою узагальнюючою здатністю [2, 3].

Для калібрування ймовірностей застосовується temperature scaling:

$$p'(y | x) = \text{softmax}(z/T) \quad (3)$$

де: z – вектор логітів (вихідних оцінок) моделі до застосування softmax;

$T > 0$ – температурний параметр, який підбирається на валідаційній вибірці шляхом мінімізації негативної логарифмічної правдоподібності;

$p'(y|x)$ – відкалібрована ймовірність класу. Збільшення T «згладжує» розподіл ймовірностей і зменшує надмірну впевненість моделей.

Ознаковий простір формується з трьох груп характеристик: (1) статистичні та часові ознаки мережевих потоків; (2) ознаки системної активності; (3) поведінкові послідовності (n-грами API та марковські ймовірності переходів) [7]. Для зменшення розмірності застосовано метод взаємної інформації та Recursive Feature Elimination [1].

Важливість ознаки оцінюється за взаємною інформацією:

$$I(X; Y) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} \quad (4)$$

де: X – випадкова величина (значення ознаки);

Y – мітка класу;

$p(x, y)$ – сумісний розподіл;

$p(x)$ та $p(y)$ – маргінальні розподіли. Ознаки з найвищими значеннями $I(X; Y)$ зберігаються для навчання моделей.

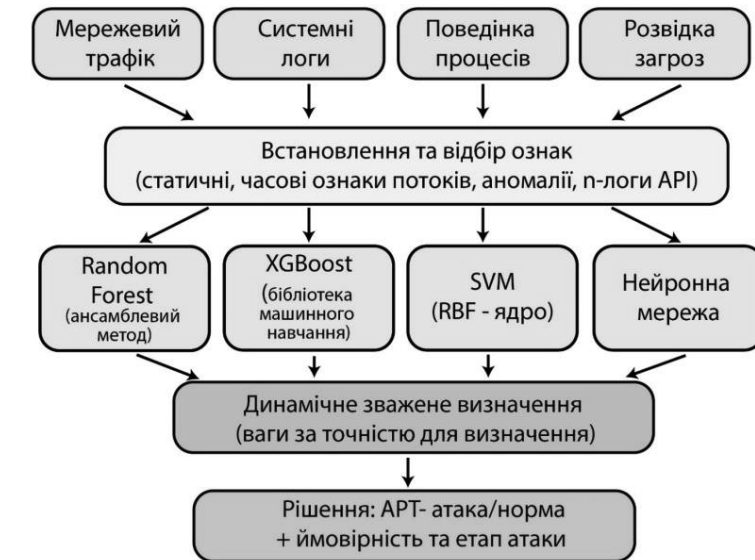


Рис. 1. Архітектура запропонованого методу детектування мультимекторних АРТ-атак

На рис. 1 представлено загальну архітектуру запропонованого методу. Вхідними даними слугують чотири основні джерела: мережевий трафік, системні логи, поведінкові характеристики процесів та інформація з бази знань MITRE ATT&CK. Після етапу витягання та відбору ознак (статистичних, часових, n-грам API тощо) сформований вектор подається паралельно на чотири базові класифікатори ансамблю. Остаточне рішення формується шляхом динамічного зваженого голосування, що дозволяє адаптивно враховувати сильні сторони кожної моделі та підвищувати стійкість до різноманітних сценаріїв мультимекторних атак.

Експериментальне дослідження проведено на об'єднаному наборі даних, що включає фрагменти CIC-IDS2018 та SCVIC-APT-2021, доповнені синтетичними мультимекторними сценаріями, згенерованими відповідно до тактик MITRE ATT&CK [5]. Дані розділено у пропорції 70/15/15 (навчання / валідація / тест) із збереженням стратифікації за класами. Для боротьби з дисбалансом класів використано комбінацію SMOTE та cost-sensitive навчання.

Отримані результати демонструють, що ансамбль досягає Macro F1-score 96,8 % та accuracy 97,4 %, що на 3,1–4,7 % перевищує показники найкращого окремого класифікатора (XGBoost). Рівень хибних позитивних спрацьовувань знижено до 0,9 % [2, 3]. Особливо помітне покращення спостерігається на етапах розвідки та латерального переміщення, де окремі моделі часто дають пропуски. Аналіз важливості ознак підтвердив ключову роль комбінації часових характеристик потоків і поведінкових n-грам.

Практична реалізація методу можлива у вигляді модуля для SIEM-систем або як самостійний агент на хостах. Обчислювальна складність ансамблю залишається прийнятною для онлайн-режиму завдяки паралельному виконанню базових моделей і використанню попередньо навчених ваг [4, 6].

Висновки. Запропонований метод детектування мультимекторних АРТ-атак на основі ансамблю алгоритмів машинного навчання забезпечує вищу точність і стійкість порівняно з окремими класифікаторами. Використання різноманітних ознак і динамічного зважування дозволяє ефективно виявляти складні багатоетапні атаки. Подальші дослідження плануються спрямувати на адаптацію методу до потокового режиму та інтеграцію з графовими моделями зв'язків між сутностями.

Література

1. Dau D.D., Lee S., Kim H. A comprehensive comparison study of ML models for multistage APT detection: focus on data preprocessing and resampling // Journal of Supercomputing. 2024. Vol. 80. P. 14143–14179.

2. Tung N. T., Do Xuan C., Long V. T. Ensemble learning-based adaptive and adversarial techniques for APT attack detection // International Journal of Information Security. 2025. Vol. 24. Art. 152. <https://doi.org/10.1007/s10207-025-01053-9>

3. TSE-APT: An APT Attack-Detection Method Based on Time-Series and Ensemble-Learning Models // Electronics. 2025. Vol. 14, No. 15. Art. 2924.

4. Гребенюк М.С. Виявлення АРТ-атак на рівні операційних систем за допомогою методів машинного навчання: магістерська дис. Київ : КПІ ім. Ігоря Сікорського, 2023.

5. MITRE ATT&CK® Framework. URL: <https://attack.mitre.org>

6. Савченко, В., Поночовний, П., & Аверічев, І. (2024). ВИЯВЛЕННЯ DDOS-АТАКИ НА ВИСОКОШВИДКІСНУ МЕРЕЖУ: ОПИТУВАННЯ. Науковий журнал «Прикладні проблеми комп’ютерних наук, безпеки та математики», (3), 71–81. вилучено із <https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/127>

7. Shafiee M.A., Shajari M., Barzegar M. Methods to Identify the Family of Advanced Persistent Threats Based on Deep Neural Network and n-gram of API calls // arXiv preprint. 2023.

УДК 004.75:004.94

Бабенко К. Є.

МОДЕЛЬ НАСКРІЗНОЇ ЗАТРИМКИ ДОСТУПУ ДО ОНОВЛЕНОГО СТАНУ ПРОГРАМОВАНИХ БЛОКЧЕЙН-СИСТЕМ ПЕРШОГО РІВНЯ

Дніпровський національний університет імені Олеся Гончара, Дніпро, Україна
babenko-k@365.dnu.edu.ua

Анотація. Розглянуто задачу мінімізації наскрізної користувацько-видимої затримки у програмованих блокчейн-системах першого рівня. Запропоновано операційне визначення $T_{visible}$ від подання транзакції до першого підтвердженого RPC-читання оновленого фіналізованого стану, причинну декомпозицію критичного шляху, модель взаємопов’язаних черг та контур адаптивного керування параметрами формування блоків, backpressure і ресурсами. Наведено систему метрик і схему експериментальної перевірки на *Avalanche L1 / EVM-L1*.

Ключові слова: блокчейн, *Avalanche L1*, наскрізна затримка, *RPC*, *tail latency*, черги, адаптивне керування.

Для інтерактивних розподілених застосунків продуктивність блокчейн-системи визначається не лише TPS або часом консенусної фінальності. Практично значущим є момент, коли наслідок транзакції стає доступним зовнішньому клієнту через *RPC*. Між прийняттям блока та таким читанням виникають додаткові затримки виконання, durable commit, індексації, реплікації, *RPC*-черги, кешування та клієнтського виявлення. Тому оптимізація окремої стадії не гарантує мінімізації повного критичного шляху.

Одиницею спостереження є транзакція τ , що змінює унікальний ключ $x\tau$ на значення $v\tau$. Початковою подією є передавання `eth_sendRawTransaction`, кінцевою – перша відповідь, у якій `state read` повертає $x\tau=v\tau$, а блок задовольняє визначену політику фінальності. Операційна метрика:

$$T_{visible}(\tau) = t_{first_{visible}}(\tau) - t_{submit}(\tau). \quad (1)$$

Це визначення відокремлює користувацько-видиму затримку від `receipt latency` та `consensus finality`. Серверна складова описується причинним DAG, тому перекривні стадії враховуються через `critical path/max-plus` залежності.

$$T_{visible} = T_{ingress} + T_{core} + T_{publish} + T_{detect} \quad (2)$$

$$T_{publish} = T_{persistence} + T_{indexing} + T_{replication} + T_{RPC_{queue}} \quad (3)$$

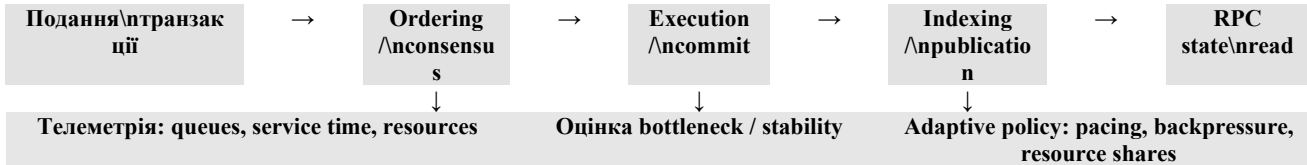


Рисунок 1. Наскрізний конвеєр та контур адаптації

За змінного навантаження ключовим обмеженням стає стійкість внутрішніх черг. Для стадії k дискретна динаміка backlog описується:

$$Q_k(t + 1) = \max\{Q_k(t) - S_k(t, u_t), 0\} + A_k(t), \quad (4)$$

де $A_k(t)$ – надходження, $S_k(t, u_t)$ – обсяг обслуговування. Необхідним стаціонарним орієнтиром є $\rho_k = \lambda_k / \mu_k < 1$, однак для `fork-join` і `feedback`-структур достатня стійкість потребує `fluid/Lyapunov` аналізу. При тривалому `overload` потрібні `backpressure` або `admission control`.

Таблиця 1. Компоненти $T_{visible}$ та керовані параметри

Компонент	Джерело затримки	Спостереження	Керуюча дія
Ingress / ordering	RPC, mempool, builder	arrival rate, queue	admission, batching
Consensus / execution	network, EVM	critical path, CPU	block interval, concurrency
Commit / indexing	disk I/O, state/index	I/O queue	resource shares, priority
Publication / RPC	replication, read queue	visibility gap, stale	isolation, read priority

Мінімізація хвостової затримки є багатокритеріальною задачею, оскільки агресивне скорочення `block interval` може погіршити `goodput`, збільшити конкуренцію за `CPU/I/O` та викликати `queue runaway`. Робоча цільова функція:

$$J = w_{95}P_{95}(T_{visible}) + w_{99}P_{99}(T_{visible}) + w_qSE[Q_k] + w_rC_{resource} + w_dP_{drop} + w_sP_{stale}. \quad (5)$$

Оптимізація виконується за обмежень $X \geq X_{min}$, коректності, ресурсного бюджету, відсутності передчасної видимості та стійкості черг. Вектор дій $u(t)$ охоплює `block interval`, `batching`, `concurrency`, `backpressure` і `resource shares`. Політика повинна містити `hysteresis`, `rate limits` і `safe fallback`.

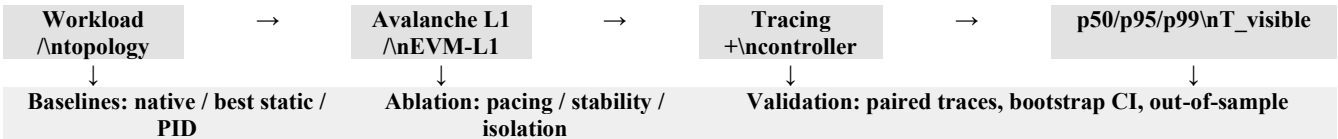


Рисунок 2. Схема експериментальної перевірки

Експериментальна програма передбачає `native baseline`, найкращу статичну конфігурацію, простий `feedback-controller` та повний адаптивний метод. `Primary metric` – `p95  $T_{visible}$` ; додатково оцінюються `p99`, `CVaR_0.99`, `committed goodput`, `backlog`, `queue slope`, `drain time`, `P_stale`, `P_drop` і ресурсні витрати. Порівняння виконуються на однакових `arrival traces`, `network seeds` і `fault schedules` із `bootstrap confidence intervals` та `paired tests`.

Пороги `p95 ≤ 500` мс для визначеного нормального навантаження та `p95 ≤ 250` мс для локальної топології є гіпотезами, а не отриманими результатами. Вони мають оцінюватися разом із `workload`, `topology`, `hardware`, версією ПЗ, `goodput` та довірчим інтервалом.

Висновки. Запропонована постановка переносить фокус із локальної `consensus latency` на повний шлях «`submission` – `finalized state read`». Науково значущими результатами є операційна метрика $T_{visible}$, причинно-чергова модель критичного шляху, умови стійкості та адаптивний алгоритм керування параметрами конвеєра. Подальша перевірка має встановити `effect size`, область стійкої роботи та межі переносимості моделі.

Окремою складовою методики є контроль `visibility gap` – інтервалу між прийняттям блока та фактичною доступністю його стану через користувацький *RPC*. Для кожної транзакції доцільно корелювати `timestamps ingress`, `ordering`, `execution`, `persistence`, `indexing` і `state read` за `trace ID`. Основний `endpoint` вимірюється одним клієнтським `monotonic clock`, що зменшує вплив похибки міжвузлової синхронізації; `RTP/chrony` потрібні лише для внутрішньої декомпозиції.

Для перевірки стійкості слід використовувати `steady`, `ramp`, `step`, `burst` і `heavy-tail` профілі надходження. Важливо фіксувати `saturation point`, `queue slope` та `drain time` після скінченного `burst`. Якщо λ перевищує оцінену стійку пропускну здатність, зростання черг не може бути усунене лише зміною `block pacing`, тому алгоритм має переходити до контрольованого `admission/backpressure` режиму.

Відтворюваність забезпечується фіксацією версій *AvalancheGo/EVM-L1*, `genesis`, `validator/RPC placement`, контейнерних `image digests`, конфігурацій вузлів, `random seeds` і `fault schedules`. `Training` і `test` сценарії мають розділятися за цілими `topology/workload cells`, щоб уникнути `leakage` під час вибору параметрів адаптивної політики.

Наукова валідація повинна включати ablation-аналіз: estimator off/on, adaptive pacing окремо, pacing разом зі stability guard, shared resources проти isolation та повний метод із fallback. Це дозволяє кількісно відокремити внесок кожного механізму і визначити режими, у яких складніша адаптивна політика не має переваги над best static baseline.

Література

1. Xiang Z., Li Z., Arun B., Zhang T., Spiegelman A. Zaptos: Towards Optimal Blockchain Latency. CoRR. 2025. arXiv:2501.10612. DOI: 10.48550/arXiv.2501.10612.

2. Amores-Sesar I., Cachin C., Schneider P. An Analysis of Avalanche Consensus. Theoretical Computer Science. 2026. Art. 116147. DOI: 10.1016/j.tcs.2026.116147.

3. Sokolik Y., Nassar M., Rottenstreich O. Age-Aware Fairness in Blockchain Transaction Ordering for Reducing Tail Latency. IEEE/ACM Transactions on Networking. 2025. Vol. 33, No. 2. P. 807-822. DOI: 10.1109/TNET.2024.3503758.

4. Dinh T. T. A. et al. BLOCKBENCH: A Framework for Analyzing Private Blockchains. Proceedings of the 2017 ACM SIGMOD International Conference on Management of Data. 2017. P. 1085-1100. DOI: 10.1145/3035918.3064033.

5. Lee J. et al. Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance. Blockchain: Research and Applications. 2021. Vol. 2, No. 1. Art. 100009. DOI: 10.1016/j.bcr.2021.100009.

УДК 004.056.53

Аверічев І.М., Зарванський М. В.

ФІШИНГ У КОРПОРАТИВНИХ СЕРЕДОВИЩАХ
КОМУНІКАЦІЇ (SLACK, MICROSOFT TEAMS, DISCORD)

Державний університет інтелектуальних технологій і зв’язку
iaverichev19@gmail.com, m.zarvanskiy@duikt.edu.ua

Анотація. Проаналізовано сучасні фішингові атаки, що здійснюються через корпоративні платформи комунікації Slack, Microsoft Teams та Discord. Показано, що зловмисники активно використовують довіру користувачів до внутрішніх каналів, імперсонацію IT-підтримки, підроблені запрошення на зустрічі та компрометацію облікових записів. Описано основні вектори атак, методи обходу багатофакторної автентифікації та типові сценарії соціальної інженерії. Запропоновано комплекс заходів захисту, що включає політики доступу, моніторинг аномальної активності, навчання персоналу та технічні обмеження зовнішніх комунікацій.

Ключові слова: фішинг, корпоративні комунікації, Slack, Microsoft Teams, Discord, соціальна інженерія, кібербезпека, MFA.

Корпоративні платформи обміну повідомленнями (Slack, Microsoft Teams, Discord) стали невід’ємною частиною бізнес-процесів сучасних організацій. Вони забезпечують швидкий обмін інформацією, спільну роботу над документами та інтеграцію з іншими сервісами. Водночас високий рівень довіри співробітників до внутрішніх каналів комунікації створює сприятливі умови для проведення цільових фішингових атак [1; 2].

Останніми роками спостерігається значне зростання кількості атак, у яких зловмисники використовують саме ці платформи. Групи на кшталт Scattered Spider, APT29 (Midnight Blizzard) та інші активно застосовують імперсонацію IT-підтримки, підроблені запрошення на зустрічі, компрометовані облікові записи та федеративні підключення [1; 3]. На відміну від класичного електронного листування, повідомлення в Slack чи Teams часто сприймаються як внутрішні та безпечні, що суттєво підвищує ймовірність успіху атаки.

Ймовірність успіху фішингової атаки через корпоративний месенджер можна оцінити як:

$$P_{success} = P_{click} \cdot P_{cred} \cdot (1 - P_{detect}) \tag{1}$$

де: $P_{success}$ – загальна ймовірність успішної компрометації;
 P_{click} – ймовірність того, що користувач перейде за шкідливим посиланням або відкриє повідомлення;
 P_{cred} – ймовірність надання облікових даних або підтвердження MFA;
 P_{detect} – ймовірність своєчасного виявлення атаки системами захисту.

Типові сценарії атак включають: (1) створення підроблених робочих просторів або оренду компрометованих тенантів Microsoft 365; (2) надсилання повідомлень від імені «IT Support» з проханням перейти за посиланням, підтвердити MFA-запит або встановити віддалений доступ; (3) використання функцій гостьового доступу та зовнішньої федерації; (4) розповсюдження шкідливих файлів через канали [2; 4].

Рівень ризику для організації від фішингу в месенджерах можна виразити формулою:

$$R = L \cdot I \cdot E \tag{2}$$

де: R – інтегральний рівень ризику;
 L – ймовірність (likelihood) реалізації загрози;
 I – потенційний вплив (impact) на конфіденційність, цілісність та доступність даних;
 E – коефіцієнт експозиції (exposure), що залежить від кількості користувачів платформи та наявності зовнішніх інтеграцій.

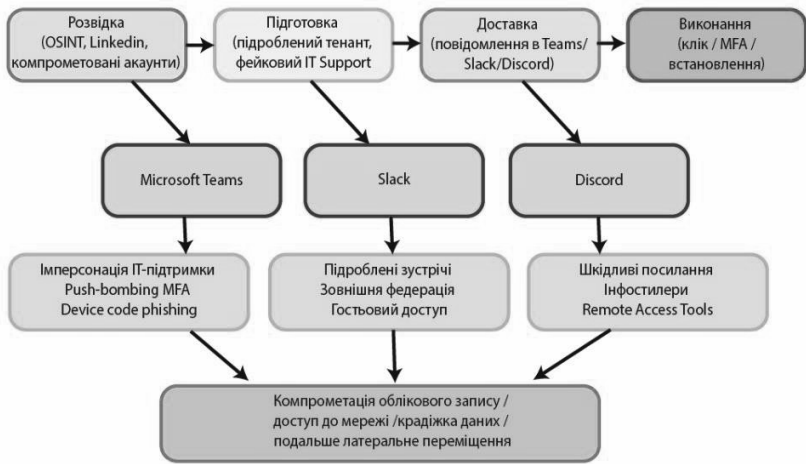


Рис. 1. Типова схема фішингової атаки в корпоративних месенджерах

На рис. 1 представлено типову схему фішингової атаки через корпоративні платформи комунікації. Атака складається з чотирьох основних етапів: розвідка (збір інформації про співробітників), підготовка інфраструктури (підроблені тенанти, фейкові акаунти IT-підтримки), доставка шкідливого повідомлення через Teams, Slack або Discord та виконання дій жертвою (перехід за посиланням, підтвердження MFA, встановлення remote access tools). Успішна реалізація призводить до компрометації облікового запису та подальшого латерального переміщення в корпоративній мережі.

Discord, хоча й менш поширений у великих корпораціях, активно використовується в IT-компаніях та стартапах. Тут фішинг часто маскується під запрошення до приватних серверів або оголошення про вакансії. Компрометація акаунтів через інфостилери дозволяє зловмисникам отримувати доступ до історії листування та токенів сесій [5, 7].

Для протидії зазначеним загрозам рекомендується комплексний підхід. Технічні заходи: обмеження зовнішніх комунікацій і гостьового доступу, Conditional Access, моніторинг аномальної активності, CASB та EDR. Організаційні заходи: регулярне навчання персоналу, чіткі процедури верифікації запитів IT-підтримки через альтернативні канали [3; 6].

Ефективність захисту значно підвищується при поєднанні технічних контролів з підвищенням обізнаності користувачів та впровадженням політики zero trust щодо повідомлень навіть від внутрішніх контактів.

Висновки. Фішинг у корпоративних середовищах комунікації Slack, Microsoft Teams та Discord становить зростаючу загрозу через високий рівень довіри користувачів до цих платформ. Зловмисники ефективно використовують соціальну інженерію, імперсонацію та технічні можливості платформ для обходу традиційних засобів захисту. Комплексний підхід, що поєднує технічні обмеження, моніторинг та навчання персоналу, є необхідною умовою зниження ризиків. Подальші дослідження доцільно спрямувати на розробку автоматизованих систем виявлення аномальної поведінки в корпоративних месенджерах.

Література

1. Noureen, R. (2025, July 31). Hackers infiltrate Microsoft Teams, Slack in phishing attacks. Petri. <https://petri.com/hackers-microsoft-teams-slack-phishing-attacks/>

2. Batchelor, B. (2026, August 20). Identity abuse through trusted communication channels. *Unit 42*. <https://unit42.paloaltonetworks.com/communication-channel-identity-risks/>

3. InsiderSecurity. (2025, June 23). *APT29 phishing attacks via Microsoft Teams: Tactics, techniques, and prevention*. <https://insidersecurity.co/apt29-midnight-blizzard-phishing-attacks-via-microsoft-teams-tactics-techniques-and-prevention/>

4. Mascellino, A. (2025, August 28). Fake IT support attacks hit Microsoft Teams. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/fake-support-attacks-hit-microsoft/>

5. InfoStealers. (2025, November 5). *Nikkei breached: Infostealer infection grants access to 17K+ employee Slack chat histories*. <https://www.infostealers.com/article/nikkei-breached-infostealer-infection-grants-access-to-17k-employee-slack-chat-histories/>

6. Microsoft. (2025, May 29). Defending against evolving identity attack techniques. *Microsoft Security Blog*. <https://www.microsoft.com/en-us/security/blog/2025/05/29/defending-against-evolving-identity-attack-techniques/>

7. Іванченко, Є., Шульга, В., Аверічев, І., & Дубровський, В. (2025). Класифікація та вплив кібератак, спрямованих на критично важливих постачальників послуг. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, Article 3. <https://doi.org/10.32782/IT/2025-2-3>

УДК 004.056:004.942

^{1,2}Хохлячова Ю. Є., ²Аскеров М.Г.

ДОКАЗОВО КЕРОВАНІЙ ЦИФРОВИЙ ДВІЙНИК ДЛЯ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СМАРТ-РЕГІОНУ

¹Державний торговельно-економічний університет, м. Київ

²Державний університет інформаційно-комунікаційних технологій, м. Київ
yuliiiahohlachova@gmail.com

Анотація. Запропоновано концептуальну модель доказово керованого цифрового двійника для оцінювання кіберстійкості взаємозалежних об’єктів критичної інфраструктури смарт-регіону. На відміну від статичних індексів, модель пов’язує якість кіберфізичних доказів із часовою траєкторією критичних функцій, прогнозом міжсекторного каскаду та вибором безпечних адаптивних дій. Смарт-регіон подано як часовий багатошаровий гіперграф, а довіру до телеметрії – як калібровану оцінку з жорсткими криптографічними предикатами й явною невизначеністю. Запропоновано місійно орієнтовану метрику стійкості з обмеженням компенсації життєво важливих функцій. Сформовано замкнений цикл «доказ – стан – прогноз – рішення – вимірний ефект», придатний для інтеграції з SIEM/SOAR, edge/fog та permissioned DLT.

Ключові слова: кіберстійкість, критична інфраструктура, смарт-регіон, цифровий двійник, кіберфізичні докази, каскадні відмови.

Цифровізація енергетики, водопостачання, транспорту та зв’язку формує систему систем, у якій порушення локального кіберфізичного контуру може трансформуватися у втрату регіональної критичної послуги. Класичний ризик-орієнтований захист переважно відповідає на запитання про ймовірність і наслідки окремої загрози, тоді як кіберстійкість охоплює здатність передбачати вплив, витримувати деградацію, відновлювати функцію та адаптуватися після інциденту [1]. Взаємозалежність інфраструктур ускладнює оцінювання, оскільки фізичні, інформаційні, кібернетичні й організаційні зв’язки утворюють часові каскади, що не зводяться до суми локальних відмов [2].

Безпека кіберфізичних систем залежить не лише від мережевого трафіку, а й від достовірності сенсорних вимірювань, стану виконавчих механізмів та узгодженості даних із фізичним процесом [3]. Цифровий двійник забезпечує синхронізоване подання фізичного об’єкта, його станів і сценаріїв «що-якщо» [4]. Permissioned DLT доцільно використовувати для незмінного походження доказів, кворумного аудиту та відтворюваності рішення, однак сам факт запису в реєстрі не доводить фізичної істинності показання сенсора [5]. Тому центральною задачею є поєднання криптографічної перевірки, процесної узгодженості, оцінки невизначеності та місійного наслідку в одному керованому контурі.

Метою роботи є формалізація такого контуру для смарт-регіону. Його базовим об’єктом є часова композиційна модель:

$$M_{SR}(t) = \langle O, F, L, D, E, \Theta, C, A, P, U, K \rangle,$$
 (1)

де O – об’єкти критичної інфраструктури; F – критичні функції; L – фізичний, кібернетичний, інформаційний, організаційний і сервісний шари; D – потоки даних; E – докази; Θ – загрози; C – контрзаходи; A – дії; P – політики; U – ресурси; K – обмеження функційної безпеки та авторизації. Замкнений цикл моделі показано на рис. 1.



Рис. 1. Замкнений контур доказово керованого забезпечення кіберстійкості смарт-регіону

Довірений evidence pipeline формує для кожного доказу є вектор $z_e(t) = [I, P, A, C, D, U]$, де I характеризує криптографічну цілісність, P – походження та атестацію, A – свіжість і доступність, C – контекстну узгодженість, D – незалежність джерела, U – невизначеність. Підсумкова оцінка визначається за виразом:

$$\hat{t}_e(t) = H_e(t)[1 - U_e(t)] \sum_{k \in \{I, P, A, C, D\}} \omega_k(t) z_{e,k}(t), \sum_k \omega_k(t) = 1.$$
 (2)

Бінарний предикат $H_e(t)$ дорівнює нулю за невалідного підпису, відкликаного ключа, порушення послідовності або невідповідності атестації; такі порушення не можуть бути компенсовані високими значеннями інших ознак. Ваги $\omega_k(t)$ не задаються раз і назавжди, а калібруються для сектора й режиму функціонування за еталонними трасами, після чого контролюються за Brier score, expected calibration error та покриттям інтервалів. У такий спосіб DLT-якоріння виконує роль доказу походження, а фізична правдоподібність встановлюється через робастне злиття різнорідних джерел і процесні інваріанти.

Стан кіберзахисту оцінюється через збереження критичної функції, а не через сам факт наявності механізмів безпеки. Для функції f на інтервалі [0, T] вводиться нормована метрика:

$$R_f[0, T] = 1 - \frac{\int_0^T L_f(t) dt}{T L_{f, \max}},$$
 (3)

де $L_f(t)$ – втрата якості або доступності сервісу, $L_{f, \max}$ – максимально допустима шкала втрати. Значення $R_f = 1$ відповідає відсутності втрат, а зростання площі деградації монотонно зменшує оцінку. Щоб середнє значення не приховувало неприйнятний стан життєво важливої функції, регіональна агрегація має бар’єр компенсації:

$$R_{SR} = (\sum_{f \in F} w_f R_f) \prod_{f \in F_{crit}} \min \left\{ 1, \frac{R_f}{\tau_f} \right\}, \sum_f w_f = 1.$$
 (4)

Тут w_f відображає критичність функції, τ_f – мінімально прийнятний рівень для множини F_{crit} . Якщо хоча б одна життєво важлива функція опускається нижче свого порога, мультиплікативний множник знижує інтегральну оцінку незалежно від високих значень інших сервісів. Це усуває компенсаційний ефект звичайного зваженого середнього.

Таблиця 1 – Функції блоків доказово керованого циклу та критерії їх перевірки

Блок	Основні дані й операції	Результат	Критерій перевірки
Evidence pipeline	Підпис, attestation, provenance, часові мітки, процесні інваріанти	Калібрована довіра до доказу	Brier/ECE, FPR, покриття інтервалу
Цифровий двійник	Стани функцій, ресурси, резерви, міжсекторні залежності	Узгоджена оцінка поточного стану	Похибка стану, синхронізація, out-of-sample
Прогноз каскаду	Напрямы, затримка, поріг, резерв, довіра до залежності	Шлях, розмір і час поширення	Forecast error, coverage, backtesting
Контролер рішень	Місійна втрата, час, ресурс, ризик, ролі, rollback	Оборотна safety-обмежена дія	Нуль unsafe-дій, authorization, час відкату
Зворотний зв’язок	Телеметрія після дії, фактична втрата, відхилення прогнозу	Оновлення twin і калібрування	Відтворюваний decision record

Прогнозний модуль цифрового двійника поширює локальне порушення через часові гіперребра з параметрами напряму, затримки, порога спрацювання, резерву та довіри до самої залежності. Принципово розрізняються фізичне перенесення дефіциту, кібернетичне поширення через спільну мережу, інформаційне зараження хибними даними й організаційна затримка рішень. Результатом є не лише ймовірність інциденту, а прогноз траєкторії втрати сервісу та доступного часового вікна для локалізації каскаду.

Контролер кіберстійкості вибирає політику карантину, сегментації, rate limiting, перемаршрутизації, резервування або переходу в деградований режим. Оптимізаційна постановка має вигляд:

$$\pi = \underset{\pi}{argmin} E[J_{loss} + \lambda_1 J_{time} + \lambda_2 J_{cost} + \lambda_3 J_{risk}],$$
 (5)

$$g_{\text{safety}}(\pi) \leq 0, g_{\text{resource}}(\pi) \leq 0, g_{\text{auth}}(\pi) = \text{true.} \quad (6)$$

Функціонал J_{loss} визначається площею місійної втрати та критичністю уражених функцій; J_{time} враховує затримку виявлення і відновлення; J_{cost} – обчислювальні, мережеві та організаційні витрати; J_{risk} – імовірність побічного фізичного ефекту. Автоматичний контур допускає лише оборотні дії класу карантину, обмеження швидкості, reroute або failover у попередньо затверджених межах. Фізично значущі й незворотні операції залишаються в контурі оператора та потребують подвійного погодження, interlock і попередньої перевірки в цифровому двійнику або NPL-середовищі.

Практична реалізація передбачає чотири взаємопов’язані шари. На OT/IoT-рівні формуються підписані й канонікалізовані вимірювання; edge/fog виконує ранню перевірку, буферизацію та робастне злиття; permissioned DLT фіксує мінімальний доказ походження і версію політики; регіональний digital twin синхронізує стан критичних функцій та передає перевірені події до SIEM/SOAR і policy engine. Для кожного рішення зберігається decision record: первинні докази, оцінка стану, прогноз каскаду, альтернативні політики, авторизація, виконана дія, фактичний ефект і можливість відкату.

Перевірка моделі повинна бути багаторівневою. Формальні властивості safety, liveness, authorization і no-deadlock встановлюються model checking. Далі застосовуються дискретно-подійне моделювання, мережеве емулявання з реальним messaging stack, порівняння щонайменше двох permissioned DLT та hardware-in-the-loop. Обов’язковими є сильні baseline конфігурації: security stack без DLT, DLT без контекстної довіри, доменний IDS або робастний оцінювач стану, а також абляції provenance, uncertainty, digital twin і controller. Первинними показниками доцільно визначити area of loss, MTTR, p95/p99 latency, F1/FPR, похибку прогнозу каскаду, кількість safety-порушень і час відкату. Числові переваги можуть заявлятися лише після незалежних трас, довірчих інтервалів та ресурсно чесного порівняння.

Сценарна перевірка повинна охоплювати модифікацію даних після підписання, валідно підписані неправдиві показання, replay і clock drift, компрометацію edge-шлюзу, DDoS разом із легітимним flash crowd, network partition, втрату кворуму, Byzantine validator, скоординовану компрометацію сенсорного кластера та міжсекторний каскад. Активні впливи допускаються лише в ізольованому стенді або NPL-контурі; відкриті набори даних мають бути синтетичними, агрегованими чи деідентифікованими та не містити реальних топологій, правил доступу або параметрів захисту об’єктів критичної інфраструктури.

Умови застосовності. За конструкцією метод забезпечує п’ять контрольованих властивостей: простежуваність рішення від первинного доказу до фактичного ефекту; некомпенсаційність оцінки щодо життєво важливих сервісів; обмежену автономність із поділом дій на оборотні й фізично значущі; декомпозицію внеску provenance, edge, IDS, DLT, digital twin і controller; відтворюваність через версіонування політик, конфігурацій, насінин і журналів. Межі перенесення визначаються якістю калібрування, повнотою моделі залежностей, часовою синхронізацією та відповідністю NPL-процесу реальному сектору.

Наукова новизна запропонованого підходу полягає в інтеграції трьох раніше роз’єднаних контурів: довіри до кіберфізичного доказу, місійної динаміки взаємозалежних критичних функцій і формально безпечного синтезу дій. Метрика R_{SR} є некомпенсаційною щодо життєво важливих сервісів; evidence pipeline не ототожнює незмінність реєстру з фізичною істинністю; контролер оцінює не лише локальний incident score, а очікувану регіональну втрату та каскадний ефект.

Висновки. Сформовано концептуальну й формальну основу доказово керованого цифрового двійника кіберстійкості смарт-регіону. Запропоновано часову системно-системну модель, калібровану оцінку довіри з жорсткими предикатами, місійний показник із бар’єром компенсації та safety-обмежену оптимізацію адаптивних дій. Підхід забезпечує простежуваність від первинного доказу до виміряного ефекту, дозволяє прогнозувати міжсекторні каскади та відокремлює внесок DLT від edge-фільтрації, IDS і цифрового двійника. Подальше дослідження має бути спрямоване на калібрування параметрів, формальну верифікацію та багаторівневу експериментальну перевірку на незалежних сценаріях.

Література

1. Linkov I., Bridges T., Creutzig F. et al. Changing the resilience paradigm. Nature Climate Change. 2014. Vol. 4, No. 6. P. 407–409. DOI: 10.1038/nclimate2227.
2. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety. 2014. Vol. 121. P. 43–60. DOI: 10.1016/j.res.2013.06.040.
3. Humayed A., Lin J., Li F., Luo B. Cyber-Physical Systems Security—A Survey. IEEE Internet of Things Journal. 2017. Vol. 4, No. 6. P. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.
4. Minerva R., Lee G. M., Crespi N. Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models. Proceedings of the IEEE. 2020. Vol. 108, No. 10. P. 1785–1824. DOI: 10.1109/JPROC.2020.2998530.
5. Makhdoom I., Abolhasan M., Abbas H., Ni W. Blockchain’s adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications. 2019. Vol. 125. P. 251–279. DOI: 10.1016/j.jnca.2018.10.019.

ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ТЕОРЕТИКО-МНОЖИННОЇ МЕТРИЧНОЇ МОДЕЛІ

¹ Державний університет інформаційно-комунікаційних технологій

² Державний торговельно-економічний університет
agkorchenko@gmail.com, yuliiiahohlachova@gmail.com

Анотація. Розглянуто проблему формалізованого оцінювання кіберстійкості об’єктів критичної інфраструктури (ОКІ) в умовах зростаючої складності кіберзагроз. Визначено, що існуючі підходи характеризуються фрагментарністю та відсутністю строгого зв’язку між базовими заходами кіберстійкості та метриками їх оцінювання. Метою дослідження є розроблення теоретико-множинної метричної моделі (ТМММ), яка забезпечує формалізацію множини можливих метрик (МММ) для кожного базового заходу (БЗ). Запропоновано формальне представлення множини метрик як функції від БЗ та способів його реалізації, введено поняття кардинальності множини метрик та обґрунтовано її залежність від контексту застосування. Запроваджено розмежування структурних (ex-ante) та операційних (ex-post) метрик у межах єдиної математичної конструкції, а також побудовано функціональне відображення «БЗ → МММ». Показано, що для одного заходу може існувати декілька метрик різної природи (зовнішні, універсальні, локальні). Отримані результати забезпечують перехід від описових оцінок до формалізованого кількісного оцінювання кіберстійкості, створюють основу для побудови інтегральних показників та автоматизації процесів аналізу.

Ключові слова: кіберстійкість, оцінювання кіберстійкості, об’єкти критичної інфраструктури, метрики кіберстійкості, theoretical-set model, MITRE CREF, інформаційна безпека, кібербезпека, захист інформації.

Вступ та актуальність роботи. Сучасні об’єкти критичної інфраструктури (ОКІ) функціонують у довкіллі постійних та високоадаптивних кіберзагроз, що вимагає переходу від класичних моделей забезпечення інформаційної безпеки до концепції кіберстійкості (cyber resilience) як здатності системи підтримувати функціональність та швидко відновлюватися в умовах деструктивного впливу. Водночас наявні підходи до оцінювання кіберстійкості мають фрагментарний характер та не забезпечують формалізованого зв’язку між базовими заходами (БЗ), підходами їх реалізації та відповідними метриками.

Актуальність дослідження зумовлена такими основними чинниками:

1. Відсутністю формалізованого зв’язку між БЗ кіберстійкості та відповідними метриками їх вимірювання.
2. Методологічною невизначеністю у формуванні формалізованих систем кількісного оцінювання.
3. Потребою автоматизації процесів оцінювання кіберстійкості в умовах цифрової трансформації ОКІ та зростання кардинальності множини загроз.
4. Необхідністю інтеграції структурних (ex-ante) та операційних (ex-post) характеристик реалізації заходів.
5. Вимогами сучасних міжнародних регуляторних підходів до доказовості, порівнюваності та відтворюваності результатів оцінювання.

Постановка завдання. Метою дослідження є розроблення теоретико-множинної метричної моделі (ТМММ) оцінювання кіберстійкості ОКІ, що формалізує множину можливих метрик (МММ) для кожного БЗ та забезпечує математичну основу для побудови інтегральних показників резильєнтності.

Для досягнення поставленої мети необхідно сформувати та виконати такі наукові завдання:

1. Формалізувати МММ для кожного базового заходу кіберстійкості.
2. Визначити кардинальність множини метрик та її залежність від аргументів реалізації.
3. Ввести розмежування структурних (ex-ante) та операційних (ex-post) метрик у межах єдиної математичної конструкції.
4. Побудувати функціональне відображення «БЗ → МММ».
5. Запропонувати узагальнену ієрархічну метричну конструкцію та верифікувати її узгодженість із міжнародним фреймворком MITRE Cyber Resiliency Engineering Framework (CREF).

Аналіз останніх досліджень і публікацій. Аналіз наукових праць і нормативних документів (MITRE CREF, NIST CSF 2.0, NIST SP 800-160, DORA) свідчить про наявність розвиненої концептуальної та рамкової бази [1–4]. Зокрема, у працях D. Bodeau та R. Graubart [1–3] наведено широку таксономію цілей, продуктів та методів вимірювання кіберстійкості. Водночас наявні підходи обмежуються описовими конструкціями або експертним скорингом без жорсткої математичної прив’язки метрик до інтегрального рівня стійкості.

Дослідження [5–10] пропонують ризик-орієнтовані та сценарні моделі оцінювання, проте вони часто зводяться до класичних показників доступності (MTTR, availability) та не враховують специфіку доказовості цілісності (provenance, integrity evidence). Праці [11–20] висвітлюють проблеми критичності та залежностей, але не визначають уніфікованої математичної структури для узгодження різнорідних метрик. Роботи [21–38] формують базу для нормалізації та сценарного оцінювання, підтверджуючи існування методологічного розриву між високорівневими фреймворками та формальними математичними моделями вимірювання.

Основна частина дослідження. Для побудови TMMM використано теоретико-множинний підхід. Введено множину ідентифікаторів цілей забезпечення кіберстійкості: $GS = \{gs_1, gs_2, ..., gs_m\}$, де m – кількість цілей. Структура параметрів описується теоретико-множинною моделлю даних (TММД):

$$OS = \{ (gs_i, \{ (ts_ij, \{ (sts_ijk, f_ijk(a_ijk1, ..., a_ijkn)) \}_{k=1^K_ij}) \}_{j=1^J_i}) \}_{i=1^M},$$

де ts_ij – i -а задача, sts_ijk – j -а підзадача, f_ijk – функція реалізації базового заходу (БЗ), a_ijk – аргументи реалізації (технічні рішення, підходи, методи).

Для реалізації процесів вимірювання введено множину $M_ijk(a_ijk)$ можливих метрик (MMM). Узагальнена TMMM набуває вигляду:

$$M_ijk(a_ijk) = \{ m_ijk1(a_ijk1), m_ijk2(a_ijk2), ..., m_ijk, m_ijk(a_ijk, m_ijk) \},$$

де m_ijk – кардинальність множини метрик для оцінювання k -го БЗ. Показано, що кардинальність є змінною величиною (від 1 до 11 метрик у реальних сценаріях) і залежить від контексту застосування та способів реалізації.

Приклад структурованого відображення TMMM/ У таблиці 1 наведено фрагмент ієрархічної індексації та відповідності між БЗ, аргументами реалізації та метриками різної природи (зовнішні, універсальні, локальні).

i (Ціль)	j (Задача)	k (БЗ)	q (Метрика)	Позначення метрики	Опис (контекст) метрики
1	1	1	1	PA.S1.A1.M1 (PR,S)	Відсоток кіберресурсів, доступ до яких контролюється на основі критичності
1	1	1	2	PA.S1.A1.M2 (PR,S)	Відсоток кіберресурсів, доступ до яких контролюється на основі чутливості
1	1	2	1	PA.S1.A2.M1 (PR)	Відсоток користувачів, для яких поведінка обмежена на основі ступеню довіри
3	1	1	1	CN.S1.A1.AM-DA-1	Час, витрачений на оцінювання пошкоджень у місії після початку CCoA
6	1	1	1	UN.S1.A1.M1 (AM,CA)	Кількість потоків інформації про загрози (ТИ), які використовує організація

Практична апробація на сценарії фішингової атаки. Функціонування моделі апробовано на прикладі сценарію фішингової атаки на банківську установу:

- Для цілі = ANT (Передбачати) та БЗ UN.S1.A1(AM,CA) вимірюються показники роботи з Threat Intelligence (ТИ). Зокрема, метрика UN.S1.A1.M1 = 4 визначає кількість незалежних джерел ТІ (CERT-UA, FS-ISAC, ТІ-провайдер тощо), а UN.S1.A1.3 = 25 хв – час оцінки релевантності даних.
- Для цілі = WITH (Витримувати) та БЗ CN.S1.A1(AM,CA,SI) оцінюється час оцінювання пошкоджень місії (CN.S1.A1.AM-DA-1 = 3?5 год) та відсоток перевірених критичних даних (CN.S1.A1.M1 = 70%).
- Для цілі = REC (Відновлюватися) та БЗ RE.S1.A2(AM,SI) вимірюється відновлення довіри до даних (RE.S1.A2.SI-IC-2 = 90% підтверджених критичних записів).

- Для цілі = AD (Адаптуватися) та БЗ TR.S2.A2(R,CP) аналізується усунення єдиних точок відмови (SPOF) та оптимізація привілейованого доступу (TR.S2.A2.M2 = 75% переглянутих прав).

Обговорення та практичне значення. Запропонована TMMM усуває методологічний розрив між концептуальними фреймворками та практичними системами вимірювання. Основні переваги моделі:

- Забезпечення строгого відображення «БЗ → MMM», що виключає суб’єктивізм експертних оцінок.
- Одночасне розмежування та врахування структурних (ex-ante) і операційних (ex-post) метрик.
- Масштабованість та можливість інтеграції в SIEM/SOC-платформи для автоматизованого моніторингу.

Висновки. У результаті дослідження розв’язано наукову задачу розроблення теоретико-множинної метричної моделі оцінювання кіберстійкості OKI:

- Формалізовано MMM для кожного базового заходу, що забезпечило перехід від фрагментарних оцінок до системної формалізованої конструкції.
- Визначено та обґрунтовано залежність кардинальності множини метрик (від 1 до 11) від аргументів реалізації та контексту безпеки.
- Запроваджено розмежування структурних (ex-ante) та операційних (ex-post) метрик, що забезпечує комплексність оцінювання підготовленості та реальної поведінки системи під час атак.
- Побудовано функціональне відображення «БЗ → MMM» та підтверджено узгодженість модельних конструкцій із міжнародним фреймворком MITRE CREF.

Література

- Bodeau D., Graubart R., McQuaid R., Woodill J. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. MITRE Technical Report, 2018.
- Bodeau D., Graubart R. Cyber Resiliency Engineering Framework. MITRE Corporation Technical Report MTR110237, 2011.
- Bodeau D., Brtis J., Graubart R., Salwen J. Cyber Resiliency Engineering Aid. MITRE Technical Report MTR150264, 2015.
- Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST SP 800-160, Vol. 2, Rev. 1, 2021.
- Linkov I., Eisenberg D. A., Plourde K. et al. Resilience metrics for cyber systems. Environment Systems and Decisions, 2013, 33(4), pp. 471-476.
- Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. Springer, 2015, pp. 311-316.
- Cam H., Mouallem P., Mo J., Farris J. Resilience metrics for cyber systems. INCOSE International Symposium, 2016, 26(1), pp. 1476-1489.
- Linkov I., Kott A. Cyber Resilience of Systems and Networks. Springer, Cham, 2019.
- Zio E. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliability Engineering & System Safety, 2016, 152, pp. 137-150.
- Petersen L., Fallou L., Reilly P., Serafinelli E. A resilience assessment framework for critical infrastructure. IJCIP, 2019, 25, pp. 1-14.
- Yusta J. M., Correa G. J., Lacal-Arántegui R. Methodologies and applications for critical infrastructure protection: State-of-the-art. Energy Policy, 2011, 39(10), pp. 6100-6119.
- Rinaldi S. M., Peerenboom J. P., Kelly T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 2001, 21(6), pp. 11-25.
- Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. RESS, 2014, 121, pp. 43-60.
- Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. IJCIP, 2015, 8, pp. 53-66.
- Musman S., Temin A. A cyber mission impact assessment tool. IEEE HST, 2015, pp. 1-7.
- Falco G., Caldera C., Shrobe H. IIoT cybersecurity risk modeling for SCADA systems. IEEE IoT Journal, 2018, 5(6), pp. 4486-4495.
- Haque M. A., Shetty S., Krishnappa B. Cybersecurity resilience model for industrial control systems. IET Cyber-Physical Systems, 2020, 5(3), pp. 271-282.
- Jackson S., Ferris T. L. Resilience principles for engineered systems. Systems Engineering, 2013, 16(2), pp. 152-164.

19. Rieger C., Gertman D., McQueen M. Resilient control systems: Next generation design research. IEEE HSI, 2009, pp. 632-636.

20. Woods D. D. Four concepts for resilience and the implications for the future of resilience engineering. RESS, 2015, 141, pp. 5-9.

21. Stergiopoulos G. et al. Time-based critical infrastructure dependency analysis. IJCIP, 2016, 12, pp. 46-60.

22. Hossain M. S. et al. Big data-driven service composition using parallel clustered PSO. IEEE TSC, 2014, 9(5), pp. 806-817.

23. Teixeira A. et al. A secure control framework for resource-limited adversaries. Automatica, 2015, 51, pp. 135-148.

24. Vugrin E. D. et al. A framework for assessing the resilience of infrastructure and economic systems. 2010, pp. 77-116.

25. Hosseini S. et al. A review of definitions and measures of system resilience. RESS, 2016, 145, pp. 47-61.

26. Ganin A. A. et al. Operational resilience: concepts, design and analysis. Scientific Reports, 2016, 6(1), p. 19540.

27. Amin M. Energy infrastructure defense systems. Proceedings of the IEEE, 2005, 93(5), pp. 861-875.

28. Pursiainen C. Critical infrastructure resilience: A Nordic model in the making? IJDRR, 2018, 27, pp. 632-641.

29. Theocharidou M. et al. A multi-layer criticality assessment methodology based on interdependencies. Computers & Security, 2016, 62, pp. 251-272.

30. Giannopoulos G. et al. Risk assessment methodologies for critical infrastructure protection. JRC Technical Report, 2012.

31. Setola R. et al. Managing the Complexity of Critical Infrastructures. Springer, 2016.

32. NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 2024.

33. NIST. Integrating Cybersecurity and Enterprise Risk Management (ERM) (IR 8286 Rev. 1), 2025.

34. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). OJ L 333, 2022.

35. MITRE Corporation. Cyber Resiliency Engineering Framework (CREF) Navigator, 2024.

36. AlHidaifi A. et al. Simulation-Based Quantification of Cyber Resilience for Critical Systems. Decision Support Systems, 2024, Vol. 178.

37. Lezzi M. et al. Measuring Cyber Resilience in Industrial IoT: A Systematic Review. SOCA, 2025.

38. Cho H. et al. A Quantitative Framework for Cyber Resilience Assessment with Normalization Techniques. Electronics, 2025, 14(12).

УДК 159.98:331.108.2:355

Костюніна О. В.

КІБЕРБЕЗПЕКА ТА ЦИФРОВА СУПЕРВІЗІЯ: АНАЛІЗ РИЗИКІВ ТА ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ІІІ-СИМУЛЯЦІЙ У ПІДГОТОВЦІ ПСИХОЛОГІВ

Державний університет інтелектуальних технологій і зв’язку
favoritelna09@gmail.com

Анотація. У тезах досліджено проблематику захисту інформації та забезпечення кібербезпеки під час інтеграції генеративного штучного інтелекту (LLM-моделей) в освітній простір. На основі результатів формуючого експерименту, проведеного в межах дисертаційного дослідження автора на виділеній групі практикуючих психологів (n=45), проаналізовано амбівалентність використання ІІІ-клієнтів як безризикових симуляційних платформ. Проведено контент-аналіз рефлексивних есе фахівців за авторською кодувальною матрицею, який виявив латентні загрози екранної деперсоналізації та витоку конфіденційних клінічних даних. Обґрунтовано модель захисту персональних даних та алгоритм безпечного промпт-інжинірингу для впровадження у практикум для магістрантів у новому навчальному році.

Ключові слова: кібербезпека, штучний інтелект, промпт-інжиніринг, захист персональних даних, контент-аналіз, цифрова супервізія, ОІПОПІ, формуючий експеримент.

Постановка проблеми. Стрімка цифровізація психологічної практики та вищої освіти в Україні актуалізує критичні виклики у сфері кібербезпеки та захисту інформації. Згідно з Постановою Кабінету Міністрів України від 06.08.2026 р. № 993 «Про затвердження Положення про супервізію», інструменти супервізійної та інтерв'язійної підтримки стають обов'язковими для практикуючих фахівців у сфері психічного здоров'я. Інноваційним кроком у розв'язанні проблеми «синдрому початківця» та адаптації до нових

нормативних вимог є використання штучного інтелекту (ІІІ) як безризикового симулятора клієнта. Проте текстова взаємодія з LLM-моделями у межах хмарних обчислень створює латентні канали витоку конфіденційної інформації, деперсоналізації даних та уразливості критичної інформаційної інфраструктури ЗВО, що потребує превентивного моделювання безпечного освітнього середовища.

Аналіз останніх досліджень і публікацій. Фундаментальні моделі супервізії описані в працях П. Говкінса та Р. Шохета. Теоретичні засади психологічного наставництва та формування професійної ідентичності в Україні досліджували С. Максименко, І.Іщенко І., М.Кононець, О.Большая, Г.Люлька, М. Мушкевич, Н. Гусак, В. Онуфрієва, а також, О. Костюніна у контексті дискурсивно-графічної рефлексії. Базис організації групової динаміки спирається на праці К. Левіна та І. Ялома. Трансформаційна роль генеративного ІІІ в клінічній практиці аналізується у працях Б. Грау, а готовність до використання ІІІ — у розвідках О. Ключка та В. Ковальчука. Проте синергетичне поєднання кібербезпеки, ІІІ-симуляцій та Т-групової динаміки у межах підготовки магістрантів залишається невідомим.

Мета дослідження — на основі емпіричних даних дисертаційного дослідження автора здійснити якісний контент-аналіз ризиків використання ІІІ-симуляцій та обґрунтувати безпекову модель кіберзахисту персональних даних для впровадження у запланований навчальний практикум кафедри кіберпсихології та реабілітації.

Методологічну основу роботи складають результати **формуючого експерименту, проведеного в межах дисертаційного дослідження автора на виділеній групі практикуючих психологів (n=45)**. На вхідному та вихідному етапах експерименту було застосовано:

1. *Опитувальник дослідження професійної ідентичності (ОІПОПІ)* (О. В. Костюніна та С. М. Симоненко) для диференціації когнітивного (ІІКгн), автономного (ІІПавт) та інтегрального (ІІІнт) рівнів «Я».
2. *Дискурсивно-графічний тест (ДГТ)* (О. В. Костюніно) з метою детекції латентних афектів та потреби в безпеці (*маркери «ЗАМ», «СТО»*).
3. *Ольденбурзький опитувальник вигорання (OLBI)* Е. Демеруті для фіксації рівнів емоційного виснаження та деситуативності фахівців.

На проміжному етапі психологи взаємодіяли з ІІІ-клієнтом за захищеним авторським промптом. (Приклад: *«Дій як клієнт на прийомі у психолога. Твоє ім'я — Олена, 28 років. Твій запит: підвищена тривожність через зміну роботи. Не видавай усю інформацію одразу, демонструй легкий опір...»*). Після сесій транскрипти діалогів піддавалися якісному контент-аналізу. Розроблена за результатами дисертації модель покладена в основу нового навчального курсу «Коучинг психолога-початківця», який запускається на кафедрі кіберпсихології та реабілітації з початку найближчого навчального року.

Результати дослідження та їх обговорення. Впровадження розробленого інноваційного практикуму в межах формуючого експерименту на виділеній групі практикуючих психологів (n=45) дозволило зафіксувати виражену позитивну динаміку розвитку їхньої професійної суб'єктності та стійкості. Емпірична оцінка ефективності запропонованої моделі базувалася на зіставленні кількісних показників вхідного і вихідного зрізів, а також на якісному проміжному контент-аналізі рефлексивних звітів.

Кількісні результати перерозподілу статусів професійної ідентичності (за методикою ОІПОПІ, О. В. Костюніна та С. М. Симоненко) та рівнів професійного вигорання фахівців (за опитувальником OLBI Е. Демеруті) систематизовано й представлено у таблиці 1.

Таблиця 1. Динаміка показників професійного становлення та стійкості психологів у межах формуючого експерименту (n=45)

№ з/п	Психодіагностичний критерій (параметр виміру)	До впровадження практикуму (%)	Після впровадження практикуму (%)	Статистичний вектор змін
1	Когнітивний та дифузний статуси (ІІКгн) за ОІПОПІ	72%	24%	↓ 48% (критичне зниження)
2	Автономний та інтегральний статуси (ІІПавт), (ІІІнт) за ОІПОПІ	28%	76%	↑ 48% (вихід на рівень суб'єктності)
3	Високий ризик дезадаптації та демеутрії (виснаження за OLBI Е. Демеруті)	69%	15%	↓ 54% (емоційна стабілізація)
4	Професійна самоефективність та резильєнтність (субшкала OLBI)	31%	85%	↑ 54% (інтеграція Я-концепції)

Якісний аналіз проміжного етапу взаємодії з ІІІ-симулятором клієнта здійснювався за допомогою контент-аналізу рефлексивних есе. Виділені смислові одиниці (коди) були категоризовані за методологічною схемою авторки на чинники полегшення практики (ресурси) та суб'єктивні бар'єри. Частотний розподіл зафіксованих кодів представлено в таблиці 2.

Таблиця 2. Кодувальна матриця якісного контент-аналізу сприйняття ІІІ-клієнтів (n=45)

Код аналізу	Назва виділеного семантичного коду (Смислові домінанти звітів)	Категоріальний вектор маркерів	Частота фіксації у звітах (%)
Код А.1	Безпека полігону та інваріантність помилки	Полегшення практики / Цифровий ресурс	42%
Код Б.1	Дефіцит сенсорно-невербальних маркерів	Складність / Обмеження каналу зв'язку	38%
Код А.2	Дидактична пауза та тайм-аут для рефлексії	Полегшення практики / Ресурс обробки	35%
Код Б.2	Гіперкомплаєнтність та лінійність ІІІ	Складність / Бар'єр алгоритму	32%
Код Б.3	Екранно-текстова депресоналізація	Складність / Ризик захисного регресу	30%
Код А.3	Варіативність нозологічних запитів	Полегшення практики / База симуляцій	23%

Зіставлення даних таблиці 1 та таблиці 2 унаочнює унікальний психологічний ефект: штучний інтелект діє як ідеальний безризиковий «буфер», повністю нівелюючи первинний страх нашкодити клієнту (Код А.1 — 42%). Водночас вираженість Коду Б.1 (38%) та Коду Б.3 (30%) підтверджує нашу гіпотезу: цифрова супервізія не може бути самодостатньою. Вона виступає пропедевтичним містком до живих інтерв'їзійних Т-груп за моделлю І. Ялома, де депресоналізація екологічно долається через реальну групову динаміку «тут-і-тепер». З погляду захисту інформації, головна загроза криється у транскриптах діалогів. Студенти, намагаючись деталізувати ІІІ-клієнта, схильні завантажувати у хмарні комерційні платформи елементи реальних анамнестичних карт живих пацієнтів, що створює прецедент витоку конфіденційних даних за межі інформаційного контуру держави.

Проективна експресія за Дискурсивно-графічним тестом ДГТ (О. В. Костюніна) на виході зафіксувала повну трансформацію латентних афектів у чіткі інтегральні структури кордонів «Я» фахівця за умов 100% кіберзахисту інфо Аналіз даних унаочнює, що ліквідація страху помилки (Код А.1 — 42%) супроводжується ризиком екранної деперсоналізації (Код Б.3 — 30%), що вимагає обов'язкового виходу з ІІІ-сесії у живі Т-групи на основі класичної моделі І. Ялома для відновлення емоційного резонансу.

Для запобігання цим загрозам пропонується трирівневий протокол цифрової гігієни:

1. Анонімізація вхідного промпту (виключення біографічних збігів).
 2. Локалізація обчислень (запуск Open-Source моделей Llama-3 чи Mistral виключно на внутрішніх локальних серверах ЗВО фреймворком Ollama без виходу логів сесії у глобальні хмари).
 3. Хешування та деідентифікація транскриптів перед груповою інтерв'їзією.
- Впровадження цього протоколу дозволило підняти рівень автономної ідентичності студентів (за ОІПОПІ) на виході до **76%**, а рівень самоефективності (за OLBI) зріс на **54%** за умови стовідсоткової безпеки інформації.

Висновки.

1. У дослідженні теоретично обґрунтовано та практично верифіковано інноваційну модель цифрової супервізії в межах формуючого експерименту на виділеній групі практикуючих психологів (n=45). Доведено, що класична лекційно-шаблонна підготовка в ЗВО провокує когнітивну ригідність та страх перед реальною практикою. Синергетична інтеграція засобів EdTech та групової динаміки дозволяє подолати цей бар'єр, трансформуючи академічні знання у зрілу суб'єктну позицію фахівця, що є прямим виконанням державних вимог Постанови КМУ № 993 від 06.08.2026 р. Використання ІІІ-симуляцій у підготовці психологів є потужним інструментом EdTech, який знижує професійну тривожність, але потребує жорсткої регламентації з погляду кібербезпеки.
2. На основі кількісних даних (Таблиця 1) доведено високу ефективність розробленої моделі практикуму для стимулювання професійного розвитку. Фінальний зріз зафіксував статистично достовірне зниження когнітивного та дифузного статусів ідентичності (за опитувальником ОІПОПІ) на 48% з одночасним виходом 76% учасників на автономний та інтегральний рівні професійного «Я». Паралельно зафіксовано зниження ризиків емоційного виснаження на 54% та зростання професійної самоефективності до 85% (за шкалою OLBI), що підтверджує превентивну реабілітаційну цінність підходу.
3. За результатами якісного контент-аналізу (Таблиця 2) визначено екологічні межі застосування штучного інтелекту в супервізійному процесі. Домінування Коду А.1 («Безпека полігону та інваріантність помилки» — 42%) підтверджує роль ІІІ як безпечного симуляційного середовища. Водночас вираженість Коду Б.1 («Дефіцит сенсорно-невербальних маркерів» — 38%) та Коду Б.3 («Екранно-текстова депресоналізація» — 30%) доводить неможливість ізольованого використання LLM-моделей і вимагає обов'язкового логічного переходу до живих Т-груп за моделлю І. Ялома та проективної детекції меж «Я» за тестом ДГТ.
4. Обґрунтований у роботі трирівневий протокол цифрової гігієни (анонімізація промптів, локалізація обчислень Open-Source моделей на внутрішніх серверах ЗВО та токенизація логів) гарантує 100% захист персональних даних пацієнтів від витоку в комерційні хмари. Розроблена дидактична матриця

повністю підготовлена до інтеграції в новий навчальний курс для магістрантів на кафедрі кіберпсихології та реабілітації з початку найближчого навчального року. Запропонований протокол локалізації обчислень та анонімізації промптів мінімізує ризики витоку інформації та захищає персональні дані в умовах нових нормативних вимог України (Постанова КМУ № 993).

Література

1. Про систему охорони психічного здоров'я в Україні : Закон України від 15.01.2025 р. № 4223-ІХ. *Відомості Верховної Ради України*. 2025. URL: <https://zakon.rada.gov.ua/laws/show/4223-20#Text>

2. Про затвердження Положення про супервізію: Постанова Кабінету Міністрів України від 06.08.2026 р. № 993. *Офіційний вісник України*. 2026. <https://zakon.rada.gov.ua/laws/show/993-2026-%D0%BF#Text>

3. Іщенко І., Кононец Н., Большая О., Люлька Г. Освітній консалтинг у парадигмі сучасного управління закладами вищої освіти. Адаптивне управління: теорія і практика. Серія Економіка. 2025. № 20(40). URL: <https://amtp.org.ua/index.php/journal2/article/view/764>

4. Мушкевич М. І.Супервізія : навчальний посібник (до курсу «Супервізія»). Луцьк:Вежа-Друк, 2022.188 с.

5. Hill, C. E, & Knox, S. (2023). Psychotherapy training and supervision with undergraduate and graduate students. In L. G. Castonguay & C. E. Hill (Eds.), Becoming better psychotherapists: Advancing training and supervision (pp. 31– 53). American Psychological Association. URL: <https://doi.org/10.1037/0000364-003>

6. Supervision resource manual for psychology registration. The College of Psychologists and Behaviour Analysts of Ontario. Fourth Edition, 2025. Toronto, Ontario, Canada M4R 1A3. URL: <https://cpbao.ca/wpcontent/uploads/Document-Supervision-Resource-Manual-for-Registration-FourthEdition-2025-FINAL-2025-02-13-1.pdf>

УДК 004.056:004.7

^{1, 2}Прокопович-Ткаченко Д. І.

АДАПТИВНА МІЖРІВНЕВА КООРДИНАЦІЯ МЕХАНІЗМІВ КІБЕРЗАХИСТУ І ВІДНОВЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

¹Університет митної справи та фінансів, Дніпро, Україна

²Державний університет інформаційно-комунікаційних технологій, Київ, Україна

Анотація. Запропоновано формальну модель адаптивної міжрівневої координації кіберзахисту та відновлення інформаційно-комунікаційних мереж. Семирівневу модель OSI використано для узгодження телеметрії, станів, загроз і керуючих дій. Введено місійно орієнтовану метрику кіберстійкості, критерій емерджентної синергії та задачу синтезу політики з обмеженнями safety, авторизації, стабільності й ресурсів.

Ключові слова: кіберстійкість, OSI, міжрівневе керування, кіберзахист, відновлення, SDN/NFV, цифровий двійник.

Інформаційно-комунікаційні мережі поєднують механізми L1–L7, тому кібервплив на одному рівні спричиняє каскад змін на інших: завади збільшують повторні передавання і затримку, порушення маршрутизації змінює RTT і доступність сеансів, а компрометація керуючої площини запускає хибні реакції в кількох доменах. Отже, локальна оптимізація окремого засобу захисту не гарантує збереження критичної комунікаційної функції.

Пропонується перейти від фрагментарного захисту L1–L7 до місійно орієнтованої кіберстійкості, за якої рішення формуються на основі довіреної часово узгодженої телеметрії, прогнозу міжрівневих каскадів і формально обмеженої координації дій. Формальним ядром є динамічна багатопарова модель:

$$M_{OSI}(t) = \langle L, V, E_x, s(t), y(t), A, P, \Theta, R, K \rangle, \quad (1)$$

де L – рівні; V – компоненти й агенти; E_x – внутрішньо- та міжрівневі залежності; s(t) – прихований стан; y(t) – телеметрія; A – дії; P – політики; Θ – загрози й відмови; R – ресурси; K – обмеження safety, authorization і service.

$$z_e(t) = [I, P, F, C, D, U]. \quad (2)$$

Вектор z_e(t) характеризує довіру до доказу: I – integrity; P – provenance/attestation; F – freshness; C – cross-layer consistency; D – diversity/independence джерел; U – uncertainty. Криптографічні та авторизаційні предикати є жорсткими й не компенсуються високими значеннями інших компонентів.

Таблиця 1. Відображення спостережень, дій і кібервпливів за рівнями

Рівень	Спостереження	Допустимі дії	Кібервплив
L1–L2	SNR, BER, RSSI, retries	channel/MCS, handover, isolation	jamming, deauth, spoofing
L3–L4	loss, route, RTT, jitter	reroute, ACL, multipath, rate/FEC	route poisoning, flood, reset

Рівень	Спостереження	Допустимі дії	Кібервплив
L5–L6	identity, token/key, crypto errors	re-auth, rekey, revoke	hijack, replay, downgrade
L7/місія	SLA, residual service, deadline	priority, replica, degraded mode	DDoS, logic abuse

Ефективність координації визначається часовою якістю критичної функції. Для місії m нормована втрата $L_m(t)$ охоплює недоступність, запізнення, порушення цілісності та небезпечну деградацію. Інтегральна кіберстійкість на горизонті T :

$$R_m = 1 - \frac{\int_0^T L_m(t)dt}{T \cdot L_{max}}. \quad (3)$$

Системний ефект координації порівнюється з композицією незалежних локальних політик за однакового ресурсного бюджету:

$$\Delta_{em} = R_{full} - R_{expected_{local}}. \quad (4)$$

Позитивну емерджентність підтверджують за $\Delta_{em} > 0$ з довірчим інтервалом, нульовими safety violations, bounded oscillation і стійкістю ефекту в абляційних сценаріях.

Керуючу політику синтезують за багатокритеріальною функцією місійної втрати, часу реагування, ресурсів, координаційних накладних витрат і побічного ефекту:

$$\pi = \operatorname{argmin}_{\pi} \pi E [J_{mission} + \lambda_t J_{time} + \lambda_r J_{resource} + \lambda_o J_{overhead} + \lambda_s J_{side-effect}]. \quad (5)$$

$$g_{safety}(\pi) \leq 0, g_{auth}(\pi) = true, g_{stability}(\pi) \leq 0, g_{resource}(\pi) \leq 0. \quad (6)$$



Рис. 1. Замкнений контур адаптивної міжрівневої координації кіберзахисту і відновлення

Рис. 1 відображає замкнений контур: цифровий двійник прогнозує траєкторію каскаду; policy engine формує лише допустимі дії; виконання контролюється rollback; вимірний місійний ефект повертається до моделі для повторного оцінювання та адаптації.

Телеметрію нормалізують за часом, походженням, версією політики й довірчими ознаками. На L1–L2 контролюють параметри сигналу, повторні передавання і черги; на L3–L4 – маршрути, втрати, RTT, jitter і congestion control; на L5–L6 – ідентичність, ключі, re-authentication та криптографічні помилки; на L7 – SLA, залишкову якість сервісу і критичність місії. Це дає змогу виявляти причинно пов’язаний міжрівневий каскад, а не лише локальну аномалію.

Каскад прогнозується на часовому багатшаровому графі залежностей, де для кожного ребра оцінюються напрям, затримка, поріг активації, насичення та невизначеність. Наприклад, jamming на L1 підвищує retransmission на L2, RTT і втрати на L4 та ризик порушення deadline на L7. Контур має відрізнити цей сценарій від легітимної зміни навантаження або мобільності, оскільки однакова локальна ознака потребує різних дій.

Політика адаптації є ієрархічною: локальні агенти виконують оборотні дії в межах затверджених контрактів, а міждоменні чи потенційно небезпечні зміни проходять додаткову перевірку. Rate limiting, reroute, quarantine, FEC, multipath і тимчасова зміна пріоритету можуть виконуватися автоматично. Дії зі значним blast radius допускаються лише після перевірки цифровим двійником, safety shield і, за потреби, оператором.

Стійкість контролера забезпечують локальні fallback policies, версіонування конфігурацій, TTL тимчасових правил, rollback і decision record. У разі втрати центрального оркестратора система переходить у bounded degradation: домени підтримують критичні функції в межах доступних ресурсів, а після відновлення зв’язку виконують контрольоване reconciliation. Це усуває єдину точку відмови.

Baseline-конфігурації охоплюють однорівневий IDS/IPS, rule-based SDN/NFV failover, Zero Trust + SIEM/SOAR без cross-layer прогнозу, resilient routing/multipath і централізований оптимізатор. Порівняння проводиться за однакового апаратного та часо-ресурсного бюджету.

Таблиця 2. Матриця експериментальної валідації

Рівень	Середовище та сценарії	Критерії
V0	Формальна модель; safety/liveness; конфлікт політик	safety violations = 0; bounded oscillation
V1	Дискретно-подійна модель; jamming, route poisoning, DDoS	area-of-loss; MTTR; cascade error
V2	Мережева емуляція; partition, replay, telemetry poisoning	p95/p99 latency; goodput; convergence
V3	HIL/NIL; комбіновані атаки та відмови	residual service; CPU/RAM; control traffic

Валідація виконується на рівнях V0–V3 (табл. 2) з однаковими трасами, ресурсами й часовими бюджетами для baseline та запропонованої системи. Сценарії охоплюють jamming/mobility, route poisoning, DDoS/flash crowd, controller partition, session replay, telemetry poisoning і конфлікт політик.

Ключовий критерій – зменшення area-of-loss критичної функції та MTTR без зростання небезпечних дій. Додатково оцінюються p50/p95/p99 latency, goodput, convergence time, calibration довіри, coverage прогнозу каскаду, CPU/RAM і control traffic. Міжрівневу синергію перевіряють абляціями без provenance, uncertainty, cascade predictor, safety shield або local fallback.

Цифровий двійник використовується для прогнозу, what-if аналізу та попередньої перевірки політик, але не замінює довірену телеметрію і формальні обмеження безпечної дії. Така роль відповідає підходам network digital twin до security forecast, decision-making, verification та optimization.

Висновки. Сформовано цілісний контур: довірена телеметрія → оцінювання стану → прогноз каскаду → формально обмежений синтез політики → виконання та rollback → вимірювання місійного ефекту. Наукова відмінність полягає у композиційній координації L1–L7 з кількісною перевіркою емерджентної синергії та стабільності. Практична цінність визначається інтеграцією із SDN/NFV, SIEM/SOAR, Zero Trust і цифровим двійником без втрати керованості автономних дій. Подальша валідація має підтвердити ефект на сильних baseline-конфігураціях, за ворожої телеметрії, controller partition і координованих багаторівневих атак.

Література

- Salvi A., Spagnoletti P., Saad Noori N. Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. Computers & Security. 2022. Vol. 112. Art. 102507. DOI: 10.1016/j.cose.2021.102507.
- Faleiro R., Pan L., Pokhrel S. R., Doss R. Digital Twin for Cybersecurity: Towards Enhancing Cyber Resilience. Broadband Communications, Networks, and Systems. Springer, 2022. P. 57–76. DOI: 10.1007/978-3-030-93479-8_4.
- Bagrodia R. Using network digital twins to improve cyber resilience of missions. The Journal of Defense Modeling and Simulation. 2023. Vol. 20, No. 1. P. 7–16. DOI: 10.1177/15485129221131226.
- Allaw Z., Zein O., Ahmad A.-M. Cross-Layer Security for 5G/6G Network Slices: An SDN, NFV, and AI-Based Hybrid Framework. Sensors. 2025. Vol. 25, No. 11. Art. 3335. DOI: 10.3390/s25113335.
- Zita W., Malkawi M. An explainable network-aware self-adaptive cyber-resilient architecture using policy-based reinforcement learning. The Journal of Supercomputing. 2026. Vol. 82. Art. 301. DOI: 10.1007/s11227-026-08435-3.

УДК 004.056.55:004.738.5

Онтіверо-Валлс А.

АНАЛІЗ КРИПТОГРАФІЧНИХ ПАРАМЕТРІВ БЕЗПЕКИ У TLS-HANDSHAKE НА ОСНОВІ ДОСЛІДЖЕННЯ CLIENT HELLO ТА SERVER HELLO

Державний університет інтелектуальних технологій і зв’язку, Одеса, Україна
sanastasiya2005@gmail.com

Анотація. У роботі проведено практичний аналіз криптографічних параметрів безпеки протоколу TLS під час встановлення HTTPS-з’єднання. Досліджено повідомлення Client Hello та Server Hello, визначено запропоновані та узгоджені версії протоколу, набори шифрів, алгоритми цифрового підпису, групи еліптичних кривих та параметри обміну ключами. Аналіз виконано на основі мережевого трафіку, перехопленого за допомогою Wireshark під час встановлення з’єднання з вебресурсом suitt.edu.ua. Встановлено використання TLS 1.2 та криптографічного набору TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. Проведено оцінку безпеки застосованих параметрів та обґрунтовано доцільність переходу на TLS 1.3 для підвищення рівня захищеності каналу зв’язку.

Ключові слова: TLS, TLS-handshake, Client Hello, Server Hello, криптографічна безпека, HTTPS, ECDHE, AES-256-GCM, Wireshark.

Забезпечення цілісності передавання даних є одним із фундаментальних завдань сучасної кібербезпеки. Протягом першого півріччя 2025 року фахівці Національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA опрацювали 3018 кіберінцидентів — на 17% більше, ніж у попередньому півріччі (2575) [1].

Кібератаки можуть здійснюватися різноманітними способами. Одним із найбільш небезпечних і часто вживаних методів є атака «людина посередині» (Man-in-the-Middle, MitM) [2], яка дає зловмиснику змогу перехоплювати, змінювати або замінювати інформацію, що курсує між клієнтом і сервером. Надійний захист

від подібних загроз забезпечується застосуванням криптографічних протоколів із стійкими параметрами, зокрема TLS (Transport Layer Security).

Посилаючись на оновлений список OWASP Top 10 [3], де криптографічні помилки посідають друге місце серед найкритичніших вебзагроз, актуальність дослідження TLS є очевидною. Протокол TLS є фундаментальним інструментом забезпечення безпеки даних, причому процес рукостискання визначає надійність криптографічних параметрів. Вивчення повідомлень Client Hello і Server Hello дозволяє оцінити ступінь захисту комунікаційного каналу та виявити потенційні недоліки в умовах посилення кіберзагроз. Завданням цієї роботи є не просто документування застосованих параметрів, а комплексний аналіз їхньої криптографічної стійкості, звірка з актуальними нормативами та розробка порад щодо зміцнення рівня безпеки.

Для дослідження TLS-рукостискання було використано аналізатор трафіку Wireshark, що дає змогу ретельно фіксувати та аналізувати мережеві пакети на рівні конкретних протоколів. Робота проводилася на основі даних, отриманих під час створення HTTPS-з’єднання з веб-сайтом suitt.edu.ua.

Повідомлення Client Hello виступає першим кроком у процедурі TLS-рукопотискання. У ньому міститься набір криптографічних опцій клієнта, які пропонуються серверу для подальшого погодження. На рис. 1 показано частину цього повідомлення, яку було зафіксовано під час встановлення HTTPS-з’єднання з вебсайтом suitt.edu.ua. У розширенні supported_versions клієнт пропонує серверу як TLS 1.3, так і TLS 1.2.



Рисунок 1 – Фрагмент перехопленого повідомлення Client Hello

Повідомлення Server Hello є відповіддю сервера у процесі TLS-handshake та визначає остаточні криптографічні параметри захищеного сеансу. На рис. 2 представлено фрагмент цього повідомлення, отриманий під час встановлення HTTPS-з’єднання з вебсайтом suitt.edu.ua. У межах Server Hello сервер обирає версію протоколу, шифроспосіб і параметри обміну ключами, а також підтверджує відповідні розширення клієнта, формуючи узгоджений і захищений канал зв’язку.

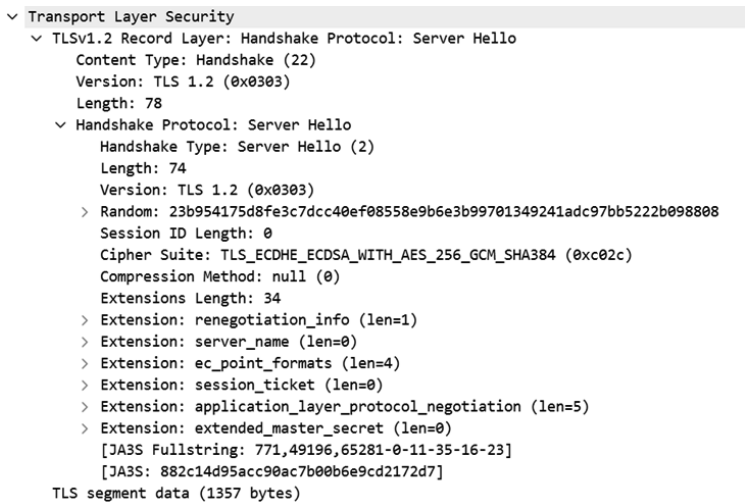


Рисунок 2 – Фрагмент перехопленого повідомлення Server Hello

Для детального розуміння того, які параметри були запропоновані клієнтом і які з них були прийняті сервером, доцільно виконати порівняльний аналіз відповідних полів повідомлень Client Hello та Server Hello. На основі отриманих даних сформовано таблицю, у якій зіставлені ключові характеристики обох повідомлень.

Таблиця 1

Порівняння Client Hello та Server Hello		
Параметр	Client Hello	Server Hello
Версія TLS	TLS 1.2	TLS 1.2
Cipher Suites	16 наборів (AES-GCM, CHACHA20, ECDHE, GREASE тощо)	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
SNI (server_name)	suit.edu.ua	Підтверджено (domain у сертифікаті збігається)
Supported Groups	x25519, secp256r1, secp384r1, x448	Сервер обрав групу, що відповідає ECDHE
Signature Algorithms	rsa_pss, rsa_pkcs1, ecdsa_sha2 групи	Сервер обирає ECDSA (підтверджено cipher suite)
Key Share	Немає (бо Client Hello = TLS 1.2)	Немає (TLS 1.2 не використовує KeyShare)
Session ID / Ticket	Session ID + session_ticket	Сервер надсилає Session ID та session_ticket
Random	587353...b2f5b8	23b954...b98808

У захопленому трафіку клієнт пропонує використання TLS 1.2, набір із 16 шифроспособів, сучасні алгоритми підпису (RSA-PSS, RSA, ECDSA) та підтримувані групи еліптичних кривих (x25519, secp256r1, secp384r1). У розширенні SNI зазначено домен suitt.edu.ua, а також передано поля Random і Session ID, необхідні для формування ключового матеріалу.

У відповідь сервер надсилає Server Hello, де підтверджує вибір TLS 1.2 та визначає шифроспосіб TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, що поєднує ECDHE, ECDSA та AES-256-GCM. Сервер оновлює Random і Session ID та надсилає розширення session_ticket для можливого відновлення сеансу; розширення key_share при цьому відсутнє, що є характерною ознакою саме TLS 1.2-узгодження (на відміну від TLS 1.3, де key_share обов'язкове).

У дослідженому з’єднанні обмін ключами реалізовано через ECDHE із використанням підтримуваних еліптичних кривих, зокрема secp256r1. Застосування ефемерної версії протоколу Діффі — Геллмана на еліптичних кривих гарантує властивість forward secrecy: навіть якщо в майбутньому довгостроковий приватний ключ сервера буде скомпрометовано, це не дозволить розшифрувати раніше перехоплений трафік. У цьому з’єднанні forward secrecy забезпечується саме завдяки використанню ECDHE. Автентифікація сервера виконана за допомогою ECDSA, що узгоджується з обраним криптографічним набором TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. Застосування ECDSA на кривій secp256r1 (P-256) відповідає приблизно 128-бітному рівню криптографічної стійкості за класифікацією NIST SP 800-57, що є мінімально прийнятним рівнем для нових систем станом на 2026 рік. Для захисту даних використовується AES-256 у режимі GCM: 256-бітний ключ перевищує цей мінімально рекомендований рівень, а сам режим належить до класу AEAD... не вимагаючи окремого HMAC (на відміну від застарілих CBC-режимів).

Додатково, використання SHA-384 у складі криптографічного набору абезпечує стійкість до колізій, що суттєво перевищує вимоги для даного класу застосунків. Сукупність виявлених параметрів — ECDHE, ECDSA, AES-256-GCM та SHA-384 — вказує на те, що безпосередньо досліджене з’єднання TLS 1.2 використовує сучасні криптографічні механізми та не демонструє ознак застосування застарілого RSA-обміну ключами або CBC-режимів шифрування.

Водночас перехід на TLS 1.3 є виправданим завдяки суворішій криптографічній політиці протоколу. TLS 1.3 унеможливорює використання статичного RSA для обміну ключами, залишаючи лише ефемерні механізми ECDHE, виключає зі специфікації низку історично вразливих механізмів, які TLS 1.2 допускає (хоча в дослідженому з’єднанні й не спостерігалися): стиснення на рівні TLS (вектор атаки CRIME), режим CBC зі спотвореним заповненням (атаки на кшталт Lucky13) та вразливий ранній механізм renegotiation. Крім того, повне TLS-рукостискання за TLS 1.2 типово потребує двох раундів обміну повідомленнями (2-RTT)... тоді як TLS 1.3 скорочує цей процес до одного раунду (1-RTT), а за наявності попереднього сеансу — до нульового (0-RTT). Тому перехід на TLS 1.3 дозволяє підвищити загальний рівень захищеності з’єднання, навіть якщо поточна конфігурація TLS 1.2 уже забезпечує forward secrecy.

Висновки. Аналіз на рівні специфікацій показав переваги TLS 1.3 порівняно з TLS 1.2. TLS 1.3 виключає зі специфікації статичний RSA та інші застарілі механізми, використовує більш жорстко визначений набір сучасних криптографічних алгоритмів і скорочує кількість раундів TLS-handshake. Це зменшує залежність безпеки від вибору окремих криптографічних параметрів та забезпечує більш сучасну модель захисту з’єднання. TLS 1.3 є рекомендованим варіантом подальшого налаштування захищеного HTTPS-з’єднання для досліджуваного ресурсу.

Література

1. Інтенсивність фішингових атак зросла, але люди стали більш обізнаними в питаннях «кібергігієни»: аналітичний звіт CERT-UA [Електронний ресурс] / Державна служба спеціального зв'язку та захисту інформації України. – Режим доступу: <https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitanniyakh-kibergigiyeni-analitichnii-zvit-cert-ua> (дата звернення: 23.08.2026);

2. Lindemulder G., Kosinski M. What Is a Man-in-the-Middle (MITM) Attack? [Електронний ресурс] / IBM. – Режим доступу: <https://www.ibm.com/think/topics/man-in-the-middle> (дата звернення: 23.08.2026);

3. OWASP Top 10:2021 [Електронний ресурс] / OWASP Foundation. – Режим доступу: <https://owasp.org/Top10/2021/> (дата звернення: 23.08.2026).

УДК 621.396.96:621.391.822

Бибик Р.Т.

ДОСЛІДЖЕННЯ ВПЛИВУ ПОХИБОК ТА ШУМІВ НА ХАРАКТЕРИСТИКИ ІСНУЮЧИХ МЕТОДІВ ПРОСТОРОВО-ЧАСТОТНОГО ОРІЄНТУВАННЯ

Національний університет «Львівська політехніка», м. Львів

romanbub3@gmail.com

Анотація. У тезах систематизовано та порівняно опубліковані результати досліджень впливу шумів, похибок просторової та частотної оцінки, а також невизначеності вхідних даних на характеристики існуючих методів просторово-частотного орієнтування (MUSIC, ESPRIT, TDOA, FDOA, RSS). На основі аналізу літературних джерел визначено характер деградації точності методів залежно від співвідношення сигнал/шум, кількості відліків, похибок положення сенсорів та невизначеності моделі поширення сигналу. Результати систематизації становлять теоретичну базу для розробки методу протидії джерелам радіоелектронної боротьби на основі просторово-частотного орієнтування засобів ураження.

Ключові слова: просторово-частотне орієнтування, похибки оцінювання, шуми, DOA, TDOA, FDOA, RSS, протидія РЕБ.

Вступ. Ефективність протидії джерелам радіоелектронної боротьби (РЕБ) на основі просторово-частотного орієнтування засобів ураження безпосередньо залежить від точності визначення кутових, часових, частотних та енергетичних параметрів сигналів джерел випромінювання. У реальних умовах експлуатації на результати оцінювання впливають шуми приймального тракту, похибки визначення положення сенсорів (антенних елементів, рознесених приймачів), похибки синхронізації часових шкал, а також невизначеність параметрів моделі поширення сигналу (кількість джерел, показник загасання траси, швидкість поширення). Це обумовлює необхідність систематизації відомих у літературі результатів досліджень впливу зазначених факторів на характеристики існуючих методів як теоретичного підґрунтя дисертаційного дослідження «Розробка методу протидії джерелам РЕБ на основі просторово-частотного орієнтування засобів ураження».

Метою тез є узагальнення та порівняльний аналіз опублікованих результатів досліджень впливу шумів і похибок на характеристики методів надрозділяючої кутової оцінки (MUSIC, ESPRIT, Root-MUSIC), різницево-часових (TDOA), різницево-частотних (FDOA) та гібридних TDOA/FDOA методів, а також методів на основі рівня прийнятого сигналу (RSS).

1. Класифікація факторів, що впливають на характеристики методів

Аналіз літературних джерел [1-15] дозволяє виділити чотири узагальнені групи факторів, що визначають точність методів просторово-частотного орієнтування: шуми каналу та приймального тракту; похибки просторової оцінки (положення сенсорів, калібрування решітки); похибки частотної оцінки (нестабільність опорних генераторів, синхронізація, доплерівські зсуви); невизначеність вхідних даних (кількість джерел, показник загасання траси, швидкість поширення сигналу). Узагальнена класифікація наведена на рисунку 1.



Рисунок 1 — Класифікація факторів, що впливають на характеристики методів

2. Аналіз впливу шумів та похибок на характеристики існуючих методів

2.1. Кутомірні методи надрозділяючої здатності (MUSIC, ESPRIT, Root-MUSIC)

Методи MUSIC та ESPRIT ґрунтуються на розділенні сигнального та шумового підпросторів кореляційної матриці прийнятих коливань, тому їхня точність істотно залежить від співвідношення сигнал/шум (SNR) та кількості відліків (снеспотів). За даними [2], субпросторові методи демонструють так званий «пороговий ефект» - різке погіршення характеристик, коли SNR або кількість снеспотів опускаються нижче певного порогового значення. У порівняльному дослідженні [1] показано, що метод MUSIC забезпечує високу роздільну здатність за ідеальних умов, проте чутливий до шуму та обчислювально затратний; Root-MUSIC знижує обчислювальну складність і підвищує стійкість оцінки, тоді як ESPRIT завдяки замкненій формі рішення демонструє найбільшу стійкість до шуму серед розглянутих алгоритмів. Дослідження [3] додатково встановлює, що чутливість MUSIC до кількості відліків пояснюється розсіюванням власних значень шумового підпростору: зі збільшенням кількості відліків це розсіювання зменшується, а отже зменшується і невизначеність оцінки; на відміну від цього, оцінка ESPRIT виявляє меншу залежність від кількості відліків. За даними [3], MUSIC потребує апріорного знання кількості джерел сигналу, якщо корисний сигнал глибоко «занурений» у шум, алгоритм може не виявити його як окреме джерело. У роботі [4] додатково підтверджено, що ESPRIT демонструє менше зміщення оцінки порівняно з MUSIC, а роздільна здатність обох методів істотно залежить від рівня шуму.

Основні обмеження групи методів: необхідність апріорного знання кількості джерел; деградація характеристик за наявності когерентних сигналів (багатопроменеве поширення); залежність від точності калібрування геометрії антенної решітки; пороговий ефект за низького SNR. Дослідники [5] також відзначають, що результуюча точність кутомірних методів істотно залежить від якості вхідних даних рівня шуму каналу, кількості елементів решітки та кількості накопичених відліків.

2.2. Різницево-часові методи (TDOA)

У методах TDOA положення джерела визначається за різницею часу приходу сигналу на рознесені сенсори, тому точність оцінки безпосередньо залежить від похибки вимірювання затримки та від точності знання координат сенсорів. Автори [6] прямо вказують, що точність локалізації є дуже чутливою до похибок положення сенсорів, хоча ця обставина довгий час залишалася малодослідженою порівняно з впливом вимірювального шуму. У дослідженні [9] отримано аналітичний результат: наявність похибок положення сенсорів вносить мультиплікативний коефіцієнт у критерій оптимальності розміщення сенсорів (Cramér–Rao Lower Bound, CRLB), який залежить від співвідношення потужності похибки положення та потужності шуму різниці відстаней. Робота [11] показує, що точність оцінки істотно падає зі зростанням випадкового вимірювального шуму, а розміщення сенсорів на рухомих платформах додатково вносить неусувні похибки положення. У [10] розглянуто спільний вплив похибок синхронізації часових шкал та похибок положення сенсорів і встановлено, що обидва фактори одночасно погіршують точність локалізації, при цьому запропоновані послідовні алгоритмічні рішення дозволяють досягати межі CRLB лише за порівняно малих

похибок. Дослідження [8] додатково зазначає, що дисперсія вимірювального шуму TDOA сама залежить від геометрії взаємного розташування джерела та сенсорів, тобто не є постійною величиною, що ускладнює узагальнену оцінку точності методу.

Обмеження методів TDOA: необхідність точної синхронізації часових шкал рознесених приймачів, що складно забезпечити за великої відстані між сенсорами; чутливість до похибок визначення координат сенсорів; погіршення геометричного фактора точності (GDOP) за несприятливої конфігурації сенсорів. У роботі [7] запропоновано використання калібрувального джерела з відомим (точно або приблизно) положенням для часткової компенсації похибок положення сенсорів; показано, що за помірного рівня шуму та похибок запропоновані алгоритми здатні досягати точності, що відповідає CRLB.

2.3. Різницево-частотні (FDOA) та гібридні TDOA/FDOA методи

Локалізація джерела за різницею частот прийому (FDOA) використовує доплерівський зсув частоти, що виникає внаслідок відносного руху джерела та сенсорів. За даними [12], точність геолокації на основі FDOA залежить від SNR, при цьому зі збільшенням дальності до джерела SNR знижується, а точність відповідно погіршується; водночас встановлено, що методи, які кутомірному типу (DOA), деградують з дальністю лінійно, тоді як гібридні TDOA/FDOA підходи є менш залежними від рівня SNR (а отже, і від дальності), оскільки SNR є лише частиною сумарної похибки за CRLB, а основний внесок дають безпосередньо виміряні різниці часу та частоти. У роботі [14] показано, що похибки положення та швидкості рухомих приймачів істотно знижують точність спільної TDOA/FDOA локалізації; розроблений замкнений алгоритм за певних умов (гаусів розподіл похибок положення) досягає межі CRLB. Дослідження [13] додатково розглядає задачу спільного оцінювання положення джерела та невідомої швидкості поширення сигналу за наявності похибок положення сенсорів; показано, що хоча оцінка методом максимальної правдоподібності є оптимальною, вона потребує вдалого початкового наближення, тоді як запропонований алгоритм на основі напіввизначеного програмування дозволяє отримати розв’язок, близький до цієї оптимальної оцінки, без початкового наближення.

Обмеження FDOA та гібридних методів: необхідність точного знання швидкості та положення рухомих сенсорів; чутливість до бази (відстані між сенсорами) та взаємної геометрії «сенсори–джерело»; пороговий ефект за низького SNR, аналогічний кутомірним методам.

2.4. Методи на основі рівня прийнятого сигналу (RSS)

Методи RSS оцінюють відстань до джерела за виміряним рівнем потужності сигналу з використанням моделі загасання траси, ключовим параметром якої є показник загасання (path loss exponent, PLE). За даними [15], невизначеність або неправильний вибір PLE є основним джерелом деградації точності, оскільки рішення, отримане за неоптимального значення PLE, набуває суттєвого зміщення. У роботі [16] на основі узагальненої логарифмічної моделі загасання аналітично отримано вираз похибки локалізації для оптимального оцінювача (Generalized Least Squares), що дозволило виявити ключові фактори, які визначають точність методу - рівень вимірювального шуму RSS, невизначеність PLE та геометрію розміщення сенсорів. Дослідження [18] показує, що додаткове врахування невідомої випромінюваної потужності джерела разом із невідомим PLE ще більше ускладнює задачу оцінювання, а похибки положення калібрувальних (анкерних) сенсорів додатково знижують досягну точність. Робота [15] також відзначає, що серед запропонованих оцінювачів найкращу точність за малого рівня шуму демонструє лінійний оцінювач (Linear Estimator), тоді як за високого рівня шуму більш робастним виявляється оцінювач на основі напіввизначеного програмування (SDP).

Обмеження методів RSS: істотно нижча потенційна точність порівняно з TDOA/AOA через високу чутливість до умов поширення сигналу (багатопроменевість, затінення); необхідність апіорного знання або спільного оцінювання параметрів моделі загасання; вплив невизначеності випромінюваної потужності джерела. Втім, як зазначається у [17], низька вартість і простота реалізації роблять RSS-методи привабливими там, де прийнятним є компроміс між точністю та складністю системи.

3. Узагальнена схема впливу похибок та шумів

На основі проведеного аналізу [1-18] узагальнену схему проходження впливу шумів і похибок від джерела випромінювання до кінцевого результату оцінювання наведено на рисунку 2. Похибки, що виникають на кожному етапі обробки (в каналі поширення, на сенсорах та під час оцінювання параметрів), накопичуються та проявляються у вигляді зміщення й зростання дисперсії підсумкової оцінки координат або частоти джерела, а також у вигляді порогових ефектів за несприятливих умов (низький SNR, мала кількість відліків, несприятлива геометрія).



Рисунок 2 — Узагальнена схема впливу похибок та шумів на кінцевий результат

4. Блок-схема проходження інформації в існуючих методах

Незважаючи на відмінності у фізичних принципах вимірювання (кутомірні, різницево-часові/частотні, енергетичні), розглянуті методи мають спільну узагальнену структуру обробки інформації: приймання сигналу, попередня обробка, формування статистики (кореляційної матриці, крос-кореляційної функції або оцінки потужності) та власне оцінювання параметра джерела. Узагальнену блок-схему наведено на рисунку 3.

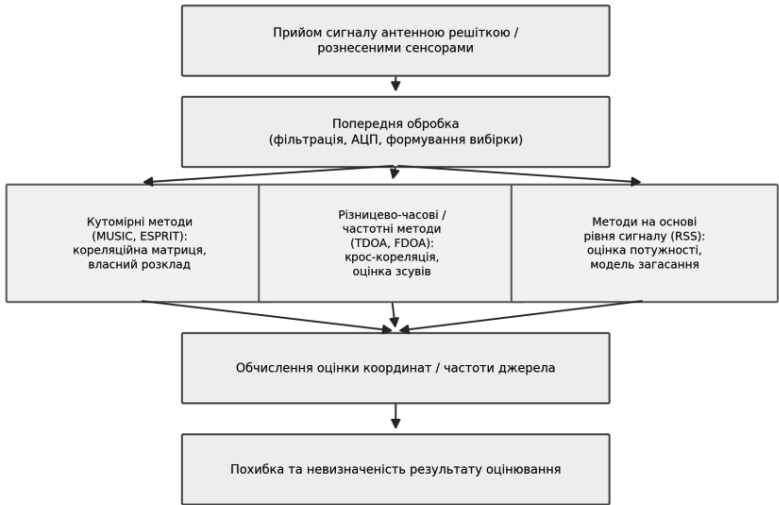


Рисунок 3 — Блок-схема проходження інформації в існуючих методах

5. Порівняльна систематизація результатів

Систематизовані за даними літератури джерела похибок та характер їхнього впливу наведено в таблиці 1.

Таблиця 1 - Джерела похибок та їхній вплив

Джерело похибки	Методи, на які впливає	Характер впливу (за даними [1-18])
Тепловий шум приймального тракту	MUSIC, ESPRIT, TDOA, FDOA, RSS	Зростання дисперсії оцінки, пороговий ефект за низького SNR [1-3, 12]
Похибки положення сенсорів	TDOA, FDOA, TDOA-AOA	Мультиплікативне погіршення CRLB, систематичне зміщення оцінки [6, 9, 14]
Похибки синхронізації часових шкал	TDOA, TDOA-FDOA	Систематична складова похибки локалізації [10]
Обмежена кількість відліків	MUSIC, ESPRIT	Збільшення розсіювання власних значень шумового

Джерело похибки	Методи, на які впливає	Характер впливу (за даними [1-18])
(снєпшотів)		підпростору [3]
Невизначеність показника загасання (PLE)	RSS	Систематичне зміщення оцінки відстані/координат [15-18]
Невизначеність швидкості поширення сигналу	TDOA, TDOA-FDOA	Додаткова похибка оцінки координат за невідомої швидкості [13]
Похибки калібрування антенної решітки	MUSIC, ESPRIT	Зміщення оцінки кута, зниження роздільної здатності [4, 5]
Багатопромєневе поширення / когерентні сигнали	MUSIC, ESPRIT	Втрата рангу сигнального підпростору, зниження точності [1, 5]

Узагальнене порівняння стійкості методів до шуму та похибок положення сенсорів за даними опрацьованих джерел наведено в таблиці 2.

Таблиця 2 - Порівняння стійкості існуючих методів за даними літератури

Метод	Чутливість до шуму (SNR)	Чутливість до похибок положення сенсорів	Джерела
MUSIC	Висока; пороговий ефект за низького SNR	Опосередкована (через калібрування решітки)	[1-3]
ESPRIT / Root-MUSIC	Помірна; стійкіші за MUSIC	Висока (потребує точної геометрії решітки)	[1, 4, 5]
TDOA	Висока	Дуже висока	[6, 7, 9, 10]
FDOA / TDOA-FDOA	Помірна (менша залежність від дальності, ніж у DOA)	Висока (залежить від швидкості й положення рухомих сенсорів)	[12-14]
RSS	Дуже висока (залежність від невизначеності PLE)	Помірна	[15-18]

Основні обмеження розглянутих методів, визначені за результатами аналізу літератури, систематизовано в таблиці 3.

Таблиця 3 - Основні обмеження існуючих методів

Метод	Основні обмеження
MUSIC / ESPRIT / Root-MUSIC	Потреба в апіорному знанні кількості джерел; деградація за когерентних сигналів; пороговий ефект за низького SNR і малої кількості відліків [1-5]
TDOA	Необхідність точної синхронізації часових шкал; висока чутливість до похибок положення сенсорів; залежність дисперсії шуму від геометрії [6, 7, 9, 10]
FDOA / TDOA-FDOA	Потреба в точному знанні швидкості й положення рухомих платформ; пороговий ефект за низького SNR [12-14]
RSS	Низька потенційна точність; сильна залежність від невизначеності моделі загасання та випромінюваної потужності [15-18]

Висновки

Проведена систематизація опублікованих результатів досліджень показує, що всі розглянуті методи просторово-частотного орієнтування, кутомірні надрозділяючі (MUSIC, ESPRIT, Root-MUSIC), різницево-часові

(TDOA), різницево-частотні (FDOA), гібридні TDOA/FDOA та енергетичні (RSS) зазнають істотної деградації характеристик за реальних умов експлуатації, що супроводжуються шумами приймального тракту, похибками положення та синхронізації сенсорів і невизначеністю параметрів моделі поширення сигналу.

Спільною закономірністю, підтвердженою незалежними дослідженнями [1–18], є наявність порогового ефекту різкого погіршення точності за низького SNR або обмеженого обсягу вхідних даних, а також істотна залежність досяжної точності від геометричного фактора (взаємного розташування джерела та сенсорів). При цьому кутомірні методи виявляють підвищену чутливість до похибок калібрування решітки та когерентності сигналів, різницево-часові й різницево-частотні методи до похибок положення та синхронізації рознесених сенсорів, а енергетичні методи до невизначеності моделі поширення сигналу.

Отримані узагальнення систематизують відомі результати щодо впливу шумів і похибок на характеристики існуючих методів та формують теоретичне підґрунтя для подальшого етапу дисертаційного дослідження, обґрунтування вимог до методу протидії джерелам РЕБ на основі просторово-частотного орієнтування засобів ураження, стійкого до сукупної дії розглянутих дестабілізувальних факторів.

Список літератури

1. Performance Comparison of Music, Root-Music, And Esprit Algorithms for DOA Estimation Under Rayleigh Fading Channels // International Research Journal on Advanced Engineering Hub (IRJAEH). 2025. URL: <https://irjaeh.com/index.php/journal/article/view/1093>
2. Wang Z., Yang W., Ling Z., Liao Z., Couillet R. A Large-Dimensional Analysis of ESPRIT DoA Estimation: Inconsistency and a Correction via RMT // arXiv preprint. 2025. URL: <https://arxiv.org/pdf/2501.02746>
3. Performance Comparison of MVDR, MUSIC, and ESPRIT for DOA Estimation // ARPN Journal of Engineering and Applied Sciences. 2020. URL: https://www.arpnjournals.org/jeas/research_papers/rp_2020/jeas_1120_8387.pdf
4. Performance analysis of MUSIC and ESPRIT DOA estimation algorithms for adaptive array smart antenna in mobile communication. 2010. URL: <https://www.researchgate.net/publication/224142246>
5. Accurate and Robust Localization Techniques for Wireless Sensor Networks: дис. URL: <https://arxiv.org/pdf/1806.05765>
6. Comparative analysis of TDOA-based localization methods in the presence of sensor position errors // IEEE Conference Publication. 2017. URL: <https://ieeexplore.ieee.org/document/8102652/>
7. Calibrating the error from sensor position uncertainty in TDOA-AOA localization // Signal Processing (ScienceDirect). 2019. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0165168419302592>
8. Accuracy analysis for TDOA localization in sensor networks // IEEE Conference Publication. URL: <https://ieeexplore.ieee.org/document/5977569/>
9. Optimal Sensor Placement for Full-Set TDOA Localization Accounting for Sensor Location Errors // IEEE Journals & Magazine. URL: <https://ieeexplore.ieee.org/iel8/7/11122308/10972121.pdf>
10. TDOA Source Localization in the Presence of Synchronization Clock Bias and Sensor Position Errors. 2013. URL: <https://www.researchgate.net/publication/260637265>
11. Source Localization Using TDOA with Sensor Position Errors Based on Constrained Total Least Squares and ADMM // IEEE Conference Publication. URL: <https://ieeexplore.ieee.org/document/10706425/>
12. Emitter Location Using Frequency Difference of Arrival Measurements Only // PMC. 2022. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9785639/>
13. TDOA Localization With Unknown Signal Propagation Speed and Sensor Position Errors. URL: <https://www.researchgate.net/publication/338727094>
14. Performance Analysis of TDOA and FDOA Location by Moving/Fixed Receivers with Location Errors // Journal of Communications. 2014. URL: <https://www.jocm.us/uploadfile/2014/0701/20140701030808485.pdf>
15. Received Signal Strength Localization With an Unknown Path Loss Exponent. 2016. URL: <https://www.academia.edu/21835901>
16. Error Analysis on RSS Range-Based Localization Based on General Log-Distance Path Loss Model // IEEE Conference Publication. 2018. URL: <https://ieeexplore.ieee.org/document/8567593>
17. Huang J., Liu P., Lin W., Gui G. RSS-Based Method for Sensor Localization with Unknown Transmit Power and Uncertainty in Path Loss Exponent // Sensors. 2016. Vol. 16, No. 9. Art. 1452. DOI: 10.3390/s16091452. URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038730/>
18. RSS-Based Target Localization With Unknown Model Parameters and Sensor Position Errors // IEEE Journals & Magazine. URL: <https://ieeexplore.ieee.org/document/9454374/>

АЛГОРИТМ ОЦІНКИ ВПЛИВУ ЗАВАД НА ФАЗОВУ ПОМИЛКУ ДИСКРЕТНОЇ СИСТЕМИ СИНХРОНІЗАЦІЇ В СТАЛИХ РЕЖИМАХ СТЕЖЕННЯ ЗА НЕСУЧОЮ ЧАСТОТОЮ

Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
bondarenko.alfa.inet@gmail.com; voloshinvasily@gmail.com

Анотація. Запропоновано алгоритм кількісної оцінки впливу імпульсної та фазоманіпульованої нефлуктуаційних завад на стаціонарну фазову помилку дискретної системи синхронізації. Алгоритм поєднує проєкцію завади на вихід узгодженого фільтра, нелінійне обчислення похибки фазового детектора та перенесення її дисперсії через дискретний контур за рівнянням Ляпунова. Передбачено перевірку стійкості, визначення середньоквадратичної фазової помилки і граничної інтенсивності завади. Наведено розрахунковий приклад і межі застосовності алгоритму.

Ключові слова: дискретна система синхронізації; фазова помилка; імпульсна завада; фазоманіпульована завада; цифрова ФАПЧ; рівняння Ляпунова.

Постановка задачі. Когерентне приймання М-PSK сигналів потребує відновлення опорного колювання, фаза якого узгоджена з фазою несучої. Навмисна структурована завада зміщує комплексний відлік не тільки безпосередньо, а й через фазовий детектор збудує контур синхронізації. У сталому режимі така дія накопичується у вигляді стаціонарної випадкової фазової помилки та зменшує кутовий запас демодулятора. Підходи, що замінують заваду лише додатковою шумовою потужністю, не враховують її фазовий напрям, часову активність і спектрально-часову проєкцію [1-3]. Тому потрібна послідовна процедура, яка перетворює фізичні параметри завади на дисперсію фази опорного колювання і дозволяє визначати допустимі режими роботи цифрової ФАПЧ.

Вхідна модель. На виході узгодженого фільтра відлік подається як сума корисного вектора, еквівалентної комплексної проєкції завади $J[k]$ та комплексного білого гауссівського шуму $n[k]$:

$$r[k] = \sqrt{(E_s)} e^{j\varphi_{s[k]}} + J[k] + n[k] \quad (1)$$

Поточну фазу корисного сигналу позначено $\varphi_s[k]$, а E_s є енергією символу. Нормовану проєкцію $\zeta J[k]$ доцільно визначати відносно корисного вектора. За малої поточної помилки контуру нелінійне збурення фазового детектора дорівнює

$$v_{J[k]} = \arg(1 + \zeta J[k]), \zeta J[k] = \frac{J[k]}{\sqrt{(E_s)} e^{j\varphi_{s[k]}}} \quad (2)$$

На відміну від лінеаризації $v_J \approx \text{Im}\{\zeta J\}$, використання аргументу комплексної суми зберігає порогову нелінійність у випадку наближення результуючого вектора до початку координат.

Імпульсна гілка. Імпульс описується двостановою пуассонівсько-марковською огинаючою $b[k] \in \{0,1\}$. Для інтенсивностей переходів λ_{01} і λ_{10} частка активних інтервалів p_i та нормована проєкція мають вигляд

$$\zeta_{I[k]} = b[k] \eta p e^{j\theta}, p_i = \frac{\lambda_{01}}{\lambda_{01} + \lambda_{10}} \quad (3)$$

Тут $\eta = A_i/A_s$ - нормована амплітудна інтенсивність; $p \in [0,1]$ - коефіцієнт часового і форм-факторного перекриття; θ - невідома відносна фаза. За рівномірної θ математичне сподівання похибки дорівнює нулю, а її дисперсія визначається числовим інтегруванням:

$$\sigma_{v,I}^2 = \frac{p_i}{2\pi} \cdot \int_{-\pi}^{\pi} \pi [\arg(1 + \eta p e^{j\theta})]^2 d\theta \approx \frac{p_i^2 \rho^2}{2} \quad (4)$$

Малосигнальне наближення в (4) показує майже лінійний вплив частоти появи імпульсів і квадратичний вплив η . Поблизу $\eta \approx 1$ інтегральний вираз є обов'язковим, оскільки лінеаризація істотно знижує небезпеку.

Фазоманіпульована гілка. Якщо протягом корисного символу діють N рівних за тривалістю бінарних фазових символів завади, її проєкція визначається коефіцієнтом G , який враховує нормоване частотне розстроювання $\delta = \Delta f T_s$, послідовність $q = (\theta_0, \dots, \theta_{N-1})$ і взаємну компенсацію складових:

$$G(q, N, \delta) = \text{sinc}\left(\frac{\pi\delta}{N}\right) \cdot \frac{1}{N} \cdot \sum_{l=0}^{N-1} e^{j\left(\theta_l + \frac{\pi\delta(2l+1)}{N}\right)}, \zeta_F = \mu G e^{j\psi} \quad (5)$$

Для нормованої інтенсивності μ і рівномірної початкової фази ψ дисперсія нелінійної похибки детектора обчислюється усередненням за $2^N N$ комбінаціями q :

$$\sigma_{v,F}^2 = \frac{1}{2^N 2\pi} \cdot \sum_q \int_{-\pi}^{\pi} \pi [\arg(1 + \mu G(q, N, \delta) e^{j\psi})]^2 d\psi \quad (6)$$

За незалежних рівноймовірних бінарних символів і $\delta=0$ середнє $E\{|G|^2\}=1/N$, але для навмисно когерентної послідовності гірше значення $|G|$ може наближатися до одиниці. Тому алгоритм повинен повертати як середню, так і граничну оцінку.

Алгоритм оцінювання. Вихідними даними є клас завади $J \in \{I, F\}$; параметри сигналу M , E_s/N_0 і T_s ; матриці дискретного контуру A , B , C , G_w та коваріація Q_w або скалярні коефіцієнти a , g ; фонові дисперсії $D_\varphi, 0$; допустима дисперсія $D_{\text{доп}}$; діапазон інтенсивності; параметри p_i , ρ для імпульсної або N , δ і статистика q для фазоманіпульованої завади. Обчислення виконують у такій послідовності.

- Перевірка режиму стеження.** Обчислити спектральний радіус $\rho(A)$; для скалярної моделі перевірити $|a| < 1$. Алгоритм застосовується лише після захоплення несучої, за відсутності циклічних прослизань, насичення АЦП і значної тактової помилки. Якщо умова порушена, слід перейти до моделювання повного нелінійного контуру.
- Нормування параметрів.** Визначити відношення амплітуд завади і сигналу, відносно частотне розстроювання та параметри перекриття. Для імпульсів p_i оцінювати за статистикою станів або як частку символівних інтервалів з ненульовою проєкцією; для ФМ-завади сформувати множину послідовностей q або заданий імовірнісний закон.
- Формування комплексної проєкції.** Для кожної точки інтенсивності та фазової сітки обчислити ζI або ζF . Для ФМ-гілки попередньо знайти $G(q, N, \delta)$; окремо зберегти $E\{|G|^2\}$ і $\max|G|$. Цей крок не дозволяє ототожнювати завади з однаковою потужністю, але різною проєкцією на корелятор.
- Обчислення нелінійної похибки.** Визначити $v_J = \arg(1 + \zeta J)$ функцією $\text{atan2}(\text{Im}\{1 + \zeta J\}, \text{Re}\{1 + \zeta J\})$. Використання atan2 запобігає втраті квадранта. Для значень $|1 + \zeta J| < \epsilon_0$ зафіксувати наближення до сингулярної області та збільшити густину фазової сітки.
- Статистичне усереднення.** Числовою квадратурою або Монте-Карло отримати $m v_J = E\{v_J\}$ і $\sigma^2 v_J = E\{(v_J - m v_J)^2\}$. Для симетричної рівномірної початкової фази $m v_J \approx 0$; відхилення від нуля вказує на фазово-узгоджену заваду і потребує окремого розрахунку систематичного зміщення.
- Перенесення через контур.** Підставити $\sigma^2 v_J$ до дискретного рівняння Ляпунова; розв'язок P одержати стандартним методом $d\text{lyap}$ або ітерацією $P_{n+1} = A P_n A^T + R$ до виконання $\|P_{n+1} - P_n\|_F < \epsilon_P$. Фазову дисперсію визначити як $D_\varphi = C P C^T$.
- Перевірка точності.** Зменшити крок за інтенсивністю та фазою вдвічі й повторити розрахунок. Результат прийняти, якщо відносна зміна D_φ не перевищує заданого допуску. Поблизу компенсації векторів доцільно підтвердити результат Монте-Карло моделюванням повного фазового детектора.
- Пошук порога.** Порівняти D_φ з $D_{\text{доп}}$ і визначити найменшу інтенсивність, за якої обмеження порушується. Після виявлення інтервалу порога застосувати бісекцію. Для ФМ-завади сформувати два пороги: усереднений за статистикою q та гарантований за $\max|G|$.
- Формування результату.** Повернути D_φ , середньоквадратичну помилку $\sigma_\varphi = \sqrt{D_\varphi}$, запас до $D_{\text{доп}}$, порогову інтенсивність, ознаку сингулярної області та рекомендацію: змінити смугу контуру, знизити позиційність M , застосувати бланкування імпульсів або придушення спектрально-часової проєкції ФМ-завади.

Модель перенесення. Для контуру довільного порядку стан $x[k]$ та фазова помилка $\epsilon[k]$ описуються

$$x[k+1] = A x[k] + B v_{J[k]} + G_w w[k], \epsilon[k] = C x[k] \quad (7)$$

де $w[k]$ об'єднує тепловий шум, фазовий шум генератора та інші невраховані збурення. За стійкої A стаціонарна коваріація і шукана фазова дисперсія дорівнюють

$$P = A P A^T + B \sigma_{v,J}^2 B^T + G_w Q_w G_w^T, D_\varphi = C P C^T \quad (8)$$

Щоб відокремити вплив параметрів завади від динаміки контуру, зручно використовувати еквівалентну модель першого порядку $\epsilon[k+1] = a \epsilon[k] + g v_J[k] + w[k]$. Тоді

$$D_{\varphi,J} = D_{\varphi,0} + \frac{g^2 \sigma_{v,J}^2}{1-a^2}, |a| < 1 \quad (9)$$

Множник $g^2/(1-a^2)$ є дискретним еквівалентом шумової смуги в прийнятій нормалізації. Зменшення g послаблює миттєве проникнення завади, однак a , близьке до одиниці, збільшує пам'ять контуру. Отже, параметри a і g слід оптимізувати спільно, а не трактувати вузьку смугу як безумовний захист.

Розрахунковий приклад. Для $a=0,92$; $g=0,08$; $D_\varphi, 0=10^{-4}$ рад²; повного перекриття $\rho=1$; $p_i=0,2$ та $\delta=0$ отримано нелінійне зростання дисперсії. Для імпульсної завади значення D_φ, I при $\eta=\{0,25; 0,50; 0,75; 1,00\}$ становлять відповідно $\{3,646 \cdot 10^{-4}; 1,215 \cdot 10^{-3}; 2,898 \cdot 10^{-3}; 6,954 \cdot 10^{-3}\}$ рад². Для ФМ-завади з $N=2$ при $\mu=\{0,25; 0,50; 0,75; 1,00\}$ одержано $D_\varphi, F=\{7,615 \cdot 10^{-4}; 2,888 \cdot 10^{-3}; 7,094 \cdot 10^{-3}; 1,723 \cdot 10^{-2}\}$ рад². За однакової числової інтенсивності ФМ-гілка в цьому прикладі є небезпечною через безперервну дію та більшу ефективну проєкцію. Для незалежних символів $N=5$ середнє $E\{|G|^2\}$ зменшується з 0,5 до 0,2, але гарантована оцінка $\max|G|=1$ не змінюється.

Інтерпретація результатів. За $\eta \ll 1$ або $\mu|G| \ll 1$ дисперсія фазового детектора і стаціонарна D_φ зростають приблизно квадратично з амплітудною інтенсивністю. Коли проєкція завади стає співмірною з корисним вектором, залежність $\arg(\cdot)$ формує різкий нелінійний підйом. У цій області середня потужність не є достатньою характеристикою: вирішальними стають напрям вектора, частка активних інтервалів, $G(q, N, \delta)$ та пам'ять контуру. Саме тому алгоритм виконує фазове усереднення до, а не після проходження дискретного контуру.

Для інженерного вибору допустимої дисперсії $D_{\text{доп}}$ її доцільно пов'язати з кутовим запасом $M\text{-PSK}$. Відстань до найближчої межі рішення дорівнює $\alpha=\pi/M$, тому збільшення M зменшує запас до фазової помилки. Практичний консервативний критерій можна задавати як $3\sigma_{\phi} \leq \kappa \alpha$, де $\kappa < 1$ враховує пряме векторне зміщення і потрібний резерв. Алгоритм не підмінює повний BER-розрахунок, але надає фазову складову, яка може бути введена до кореляційної моделі когерентного демодулятора [1, 2].

Обчислювальна реалізація. Інтеграли (4) і (6) можна обчислювати квадратурою Гаусса або рівномірною фазовою сіткою з контролем збіжності. Для випадкових q доцільне векторизоване перебирання при малих N і Монте-Карло при великих N . Рівняння (8) розв'язується без явного моделювання тривалої реалізації контуру, тому алгоритм придатний для побудови карт допустимих режимів у координатах «інтенсивність - смуга контуру - позиційність сигналу». Для нестационарної завади розрахунок повторюють у ковзному вікні з актуальними оцінками p_i , G та Q_w .

Область застосовності. Алгоритм орієнтований на сталий режим стеження, у якому залишкова фазова помилка є стаціонарним процесом, а лінеаризована модель динаміки адекватна. Обмеженнями є відсутність циклічних прослизань, насичення тракту, важких хвостів розподілу та суттєвої кореляції v_J із внутрішнім станом контуру. За $|1+\zeta_J| \approx 0$, високої ймовірності помилки, фазово-узгодженої навмисної послідовності або зриву стеження потрібне імітаційне моделювання повної нелінійної системи. Фонову коваріацію Q_w і параметри A , B , C , G_w слід ідентифікувати для конкретної цифрової ФАПЧ [4, 5].

Практичне використання. Отримана процедура може бути вбудована до засобу моніторингу приймача. Оцінки інтенсивності та спектрально-часових параметрів завади надходять від детектора, після чого модуль прогнозує D_{ϕ} і порівнює її з допустимою. Перевищення порога є підставою для адаптації коефіцієнтів контуру, переходу на нижчий порядок M , бланкування уражених відліків або активації просторово-частотного придушення. Збереження окремих середньої і гіршої оцінок запобігає надмірно оптимістичному рішенням щодо навмисної когерентної ФМ-завади.

Висновки. Розроблено алгоритм оцінки впливу імпульсної та фазоманіпульованої нефлуктуаційних завад на фазову помилку дискретної системи синхронізації в сталому режимі стеження за несучою. Алгоритм зберігає часову, фазову і векторну структуру завади, обчислює нелінійну дисперсію похибки фазового детектора та переносить її через контур за дискретним рівнянням Ляпунова. Окремі гілки враховують частку активності і перекриття імпульсів або коефіцієнт G фазоманіпульованої завади. Передбачено контроль стійкості й збіжності, пошук граничної інтенсивності та формування інженерної рекомендації. Числовий приклад підтверджує квадратичне зростання D_{ϕ} за малих інтенсивностей і різке нелінійне погіршення поблизу компенсації корисного вектора. Подальший розвиток доцільно спрямувати на врахування циклічних прослизань і онлайн-ідентифікацію параметрів завади.

Література

1. Туровський О. Л., Мелешко Т. В., Дробик В. О. Методологія оцінки впливу нефлуктуаційних завад на завадостійкість прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією. Зв'язок. 2022. № 5(159). С. 29-34. DOI: 10.31673/2412-9070.2022.053439.
2. Швець В., Мелешко Т. Оцінка завадозахищеності когерентного прийому сигналів з багатопозиційною фазовою маніпуляцією при наявності нефлуктуаційних завад. Measuring and Computing Devices in Technological Processes. 2023. № 2. С. 167-178. DOI: 10.31891/2219-9365-2023-74-21.
3. Бондаренко Є. В., Кітура О. В. Методологічний підхід до оцінки впливу імпульсних нефлуктуаційних завад на цілісність дискретних сигналів з багатопозиційною фазовою маніпуляцією. Сучасний захист інформації. 2024. № 4(60). С. 53-59. DOI: 10.31673/2409-7292.2024.040006.
4. Turovsky O. L. Estimation of the possibilities of the combined synchronization system with open-link to minimize the dispersion of the phase error when tracking the carrier frequency under additive noise. Technology Audit and Production Reserves. 2020. Vol. 3, No. 4. P. 16-22. DOI: 10.15587/2706-5448.2020.210242.
5. Berkman L., Tkachenko O., Turovsky O., Fokin V., Strelnikov V. Designing a system to synchronize the input signal in a telecommunication network under the condition for reducing a transitional component of the phase error. Eastern-European Journal of Enterprise Technologies. 2021. Vol. 1, No. 9(109). P. 66-76. DOI: 10.15587/1729-4061.2021.225514.
6. Middleton D. Statistical-physical models of electromagnetic interference. IEEE Transactions on Electromagnetic Compatibility. 1977. Vol. EMC-19, No. 3. P. 106-127. DOI: 10.1109/TEM.1977.303527.

УДК 004.056:530.145

Васіліу Є.В., Назаренко О.А., Стайкуца С.В., Іванов В.І.

ПРОТОКОЛ КВАНТОВОГО РОЗДІЛЕННЯ СЕКРЕТУ НА ОСНОВІ ТРИКУБІТНИХ ГХЦ-СТАНІВ ІЗ ДВОЕТАПНИМ КОНТРОЛЕМ КВАНТОВИХ КАНАЛІВ

Державний університет інтелектуальних технологій і зв'язку

y.v.vasiliiu@suitt.edu.ua

Анотація. Квантове розділення секрету є одним із перспективних напрямів квантової криптографії, що забезпечує розподіл конфіденційної інформації між кількома учасниками таким чином, що її відновлення можливе лише за їх спільної участі. Більшість відомих протоколів, побудованих на основі трикубітних GHZ-станів, характеризуються фіксованим розподілом кубітів між учасниками, асиметрією їхніх ролей та обмеженими можливостями контролю квантових каналів. У роботі запропоновано новий протокол квантового розділення секрету на основі трикубітних ГЦХ-станів, який поєднує випадковий розподіл кубітів між учасниками, випадкове призначення ролей посередника та вимірювача, двоетапний контроль усіх квантових каналів і маскування секретної інформації шляхом випадкового застосування локальних операторів Паулі. Наведено загальну структуру запропонованого протоколу та розглянуто його основні особливості. Попередній аналіз показує, що запропонований підхід забезпечує контроль усіх квантових каналів передавання та підвищує стійкість протоколу до атак на квантові канали. Подальші дослідження будуть спрямовані на формальний аналіз стійкості запропонованого протоколу до зовнішніх і внутрішніх атак та його узагальнення на багатокубітні ГХЦ-стани.

Ключові слова: квантова криптографія, квантове розділення секрету, ГХЦ-стани, квантові комунікації, квантова запутаність, квантова безпека.

Квантова криптографія є одним із найбільш перспективних напрямів розвитку сучасних інформаційно-комунікаційних технологій, оскільки забезпечує принципово новий рівень захисту інформації, що ґрунтується на фундаментальних законах квантової механіки. На відміну від класичних криптографічних методів, безпека квантових протоколів визначається не обчислювальною складністю математичних задач, а фундаментальними законами квантової механіки, зокрема теоремою про неможливість клонування довільного квантового стану та статистичними закономірностями квантових вимірювань, що дають змогу виявляти спроби перехоплення квантової інформації [1, 4].

Одним із важливих напрямів квантової криптографії є квантове розділення секрету (Quantum Secret Sharing, QSS), запропоноване наприкінці XX століття як квантовий аналог класичних схем розділення секрету. У таких протоколах секретна інформація розподіляється між кількома учасниками таким чином, що її відновлення можливе лише за їхньої спільної участі, тоді як жоден окремих учасник не може самостійно отримати секрет [2, 3].

Першим протоколом квантового розділення секрету став протокол Hillery–Bužek–Berthiaume (HBB99), у якому для розподілу секретної інформації використовуються трикубітні стани Грінбергера-Хорна-Цайлінгера (ГХЦ) [3]. Надалі було запропоновано значну кількість модифікацій і вдосконалень протоколів квантового розділення секрету [4–11]. Серед них найбільшого поширення набули протоколи на основі ГХЦ-, W-, кластерних і графових станів, а також схеми, що використовують одиночні фотони, безперервні стани та напівквантові моделі.

Аналіз сучасних протоколів квантового розділення секрету свідчить, що питання одночасного забезпечення симетричності учасників, контролю всіх етапів передавання квантової інформації та випадкового розподілу функціональних ролей між учасниками залишаються недостатньо дослідженими. Зокрема, більшість відомих протоколів використовує фіксований розподіл кубітів між учасниками й передбачає незмінні функції кожного з них протягом усього сеансу виконання протоколу.

У даній роботі запропоновано новий протокол квантового розділення секрету на основі трикубітних ГХЦ-станів, у якому реалізовано випадковий розподіл кубітів між учасниками, випадкове призначення ролей посередника та вимірювача, а також двоетапний контроль передавання квантових станів. Наведено опис запропонованого протоколу та виконано попередній аналіз його особливостей і безпеки.

Запропонований протокол квантового розділення секрету використовує трикубітні ГХЦ-стани для розподілу трьох бітів секретної інформації між дилером Алісою та двома учасниками протоколу – Бобом і Чарлі. Аліса готує ГХЦ-стан, кодує секретне повідомлення за допомогою локальних операторів Паулі та випадковим чином розподіляє кубіти між Бобом і Чарлі таким чином, що один із них отримує два кубіти, а інший – один.

Після першого етапу контролю квантових каналів випадковим чином призначаються ролі посередника та вимірювача. Посередник застосовує до отриманих кубітів випадкові локальні оператори Паулі та передає всі кубіти вимірювачу. Далі залежно від режиму роботи виконується або другий етап контролю передавання квантових станів, або відновлення секретної інформації на основі результатів ГХЦ-вимірювання, та відкритого обміну класичною інформацією про результати вимірювання й виконану маскувальну операцію. Загальну схему запропонованого протоколу наведено на рис. 1.

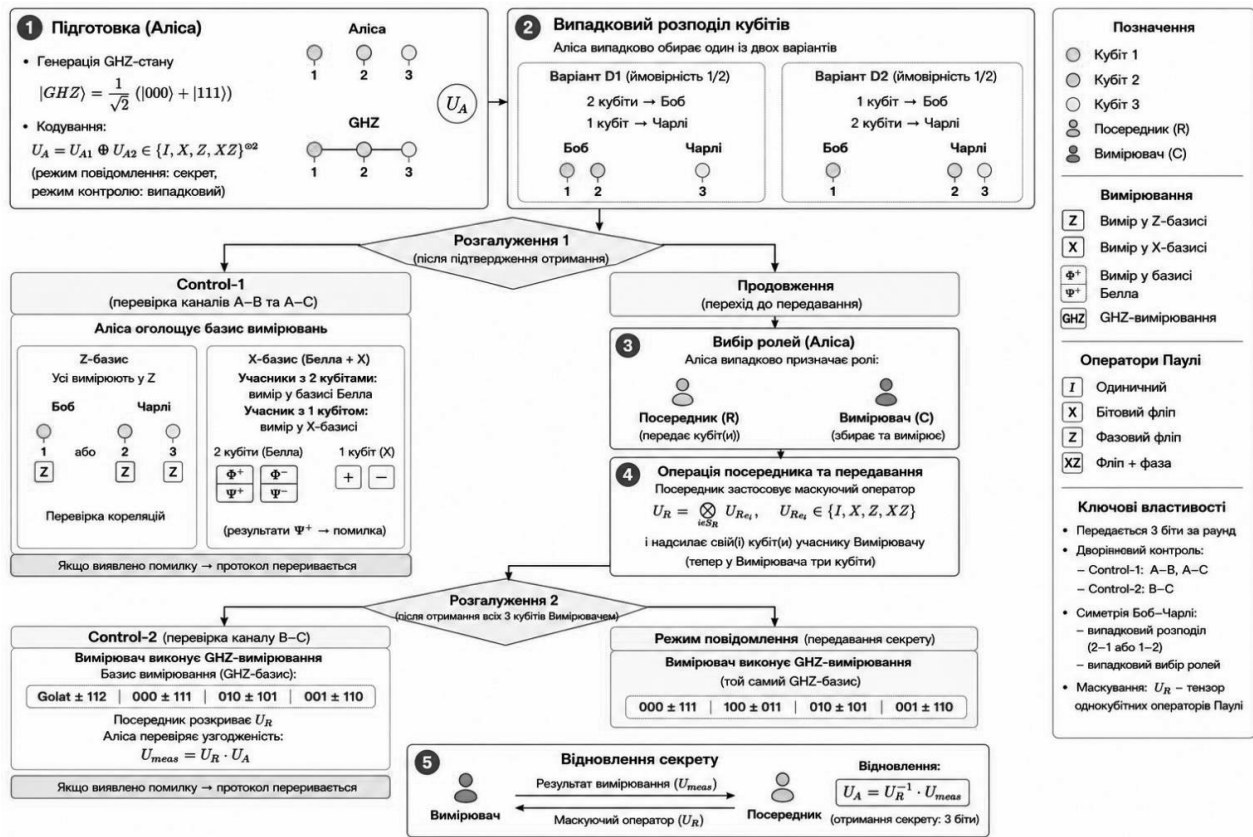


Рис. 1. Загальна схема запропонованого протоколу квантового розділення секрету на основі трикубітних ГХЦ-станів

Як показано на рис. 1, запропонований протокол складається з п'яти основних етапів: підготовки та кодування ГХЦ-стану, випадкового розподілу кубітів між учасниками, випадкового призначення ролей посередника та вимірювача, виконання двоетапного контролю передавання квантових станів і відновлення секретної інформації. Така послідовність дій забезпечує симетричність учасників протоколу, контроль усіх етапів передавання квантової інформації та можливість передавання трьох бітів класичної інформації за один сеанс роботи протоколу.

Запропонований протокол має низку особливостей, які відрізняють його від більшості відомих схем квантового розділення секрету на основі трикубітних ГХЦ-станів. Насамперед реалізовано випадковий розподіл кубітів між учасниками, унаслідок чого жоден з учасників не отримує наперед визначений набір кубітів. Крім того, випадкове призначення ролей посередника та вимірювача забезпечує симетричність учасників протоколу та ускладнює реалізацію атак, орієнтованих на конкретного учасника. На відміну від протоколу, запропонованого Liu та співавт. [7], у якому використовується фіксований розподіл кубітів між учасниками та відновлення секретної інформації ґрунтується на ГХЦ-вимірюваннях і обміні квантовою запутаністю, у запропонованому протоколі також реалізовано двоетапний контроль усіх квантових каналів передавання квантових станів.

Двоетапний контроль передавання квантових станів є однією з ключових особливостей запропонованого протоколу. На першому етапі здійснюється контроль двох квантових каналів між Алісою та учасниками протоколу під час розподілу кубітів, а на другому етапі – контроль квантового каналу між самими учасниками після передавання квантових станів від посередника до вимірювача. Такий підхід забезпечує контроль усіх квантових каналів, що використовуються під час виконання протоколу, та дає змогу своєчасно виявляти можливі атаки на квантові канали зв'язку.

Попередній аналіз безпеки запропонованого протоколу показує, що його стійкість до атаки перехоплення та повторного передавання забезпечується тим, що редукований стан окремого кубіта є повністю змішаним, тоді як редукований стан пари кубітів не містить достатньої інформації для відновлення закодованого секрету. При цьому саме виконання вимірювання руйнує початкову квантову запутаність між усіма трьома кубітами. Оскільки порушник не має доступу до повного трикубітного ГХЦ-стану, він не може сформувати коректний стан для заміни перехоплених кубітів.

Стійкість протоколу до некогерентних атак із використанням допоміжних квантових систем може бути обґрунтована перенесенням побудованої раніше математичної моделі для пінг-понг протоколу з трикубітними ГХЦ-станами [11, 12]. Таке перенесення є коректним, оскільки на кожному етапі передавання атакуються ті

самі повністю змішані підсистеми кубітів, а локальні унітарні операції Паулі не змінюють спектрів їх редукованих матриць густини. Тому залежності між імовірністю виявлення атаки та максимальною інформацією порушника, отримані для ГХЦ-пінг-понг протоколу, можуть бути використані для аналізу безпеки запропонованого протоколу квантового розділення секрету. Повний математичний аналіз цих атак буде наведено в окремій роботі.

Оскільки для запропонованого протоколу розділення секрету є застосовною математична модель некогерентної атаки, побудована для ГХЦ-пінг-понг протоколу [11, 12], запропонований протокол також є асимптотично стійким до некогерентних атак. Це означає, що порушник може отримати лише обмежений обсяг інформації, який залежить від обраної імовірності виявлення атаки. Таким чином, збільшення обсягу інформації, доступної порушнику, неминуче супроводжується зростанням імовірності його виявлення в режимі контролю підслуховування.

Висновки. Запропоновано новий протокол квантового розділення секрету для схеми з одним дилером та двома учасниками на основі трикубітних ГХЦ-станів. Протокол поєднує випадковий розподіл кубітів між учасниками, випадкове призначення функціональних ролей посередника та вимірювача, а також двоетапний контроль усіх квантових каналів передавання. Запропонований підхід забезпечує симетричність учасників протоколу, контроль усіх квантових каналів та передавання трьох бітів класичної інформації за один сеанс його роботи.

Попередній аналіз безпеки свідчить про стійкість запропонованого протоколу до атаки перехоплення та повторного передавання й підтверджує можливість застосування до нього математичної моделі некогерентних атак, розробленої для ГХЦ-пінг-понг протоколу. Це означає, що зі збільшенням обсягу інформації, яку може отримати порушник, зростає ймовірність його виявлення в режимі контролю підслуховування, яка може бути наближена до одиниці з довільною точністю. Подальші дослідження будуть спрямовані на побудову повної математичної моделі безпеки запропонованого протоколу та аналіз його стійкості до різних класів квантових атак.

Література

- Gisin N., Ribordy G., Tittel W., Zbinden H. **Quantum cryptography**. *Reviews of Modern Physics*. 2002. Vol. 74, No. 1. P. 145–195. DOI: 10.1103/RevModPhys.74.145.
- Cleve R., Gottesman D., Lo H.-K. **How to Share a Quantum Secret**. *Physical Review Letters*. 1999. Vol. 83, No. 3. P. 648–651. DOI: 10.1103/PhysRevLett.83.648
- Hillery M., Bužek V., Berthiaume A. **Quantum Secret Sharing**. *Physical Review A*. 1999. Vol. 59, No. 3. P. 1829–1834. DOI: 10.1103/PhysRevA.59.1829
- Pirandola S., Andersen U. L., Banchi L. et al. **Advances in Quantum Cryptography**. *Advances in Optics and Photonics*. 2020. Vol. 12, No. 4. P. 1012–1236. DOI: 10.1364/AOP.361502
- Li Z., Jiang X., Liu L. Multi-Party Quantum Secret Sharing Based on GHZ State. *Entropy*. 2022. Vol. 24, No. 10. Art. 1433. DOI: 10.3390/e24101433
- Cai X.-Q., Li S., Liu Z.-F. et al. **Improving security of efficient multiparty quantum secret sharing based on a novel structure and single qubits**. *Scientific Reports*. 2024. Vol. 14. Art. 18385. DOI: 10.1038/s41598-024-69417-0
- Liu B., Zhang J., Qiu S., Zhang M. **A pure quantum secret sharing scheme based on GHZ basis measurement and quantum entanglement exchange**. *Chinese Physics B*. 2025. Vol. 34, No. 3. Art. 030304. DOI: 10.1088/1674-1056/ada548
- Yin H., Shen J., Chen N., Chen Z. **Research Status and Prospects of Quantum Secret Sharing**. *Acta Physica Sinica*. 2025. Vol. 74, No. 16. Art. 160301. DOI: 10.7498/aps.74.20250586
- Zhang C., Hao F.-L., Gu S.-P. et al. **Efficient Hyperentanglement-Based Quantum Secret Sharing Protocol**. arXiv:2503.20216, 2025.
- Y. Vasiliiu. Modern Quantum Technologies of Cryptographic Protection of Information. *Cybernetics and Systems Analysis*. 2025. Vol. 61, No. 4. P. 671–684. DOI: 10.1007/s10559-025-00801-y.
- Vasiliiu E. V. Asymptotic security of the ping-pong quantum direct communication protocol with three-qubit Greenberger–Horne–Zeilinger states. *Georgian Electronic Scientific Journal: Comp. Sc. and Telecomm.* 2009. Issue 3(20). P. 3–15.
- Havel S., Vasiliiu Y., Bardis N., Staikutsa S. Eavesdropping Attack of Two Eavesdroppers on the Ping-Pong Protocol with GHZ Triplets. *2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Gliwice, Poland, September 4–6, 2025). P. 1–5. DOI: 10.1109/IDAACS68557.2025.11322111.

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ВЗАЄМОДІЇ КОРИСТУВАЧА З LLM

Державний університет інтелектуальних технологій і зв’язку
nasttyonk@ukr.net, seva.odessa@gmail.com

Анотація. Виконано аналіз вразливостей взаємодії користувача з великими мовними моделями (LLM) та LLM-інтегрованими застосунками на основі оновленої класифікації OWASP Top 10 for LLM Applications 2025. Проведено практичне дослідження атак класів LLM01 (Prompt Injection), LLM02 (Sensitive Information Disclosure), LLM04 (Data and Model Poisoning) та LLM05 (Improper Output Handling) у повністю ізольованому локальному середовищі. Отримано кількісні метрики успішності атак (ASR) та порівняльну оцінку ефективності методів захисту (XML-структурування, РІІ-фільтрація, хешування, валідація виводу).

Ключові слова: великі мовні моделі, LLM, OWASP Top 10 for LLM, Prompt Injection, Sensitive Information Disclosure, Data and Model Poisoning, Improper Output Handling, RAG, кібербезпека LLM.

Захист інформації є однією з найважливіших проблем сучасного інформаційного суспільства. Розвиток великих мовних моделей протягом 2020-2025 років перетворив їх із дослідницького інструменту на компонент виробничих систем у фінансовому секторі, охороні здоров'я, освіті та державному управлінні. За даними Gartner, станом на 2024 рік понад 55% організацій у світі або вже впровадили LLM-рішення, або перебувають на стадії пілотування. Стрімке впровадження штучного інтелекту у важливі бізнес-процеси випереджає розвиток спеціалізованих засобів захисту, що створює ризики для конфіденційності та цілісності даних.

Архітектура сучасних LLM на основі трансформерів опрацьовує системні інструкції та користувацьке введення в єдиному контекстному вікні без жорсткого розмежування привілеїв. Оскільки модель сприймає весь вхідний потік як рівноправний текст, вона не здатна відрізнити керуючі команди розробника від довільних даних користувача. Це створює специфічну поверхню атаки на рівні prompt-взаємодії.

У 2023–2025 роках організація OWASP сформувала та оновила список «OWASP Top 10 for Large Language Model Applications», що систематизує десять найкритичніших класів вразливостей LLM-систем. У цій роботі досліджено чотири ключові категорії вразливостей, які безпосередньо пов'язані з взаємодією користувача з моделлю згідно з актуальним стандартом OWASP Top 10 for LLM Applications 2025:

- 1. LLM01 (Prompt Injection): Прямі та непрямі (Indirect Prompt Injection) атаки на контекст моделі.
- 2. LLM02 (Sensitive Information Disclosure): Невмісне розкриття системних промптів, токенів та конфіденційних даних через відповіді моделі або RAG-архітектуру.
- 3. LLM04 (Data and Model Poisoning): Компрометація та отруєння баз знань або даних налаштування (fine-tuning).
- 4. LLM05 (Improper Output Handling): Неналежа обробка вихідного тексту моделі backend-системами, що призводить до XSS, SQL-ін'єкцій та RCE.

Для практичної верифікації загроз було розгорнуто локальний мікросервісний експериментальний стенд на Flask із підключенням локальних моделей (Gemma 4/Mistral). Для забезпечення чистоти експерименту середовище було повністю ізольоване, що дозволило безпечно моделювати реальні сценарії атак. У ході випробувань було продемонстровано, що прості текстові keyword-фільтри блокують прямі запити, але залишаються вразливими до непрямих ін'єкцій при завантаженні зовнішнього контенту, де показник Attack Success Rate (ASR) досяг 70% без використання спеціалізованого захисту. Оцінка успішності атак розраховувалася за формулою:

$$ASR = \frac{\text{Number of Successful Attacks}}{\text{Total Number of Attacks Attempted}} \times 100\%$$

де Number of Successful Attacks - кількість атак, що успішно обійшли механізм захисту; Total Number of Attacks Attempted - загальна кількість спроб атак у тестовому наборі.

У ході випробувань було проведено серію з 100 тестових сценаріїв непрямих ін'єкцій, де в 70 випадках модель успішно виконала шкідливі інструкції зі стороннього контенту, що зафіксувало показник ASR на рівні 70%. Це підтверджує, що статичні методи фільтрації є неефективними проти адаптивних текстових маніпуляцій.

У сценаріях RAG-архітектури (LLM02) було відтворено витік конфіденційних конфігураційних параметрів та токенів авторизації за допомогою обхідних jailbreak-запитів адаптації моделі під «режим налагодження

розробника». У дослідженні LLM04 продемонстровано можливість маніпулювання кешем бази знань із підміною класифікаційних даних. При тестуванні LLM05 зафіксовано успішне виконання несанкціонованого SQL-запиту UPDATE до бази даних SQLite через обхідний запит природною мовою до AI-асистента. Отримані практичні результати підкреслюють необхідність впровадження комплексного підходу Defense-in-Depth, який передбачає сувору валідацію як вхідних промптів, так і вихідних відповідей моделі.

Висновки. Результати експериментальних досліджень підтверджують, що захист LLM-застосунків не може обмежуватися виключно стандартними фільтрами вхідних запитів. Ефективна система безпеки потребує комбінованого підходу, який включає:

- Препроцесинг та санітизацію зовнішнього контенту перед передачею в контекстне вікно;
- Явне XML/JSON-структурування для відокремлення системного промпту від даних користувача;
- Регулярну РІІ-фільтрацію вхідних та вихідних потоків даних (наприклад, за допомогою регулярних виразів або інструментів типу Microsoft Presidio);
- Застосування суворого обмеження прав (RBAC/allowlist) та параметризованих запитів при взаємодії виводу моделі з зовнішніми середовищами виконання (базами даних, інтерпретаторами).

Література

- 1. OWASP Top 10 for Large Language Model Applications 2025. URL: <https://owasp.org/www-project-top-10-for-large-language-model-applications/>
- 2. Greshake K., Abdelnabi S., Mishra S., Endres C., Holz T., Fritz M. Not what you’ve signed up for: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection // Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security (AISec ’23). 2023. P. 139–150.
- 3. Liu Y., Deng G., Li Y., Wang H., Zhang Y., Liu T., Wang Z., Wang X., Zheng Y. Prompt Injection attack against LLM-integrated Applications // IEEE Transactions on Software Engineering. 2024. Vol. 50, Issue 6. P. 1420–1438.
- 4. Perez F., Ribeiro I. Ignore Previous Prompt: Attack Techniques for Large Language Models // arXiv preprint arXiv:2211.09527. 2022. 8 p.

ДОСЛІДЖЕННЯ ВПЛИВУ РОЗМИТТЯ ЗА ГАУСОМ НА ШУМОВІ ХАРАКТЕРИСТИКИ ЦИФРОВОГО ЗОБРАЖЕННЯ

¹ Одеський національний морський університет, вул. Мечникова, 34, м. Одеса, 65029, vikazorilo@gmail.com

² Одеський національний морський університет, вул. Мечникова, 34, м. Одеса, 65029, dd.dashikis@gmail.com

Анотація. Важливим аспектом інформаційної та кібербезпеки критичної інфраструктури є можливість перевірки цілісності цифрової інформації. Зростання кількості фішингових атак, атак зі спуфінгом сигналів та інших загроз у сфері морського транспорту додатково підкреслює необхідність ретельного аналізу інформації та її джерел, а також забезпечення можливості перевірки цілісності даних, зокрема цифрових зображень. Одним із поширених способів порушення цілісності цифрових зображень є застосування гаусового розмиття, яке може використовуватися для приховування підроблених ділянок або обробки всього зображення. Наявні методи виявлення розмиття потребують подальшого вдосконалення й розвитку. У цьому дослідженні запропоновано метод виявлення розмиття, заснований на аналізі шумових характеристик зображення.

Ключові слова: кібербезпека критичної інфраструктури, виявлення порушень цілісності цифрових зображень, аналіз шуму цифрового зображення.

Цифрові зображення є одним із найбільш поширених видів інформації та активно використовуються у засобах масової інформації, соціальних мережах, наукових дослідженнях, системах відеоспостереження, моніторингу та інформаційній безпеці. Розвиток цифрових технологій, широке поширення графічних редакторів і стрімкий розвиток технологій штучного інтелекту значно спростили процес редагування зображень. Унаслідок цього зростає актуальність перевірки їхньої достовірності та цілісності. Особливого значення це набуває для критичної інфраструктури, зокрема морського транспорту, де фальсифікована інформація може бути використана для маніпуляції даними, дезінформації або приховування важливих деталей.

Одним із видів постобробки цифрових зображень є розмиття. Воно може застосовуватися як до окремих ділянок, що безпосередньо зазнали фальсифікації, так і до зображення в цілому як інструмент приховування слідів редагування. Розмиття порушує природні статистичні, спектральні та просторові властивості зображення, зокрема зменшує кількість високочастотних складових, згладжує текстури та знижує різкість контурів. Тому виявлення таких змін є важливим завданням цифрової криміналістики.

Перспективним напрямком виявлення редагування цифрових зображень є аналіз їхніх шумових характеристик. Під час формування цифрової фотографії внаслідок роботи сенсора камери та алгоритмів обробки виникає певний шумовий патерн. Втручання в структуру зображення може змінювати цей патерн, що створює можливість використання шуму як інформативної ознаки редагування.

Одним із відомих методів аналізу таких ознак є Error Level Analysis (ELA), який базується на особливостях JPEG-стиснення. Метод полягає у повторному збереженні зображення з певним рівнем якості та порівнянні отриманого файлу з оригіналом. У результаті формується матриця помилок, яка може бути представлена у вигляді зображення або гістограми. Нерівномірність шумових характеристик окремих ділянок може свідчити про попереднє редагування.

Для виявлення розмиття традиційно використовуються аналіз градієнтів, високочастотних компонентів та частотного спектра. У розмитих ділянках спостерігається зниження різкості контурів, зменшення амплітуди високочастотних складових і згладжування текстур. Водночас такі методи не є універсальними та можуть залежати від якості початкового зображення, умов його отримання і параметрів обробки.

Метою роботи є підвищення ефективності виявлення слідів редагування цифрових фотографій шляхом розроблення методу виявлення гаусового розмиття на основі аналізу шуму цифрового зображення.

Для дослідження можливостей виявлення обробки цифрових зображень фільтром розмиття за Гаусом проведено обчислювальний експеримент із використанням методу Error Level Analysis. Сформовано базу оригінальних цифрових зображень у кількості 100 фотографій, отриманих за допомогою стандартної цифрової камери та збережених у форматі JPEG. Для кожного зображення створено модифіковані версії шляхом застосування гаусового розмиття з радіусами 1 і 2 пікселі. Після обробки зображення зберігалися без втрат та у форматі JPEG із якістю 80 %. Для кожної версії за допомогою ELA отримувалася матриця шуму, яка надалі аналізувалася у вигляді гістограми.

На першому етапі було проаналізовано оригінальні зображення. Для них рівень помилок стиснення розподілявся достатньо рівномірно по всьому зображенню, а аномальних ділянок не спостерігалось. Гістограма шуму використовувалася як основа для порівняння з результатами оброблених зображень (рис.1).

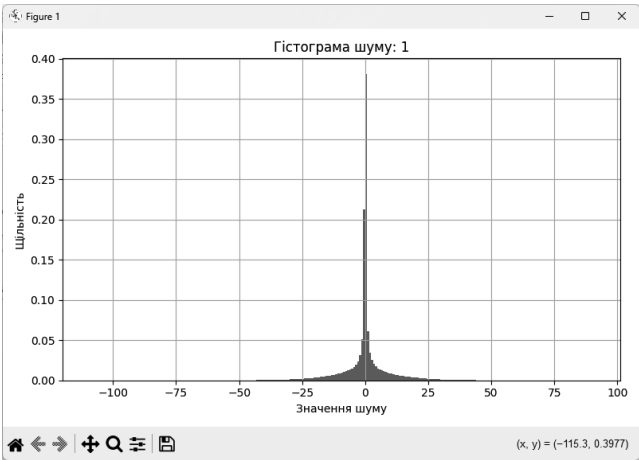


Рисунок 1 – Гістограма шуму оригінального зображення

На наступному етапі до зображень застосовано гаусове розмиття з радіусом 1 і 2 пікселі та виконано аналіз отриманих шумових гістограм. Встановлено, що характерною ознакою розмиття є зменшення амплітуди шумових значень і одночасне збільшення центрального піку гістограми.

Для розмиття за Гаусом із радіусом 1 піксель порівняно з оригіналом спостерігалось зменшення амплітуди значень шуму приблизно у 2,5 раза, а центральний пік гістограми збільшувався приблизно вдвічі. При збільшенні радіуса розмиття до 2 пікселів амплітуда значень зменшувалася більш ніж удесятеро, тоді як центральний пік збільшувався приблизно у п'ять разів. Крім того, для розмиття з радіусом 2 пікселі у деяких зображень з'являлися додаткові піки ліворуч і праворуч від центрального (рис.2).

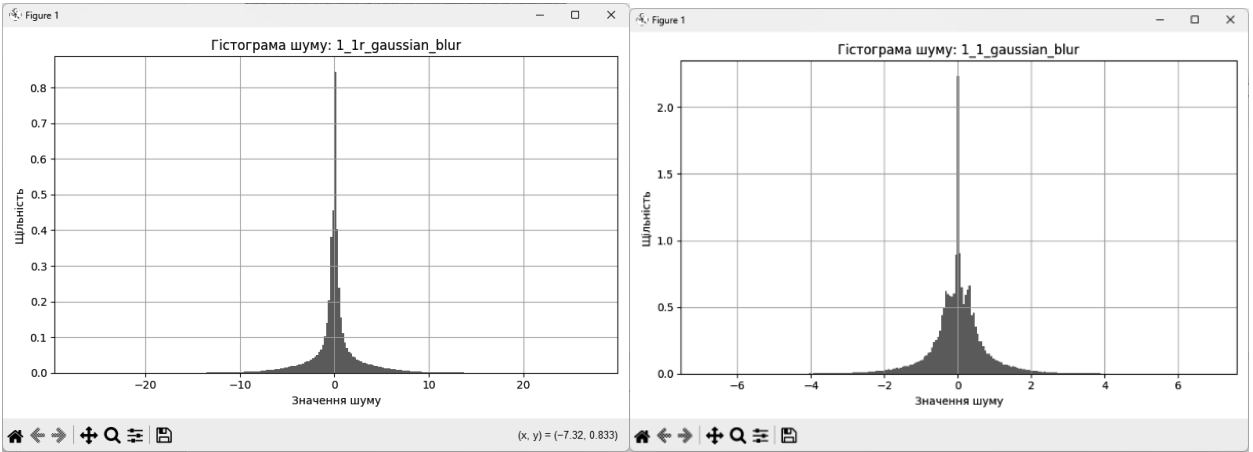


Рисунок 2 – Гістограма шуму відредагованих зображень

Збереження оброблених зображень із втратами дало аналогічний характер результатів. При цьому додаткові піки ліворуч і праворуч від центрального піку для радіуса 2 пікселі стали більш вираженими. Таким чином, встановлені зміни шумової гістограми є характерними для дослідженого типу обробки та можуть бути використані як ознаки наявності гаусового розмиття (рис.3).

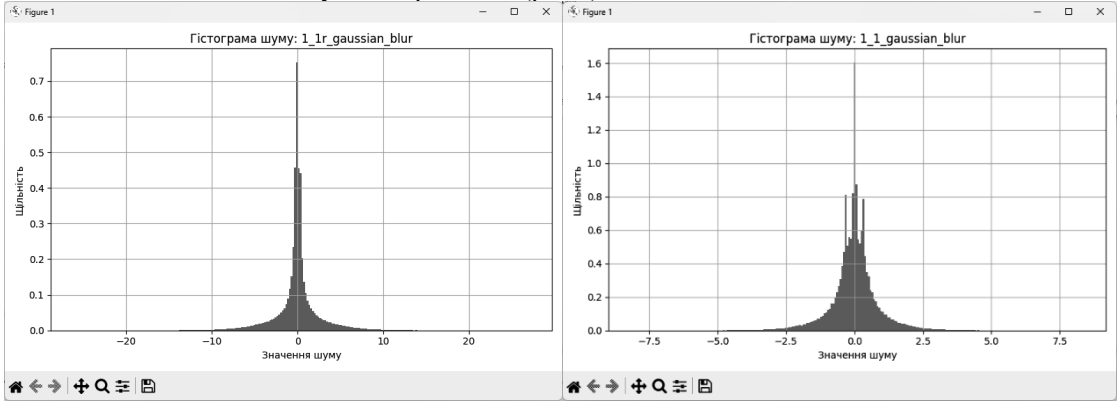


Рисунок 3 – Гістограма шуму відредагованих зображень з втратою якості

На основі отриманих результатів запропоновано модифікацію методу Error Level Analysis, яка передбачає кількісний аналіз гістограми шуму. Для матриці цифрового зображення Img за допомогою ELA формується матриця шуму $ImgN$, яка представляється у вигляді гістограми. Далі визначаються її амплітуда δ та центральний пік α . За результатами експерименту встановлено критерій: якщо $\delta < 25$ і $\alpha > 0,5$, зображення вважається розмитим за Гаусом; в інших випадках наявність такого фільтра вважається не підтвердженою.

Вказані порогові значення отримані експериментально та потребують уточнення шляхом розширення і урізноманітнення експериментальної бази зображень. Ефективність запропонованого підходу оцінювалася за показниками помилок першого та другого роду. Для дослідженої вибірки помилка першого роду становила 2 %, а помилка другого роду – 4,5 %.

Висновки. Проведене дослідження підтвердило можливість виявлення штучного гаусового розмиття цифрових зображень шляхом аналізу їхніх шумових характеристик. Використання методу Error Level Analysis у поєднанні з аналізом гістограм шуму дозволяє перейти від візуальної оцінки результатів ELA до кількісного визначення ознак обробки. Експериментально встановлено, що збільшення радіуса гаусового розмиття супроводжується суттєвим зменшенням амплітуди шуму та зростанням центрального піку гістограми.

Запропонована модифікація ELA може бути використана для автоматизованого виявлення розмиття цифрових зображень у системах інформаційної безпеки та цифрової криміналістики. Отримані результати мають практичне значення для перевірки цілісності цифрового контенту в умовах поширення графічного редагування та засобів штучного інтелекту. Подальші дослідження доцільно спрямувати на уточнення порогових значень, розширення експериментальної вибірки та перевірку стійкості методу до інших видів постобробки.

Література

- Gardella M., Musé P., Morel J.-M., Colom M. Forgery detection in digital images by multi-scale noise estimation // Journal of Imaging. 2021. Vol. 7, № 7. P. 119.
- Зоріло В. В. Вплив розмиття малого радіусу на формальні параметри цифрового зображення // Праці Одеського політехнічного університету. 2014. № 1(43). С. 137–142.

3. Зоріло В. В., Лебедєва О. Ю., Бензар Н. О. Розробка алгоритму виявлення зашумлення як фальсифікації цифрового зображення // Інформатика та математичні методи в моделюванні. 2021. Т. 11, № 1–2. С. 39–46.

УДК 004.056.5

Куліковський Д.В., Бабіч Ю.О.

КІБЕРБЕЗПЕКОВІ РИЗИКИ ГОЛОСОВОЇ БІОМЕТРІЇ ТА ПРАВОВІ НАСЛІДКИ ЇХ РЕАЛІЗАЦІЇ У ПЛАТІЖНИХ ОПЕРАЦІЯХ

Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна
denis.kylikovskii@gmail.com

Анотація. Попри численні технології автентифікації користувачів і багаторівневі системи захисту, стрімкий розвиток штучного інтелекту ставить під сумнів безпечність традиційних факторів автентифікації, насамперед голосової біометрії, яка дедалі частіше підтверджує особу в дистанційних сервісах. Простежено еволюцію факторів автентифікації, проаналізовано вразливість голосової біометрії до підробленого відтворення голосу, виявлено колізію між розподілом збитків за договором АТ КБ «ПриватБанк» і нормами Закону України «Про платіжні послуги» та практикою Верховного Суду. Запропоновано доповнити Положення Національного банку України про автентифікацію заборонаю використання голосової біометрії як елемента посиленої автентифікації за зразком NIST SP 800-63B-4.

Ключові слова: голосова біометрія, підроблене відтворення голосу, посилена автентифікація, простий електронний підпис, неакцептована платіжна операція, кібербезпека.

Методи автентифікації особи в дистанційних сервісах послідовно приходять на зміну одні одним. Кожне покоління усуває вразливості попереднього, але з часом саме стає вразливим унаслідок появи нових технологій кібератак. Нинішній етап цієї закономірності полягає у витісненні традиційних факторів голосовою біометрією, надійність якої підриває генеративний синтез мовлення. За даними компанії Pindrop, кількість спроб шахрайства з підробленим голосом зросла у 2024 році більш ніж на 1300%, у середньому з одного випадку на місяць до семи на день [1].

Вразливість властива самій технології, а тому стосується будь-яких дистанційних сервісів, що використовують голос для підтвердження особи. Банківський сектор обрано для поглибленого аналізу через доступність конкретного договору. Метою роботи є обґрунтування регуляторного рішення, здатного усунути виявлену проблему.

1. Еволюція методів автентифікації та причини втрати ними адекватності

Теорія інформаційної безпеки традиційно поділяє фактори автентифікації особи на три категорії:

- знання людини, наприклад пароль або ПІН-код;
- предмети, якими людина володіє, наприклад токен, що генерує одноразовий код, або мобільний телефон, на який надходить одноразовий пароль;
- біометричні характеристики людини.

Кожен із цих факторів проходить однаковий цикл. Він усуває проблеми попереднього покоління засобів автентифікації, певний час залишається надійним, а потім втрачає адекватність через появу нових технологій кібератак, орієнтованих саме на його специфічну вразливість (табл. 1).

Таблиця 1 – Еволюція факторів автентифікації та причини втрати ними адекватності

Фактор автентифікації	Приклад	Причина впровадження	Причина втрати адекватності
Знання	Пароль	Простота реалізації	Повторне використання паролів, витоки баз даних, фішинг, автоматизований підбір облікових даних
Володіння	Одноразовий пароль у SMS (SMS-OTP)	Захист від крадіжки статичного пароля	Підміна SIM-картки, вразливості протоколу SS7, перехоплення трафіку
Властивість	Голосова біометрія	Уявна неможливість підробити фізіологічну характеристику	Синтез і клонування голосу генеративними нейромережами

Слабкість SMS-OTP визнають і на рівні міжнародної стандартизації. Керівництво NIST SP 800-63B-4 класифікує SMS-OTP як «обмежений автентифікатор» через задокументовані атаки з підміною SIM-картки та вразливості протоколу SS7 [2].

2. Технічна вразливість систем голосової біометрії до підробленого відтворення голосу

Наукова спільнота працює над проблемою понад десять років. Перший конкурс міжнародної ініціативи ASVspoof відбувся у 2015 році. Результати вимірюють показником рівної частоти помилок (EER), причому менше значення відповідає надійнішому захисту. У 2019 році п'ять найкращих систем конкурсу досягли EER від 0,22% до 3,56% [3]. На складнішому наборі ASVspoof 5 у 2024 році п'ять найкращих систем показали EER від 8,61% до 14,75%, а базові системи RawNet2 та AASIST, ефективні на попередніх наборах, дали 36,04% і 29,12% відповідно [4]. Причиною є не деградація алгоритмів, а перехід до реалістичних умов, коли замість студійних записів приблизно ста дикторів використано записи понад чотирьох тисяч людей, зроблені різними побутовими пристроями, а атаки вперше оптимізували проти самих систем виявлення.

Ще у 2019 році клонування голосу вимагало навичок програмування, а вже у 2023 році модель Microsoft VALL-E відтворювала голос особи за трисекундним зразком аудіо [5]. До 2025–2026 років подібні рішення стали загальнодоступними онлайн-інструментами.

У 2026 році дослідники Fraunhofer AISEC провели найбільше на сьогодні дослідження сприйняття підробленого мовлення людиною. Воно охопило 35 532 оцінки від 1 768 учасників на матеріалі 138 систем синтезу та конверсії голосу. Підробки, створені комерційними сервісами та сучасними мовними моделями, учасники розпізнавали у 61,3–65,9% випадків. Водночас автори фіксують зміщення недовіри. Здатність розпізнавати підробки майже не змінилася з 2021 року, впавши з 72,9% до 71,2%, натомість здатність упізнавати справжні записи знизилася з 72,7% до 64,1% [6]. Тобто людина не лише не розпізнає синтез, а й дедалі частіше не довіряє автентичному голосу.

Атаки з підробленим голосом не обмежуються однією галуззю чи типом жертв. У 2024 році інженерна компанія Acur втратила понад 25 млн доларів США. Працівник гонконзького офісу здійснив 15 переказів після відеодзвінка, на якому всі інші учасники, включно з фінансовим директором, були згенеровані штучним інтелектом [7]. За даними FBI, у 2025 році від осіб віком 60 років і старше надійшло понад 3 100 скарг зі згадкою штучного інтелекту, а збитки за ними перевищили 352 млн доларів, з яких понад 5 млн припадає на схеми з клонуванням голосу родичів [8].

3. Рівні довіри до електронного підпису за законодавством України

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» встановлює три рівні довіри до електронного підпису (ст. 15): простий, що забезпечує найнижчий рівень достовірності, удосконалений і кваліфікований, який за юридичною силою прирівнюється до власноручного [9].

Саме простий електронний підпис, зокрема у формі голосового зліпка, банки використовують для підтвердження операцій із серйозними правовими наслідками.

4. Аналіз договірної практики українського банку

Договір про використання простого електронного підпису, укладений АТ КБ «ПриватБанк» з фізичною особою, визнає простим електронним підписом, зокрема, «біометричні дані Клієнта (голосовий зліпок, відбиток пальця, Face ID)», OTP-пароль, ПІН-код та підпис у системі голосового меню (IVR) (п. 2.2) [10]. Правочини, підписані у такий спосіб, сторони визнають дійсними та обов'язковими, «що не потребують додаткового підтвердження» (п. 2.6). Рішення про застосування конкретного способу підпису «Банк самостійно приймає» (п. 2.7), тому договір не передбачає механізму відмови клієнта від голосової автентифікації.

Пункт 2.8 договору розподіляє збитки так: «Банк відшкодовує збитки у розмірі, що не перевищує 100 грн, за умови надання підтверджуючих документів особою, яка вимагає відшкодування; відшкодування решти збитків покладається на Клієнта». Отже, банк самостійно обирає найслабший за законом вид підпису для операцій зі значними наслідками і водночас покладає основну частину ризику на клієнта.

5. Правова колізія у розподілі відповідальності

Стаття 86 Закону України «Про платіжні послуги» покладає тягар доведення на банк. Надавач платіжних послуг несе відповідальність, «якщо не доведе, що платіжні операції виконані цим надавачем платіжних послуг належним чином» (ч. 1), а у разі виконання неакцептованої платіжної операції зобов'язаний повернути її суму за рахунок власних коштів і сплатити пеню у розмірі подвійної облікової ставки Національного банку України за кожний день (ч. 12) [11]. Стаття 68 того самого Закону зобов'язує застосовувати посилену автентифікацію під час ініціювання дистанційної платіжної операції та вимагає використання даних, унікальних для кожної окремої операції (ч. 3, 5). Верховний Суд дотримується того самого підходу. У постанові від 09.04.2024 у справі № 521/20764/20 зазначено, що «саме банк має доводити, що користувач своїми діями чи бездіяльністю сприяв втраті, незаконному використанню» відповідних даних, а сам факт коректного введення вихідних даних цієї обставини не підтверджує [12] (табл. 2).

Таблиця 2 – Порівняння вимог законодавства та умов договору щодо простого електронного підпису		
Аспект	Закон України «Про платіжні послуги», практика ВС	Умови договору (п. 2.8)
Тягар доведення	Покладається на банк (ст. 86 ч. 1)	Не передбачений як умова відшкодування
Розмір відшкодування	Повна сума неакцептованої операції та пеня (ст. 86 ч. 12)	Не більше 100 грн, решта збитків покладається на клієнта
Вибір способу підпису	Посилена автентифікація обов’язкова (ст. 68 ч. 3, 5)	Спосіб визначає банк самостійно (п. 2.7)

Розбіжність між нормами закону й умовами договору стає відчутнішою з огляду на те, що голосову біометрію можна підробити за секунди аудіо, а розпізнати підробку не здатні ні пересічні люди, ні системи виявлення в реалістичних умовах.

6. Аналіз наявних підходів до вирішення проблеми

Наявні підходи до вирішення проблеми поділяються на три групи:

- технічні, до яких належать системи виявлення синтезу, змінювані контрольні фрази та поєднання кількох видів біометрії. Вони не усувають проблему принципово, оскільки перебувають у стані змагання з технологіями генерації, де перевага, за результатами ASVspoof 5, наразі на боці атаки;
- організаційні, до яких належать обмеження сум операцій, зворотний дзвінок і затримки виконання. Вони зменшують збитки, але не змінюють юридичного статусу підпису;
- регуляторні, які змінюють самі умови допустимості методу і діють незалежно від результату технологічного змагання.

У редакції SP 800-63B-4 NIST обрав саме регуляторний шлях. Документ встановлює, що біометрія має використовуватися лише як частина багатофакторної автентифікації разом із фізичним автентифікатором, а користувачу завжди має надаватися небіометрична альтернатива. Окремо встановлено, що порівняння біометричних даних на основі голосу застосовувати не дозволяється (в оригіналі «Biometric comparison based on voice SHALL NOT be used», п. 3.2.3.2) [2]. Підставою названо те, що біометричні характеристики не є секретом і можуть бути отримані онлайн без згоди особи, а показник хибних збігів не враховує активних атак, у яких зловмисник видає себе за іншу особу.

Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку, затверджене постановою Правління Національного банку України від 03.05.2023 № 58, відносить біометричні дані до категорії «притаманність» без обмежень щодо їх виду [13]. Водночас пункти 29 і 30 Положення вимагають унеможливити використання таких елементів сторонніми особами та гарантувати їх конфіденційність, а пункт 32 вимагає, щоб компрометація одного елемента не створювала загроз конфіденційності іншим.

Голосовий зліпок цим вимогам не відповідає, оскільки голос є публічно доступним, а його конфіденційність недосяжна. Крім того, передбачене договором поєднання голосового зліпка і Face ID (п. 2.2) не задовольняє вимогу незалежності, оскільки обидва елементи видобуваються з одного відеозапису.

Отже, пропонується доповнити Положення № 58 заборонаю використання голосової біометрії як елемента посиленої автентифікації за зразком NIST SP 800-63B-4, а також заборонаю поєднання елементів категорії «притаманність», які можуть бути отримані з одного джерела даних. Таке рішення не залежить від якості конкретних систем виявлення підробок і усуває колізію на тому рівні, де вона виникає.

Висновки. Голосова біометрія втратила властивості, які виправдовували її використання як фактора підтвердження платіжних операцій. Клонування голосу доступне за трисекундним зразком аудіо, системи виявлення підробок у реалістичних умовах показують EER 8,61–14,75%, а людина дедалі частіше не довіряє навіть автентичному мовленню. Договірна практика при цьому покладає основну частину ризику на клієнта, що не узгоджується зі статтею 86 Закону України «Про платіжні послуги» та практикою Верховного Суду. Технічні та організаційні заходи зменшують збитки, але не змінюють юридичного статусу підпису, тому обґрунтованим є регуляторне рішення. За результатами дослідження рекомендовано доповнити Положення НБУ № 58 заборонаю використання голосової біометрії як елемента посиленої автентифікації за зразком NIST SP 800-63B-4 та заборонаю поєднання елементів категорії «притаманність», які можуть бути отримані з одного джерела даних. До внесення таких змін банкам доцільно передбачити для клієнта можливість відмовитися від голосової автентифікації та привести умови договорів у відповідність до статті 86 Закону України «Про платіжні послуги».

Література

1. Pindrop’s 2025 Voice Intelligence & Security Report Reveals +1,300% Surge in Deepfake Fraud. PR Newswire, 2025. 12 June. URL: <https://www.prnewswire.com/news-releases/pindrops-2025-voice-intelligence--security-report-reveals-1-300-surge-in-deepfake-fraud-302479482.html> (дата звернення: 15.07.2026).

2. Temoshok D., Fenton J. L., Choong Y.-Y., Lefkovitz N., Regenscheid A., Richer J. P. Digital Identity Guidelines: Authentication and Authenticator Management. NIST Special Publication 800-63B-4. Gaithersburg: NIST, 2025. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf> (дата звернення: 06.08.2026).

3. Todisco M., Wang X., Vestman V., Sahidullah M., Delgado H., Nautsch A. et al. ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection. Proc. Interspeech. 2019. P. 1008–1012. URL: https://www.isca-archive.org/interspeech_2019/todisco19_interspeech.pdf (дата звернення: 06.08.2026).

4. Wang X., Delgado H., Tak H., Jung J., Shim H., Todisco M. et al. ASVspoof 5: Crowdsourced Speech Data, Deepfakes, and Adversarial Attacks at Scale. arXiv preprint. 2024. arXiv:2408.08739. URL: <https://arxiv.org/abs/2408.08739> (дата звернення: 18.07.2026).

5. Wang C., Chen S., Wu Y., Zhang Z., Zhou L., Liu S. et al. Neural Codec Language Models are Zero-Shot Text to Speech Synthesizers. arXiv preprint. 2023. arXiv:2301.02111. URL: <https://arxiv.org/abs/2301.02111> (дата звернення: 18.07.2026).

6. Müller N. M., Choong W. H. Eroding Trust in Real Speech: A Large-Scale Study of Human Audio Deepfake Perception. arXiv preprint. 2026. arXiv:2605.26136. URL: <https://arxiv.org/abs/2605.26136> (дата звернення: 18.07.2026).

7. Arup revealed as victim of \$25 million deepfake scam involving Hong Kong employee. CNN Business, 2024. URL: <https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk> (дата звернення: 22.07.2026).

8. 2025 Internet Crime Report. FBI, Internet Crime Complaint Center (IC3), 2026. URL: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf (дата звернення: 25.07.2026).

9. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 25.07.2026).

10. Kylikovskii D. Витяг з договору АТ КБ «ПриватБанк» про використання простого електронного підпису (фрагмент, персональні дані видалено). Zenodo, 2026. DOI: 10.5281/zenodo.21465296. URL: <https://zenodo.org/records/21465296> (дата звернення: 26.07.2026).

11. Про платіжні послуги: Закон України від 30.06.2021 № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20> (дата звернення: 25.07.2026).

12. Постанова Касаційного цивільного суду у складі Верховного Суду від 09.04.2024 у справі № 521/20764/20. URL: <https://reyestr.court.gov.ua/Review/118333777> (дата звернення: 06.08.2026).

13. Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку: постанова Правління Національного банку України від 03.05.2023 № 58. URL: https://bank.gov.ua/ua/legislation/Resolution_03052023_58 (дата звернення: 06.08.2026).

УДК 004.056.5

Клейн О. М., Савенко Б. О.

МЕТОД РАНЖУВАННЯ ПРИЧИННО-ПОВ’ЯЗАНИХ ПОДІЙ БАГАТОКРОКОВОЇ КОМП’ЮТЕРНОЇ АТАКИ НА ОСНОВІ БАЙЄСІВСЬКОЇ МЕРЕЖІ

Хмельницький національний університет, кафедра комп’ютерної інженерії та інформаційних систем, м. Хмельницький, Україна
olexandrkleyn@gmail.com; savenko_bohdan@ukr.net

Анотація. Запропоновано метод ранжування причинно-пов’язаних подій багатокрокової комп’ютерної атаки на основі байєсівської мережі. На відміну від оцінювання загального стану компрометації, вузлами моделі є спостережувані події та системні об’єкти, а результатом є компактний ранжований фрагмент причинного ланцюга навколо підтвердженого індикатора. Байєсівська мережа поєднує структурну залежність, локальну підтримку спостережень і часову допустимість. Для кількісної перевірки сформовано відтворюваний протокол на публічному наборі DARPA OpTC з оцінюванням Precision@K, Recall@K, NDCG@K, Brier score та скорочення графа.

Ключові слова: багатокрокова комп’ютерна атака; байєсівська мережа; причинний граф; ранжування подій; provenance; DARPA OpTC.

Під час розслідування багатокрокової комп’ютерної атаки аналітик зазвичай працює не з одним сповіщенням, а з великою кількістю пов’язаних процесів, файлових операцій, мережових з’єднань, подій автентифікації та службових дій. Навіть якщо початковий індикатор уже підтверджено, просте розширення його контексту на декілька переходів у графі швидко додає фонові процеси і створює великий фрагмент для ручного перегляду. У сучасних Bayesian attack graph підходах байєсівські мережі використовуються для

імовірнісного опису розвитку компрометації та неповного моніторингу [1, 2]. Водночас provenance-графи орієнтовані на причинні зв'язки між системними сутностями і дають змогу відтворювати контекст складних АРТ-сценаріїв [3].

У цій роботі ставиться інша задача: не визначити, чи скомпрометовано вузол мережі, і не передбачити наступний етап атаки, а ранжувати вже спостережувані події за їх імовірною належністю до одного причинно-пов'язаного атакуючого фрагмента. Вхідною точкою є підтверджена подія s , наприклад підозрілий запуск PowerShell або віддалене виконання. Виходом є впорядкований список подій і зв'язний підграф, що містить найбільш обґрунтований контекст до та після s . Така постановка дозволяє відокремити новий результат від задач класифікації окремих записів, оцінювання стану компрометації, марковського прогнозування та відновлення прихованих етапів.

Формування байєсівської мережі причинних подій

Початково з телеметрії формується локальний орієнтований причинний граф $G=(V,E)$. Вершина v_i відповідає події або системному об'єкту, що бере участь у події, а ребро (v_j,v_i) створюється, якщо пізніша подія може бути причинно продовжена від попередньої через спільний actorID/objectID, процес, користувача, вузол або мережеву взаємодію та не порушує часовий порядок. Для усунення циклів у локальній байєсівській моделі ребра орієнтуються за часом, тому для кожного v_i множина батьків $Pa(v_i)$ містить лише попередні причинно допустимі події.

Кожній вершині ставиться у відповідність бінарна випадкова змінна $X_i \in \{0,1\}$, де $X_i=1$ означає, що подія належить до поточного атакуючого ланцюга, а $X_i=0$ – що вона є фоновією відносно досліджуваного інциденту. Спільний розподіл байєсівської мережі має вигляд:

$$P(X_1,...,X_n)=\prod_{i=1}^n P(X_i \mid Pa(X_i))$$
 (1)

де $X_1,...,X_n$ – бінарні змінні подій у локальному графі; $Pa(X_i)$ – множина батьківських змінних, що причинно передують X_i ; $P(X_i|Pa(X_i))$ – умовна ймовірність належності події до атакуючого фрагмента за відомих станів її попередників; $\prod$ – операція добутку локальних умовних розподілів.

Для подій з декількома можливими попередниками використовується noisy-OR подання. Воно дає змогу підвищувати оцінку вершини, якщо її підтримує хоча б один сильний причинний попередник, але не вимагає одночасної активності всіх батьків:

$$P(X_i=1 \mid Pa_i)=1-(1-\pi_i)\prod_{j \in Pa_i}(1-\lambda_{ji}X_j)$$
 (2)

де π_i – локальна базова підтримка події, що враховує її власні спостережувані ознаки; Pa_i – множина батьків X_i ; $\lambda_{ji} \in [0;1]$ – сила причинної залежності від X_j до X_i ; X_j – бінарний стан батьківської події. Значення λ_{ji} визначається за типом зв'язку та часовою відстанню: пряме породження процесу або використання objectID/actorID отримує більшу вагу, ніж лише збіг hostname чи користувача.

Щоб не переносити в модель довільну вагу часу окремих евристичним доданком, часовий контекст використовується при оцінюванні самої сили причинного ребра:

$$\lambda_{ji} = \lambda_r^0 \cdot \exp(-\Delta t_{ji}/\sigma_r)$$
 (3)

де λ_r^0 – базова сила зв'язку типу r ; $\Delta t_{ji}=t_i-t_j$ – часовий інтервал між подіями; σ_r – масштаб часової чутливості для типу зв'язку r . Таким чином, швидке породження дочірнього процесу і мережеве з'єднання через кілька секунд підтримують один ланцюг сильніше, ніж формально пов'язані події, розділені тривалим інтервалом.

Спостережувана інформація подається множиною O . Для підтвердженого початкового індикатора стан відповідної змінної фіксується як доказ $X_s=1$. Для інших вершин можуть використовуватися м'які докази: тип дії, відповідність правилам SIEM, нетипова командна строка, критичність вузла або належність до операції, що узгоджується з MITRE ATT&CK [5]. Після введення доказів виконується байєсівський висновок і для кожної вершини обчислюється:

$$p_i = P(X_i=1 \mid O)$$
 (4)

де p_i – апостеріорна ймовірність належності події і до досліджуваного атакуючого фрагмента; O – сукупність жорстких і м'яких спостережень. На відміну від звичайного обходу графа, p_i залежить не лише від кількості переходів до початкового alert, а від усієї локальної структури причинних попередників і наявних доказів.



Рис. 1. Спрощена структура байєсівської мережі для ранжування причинно-пов'язаних подій

Після отримання апостеріорних оцінок формується зв'язний підграф H^* навколо початкової вершини s . Включаються лише вершини, які перевищують поріг θ і мають причинний шлях до або від s в межах локального часового вікна:

$$V^*=\{v_i \in V : p_i \geq \theta \wedge \text{Reach}(s,v_i)=1\}$$
 (5)

де V^* – множина відібраних вершин; θ – мінімальна апостеріорна оцінка; $\text{Reach}(s,v_i)$ – індикатор наявності причинно допустимого шляху між s та v_i . Зв'язність потрібна для того, щоб подія з високим локальним ризиком, але без причинного відношення до поточного інциденту, не потрапляла до результату лише через власну підозрілість.

Для представлення аналітику події додатково ранжуються за p_i . Якщо необхідно виділити один найбільш обґрунтований шлях, використовується оцінка ланцюга:

$$\Gamma^*=\arg \max_{\Gamma} [\sum_{v_i \in \Gamma} \ln p_i + \beta \sum_{(i,j) \in \Gamma} \ln \lambda_{ij}]$$
 (6)

де Γ – причинно допустимий шлях у H^* ; Γ^* – шлях із максимальною сумарною підтримкою; p_i – апостеріорна оцінка вершини; λ_{ij} – сила причинного ребра; β – коефіцієнт балансу між підтримкою окремих подій і безперервністю самого шляху. Такий результат є пояснюваним: для кожної вершини можна показати, які батьківські події та які спостереження збільшили її апостеріорну ймовірність.

Експериментальна база та протокол перевірки

Для перевірки методу обрано публічний набір Operationally Transparent Cyber (OpTC), сформований у межах робіт DARPA. У наборі endpoint-сенсори Windows формують eCAR-події, які містять timestamp, hostname, objectID, object/action, actorID, PID, principal та додаткові властивості. Офіційний опис OpTC вказує, що дані збиралися у масштабованому середовищі з сотнями Windows 10 вузлів, а під час evaluation-періоду на тлі легітимної активності виконувалися дії red team; окремо опубліковано ground truth [4]. Така структура придатна саме для перевірки причинного ранжування, оскільки actorID та objectID дозволяють пов'язувати породження процесів і наступні дії в єдиний provenance-фрагмент.

Експеримент пропонується виконувати на evaluation-частині eCAR. Для кожного епізоду з ground truth формується часовий інтервал і множина вузлів, після чого з eCAR вибираються події відповідних host та пов'язані з ними події через actorID/objectID. Початковим доказом s є одна подія, яка однозначно відповідає описаний red-team дії. Решта атакуючих подій не фіксуються як докази й мають бути підняті в ранжуванні самим байєсівським висновком.

Щоб не допустити витоку інформації між сценаріями, параметри λ^0 , σ_r , π_i та θ калібруються за схемою leave-one-scenario-out: одна red-team послідовність використовується лише для тестування, а інші – для оцінювання параметрів типів зв'язків і порога. У тестовому сценарії ground truth застосовується тільки для підрахунку метрик після формування ранжованого результату. Така схема принципово відрізняється від навчання і перевірки на випадково перемішаних записах, де сусідні події одного інциденту можуть опинитися одночасно в train і test.

Таблиця 1. Протокол експериментальної перевірки

Компонент	Основний варіант	Призначення
Дані	OpTC eCAR, evaluation	Причинні host/process/file/flow події
Еталон	OpTC Red Team Ground Truth	Позначення подій, що належать до атаки
Поділ	Leave-one-scenario-out	Виключення витоку сценарних шаблонів
Базові методи	k-hop; PageRank; static BN	Порівняння топологічного і ймовірнісного ранжування
Метрики	P@K; R@K; NDCG@K; Brier; reduction	Якість ранжування, калібрування і компактність
K	20; 50; 100	Бюджет ручного аналізу

Першим базовим методом є k-hop розширення: усі вершини на відстані не більше k від початкового alert отримують однаковий пріоритет. Другим є PageRank на локальному причинному графі, який ранжує структурно важливі вершини, але не використовує ground truth або умовні ймовірності. Третім є статична байєсівська мережа з однаковими λ для всіх типів ребер; вона дозволяє відокремити внесок типу причинного зв'язку і часової чутливості запропонованої моделі.

Основними метриками є Precision@K та Recall@K для $K \in \{20,50,100\}$. Precision@K показує, яка частка перших K подій належить до еталонного атакуючого фрагмента, а Recall@K – яку частку еталонних подій вдалося підняти в цей бюджет перегляду. NDCG@K враховує позицію релевантних подій у списку, тому винагороджує метод, який переміщує критичні причинні події ближче до початку. Brier score використовується для перевірки калібрування p_i , а коефіцієнт скорочення $1-|V^*|/|V|$ характеризує, яку частину локального графа можна не передавати на ручний аналіз.

Порогові параметри не повинні підбиратися за тестовим сценарієм. Для кожної training-комбінації θ вибирається за максимумом NDCG@50 при обмеженні Recall@100 не нижче заданого рівня. Після цього θ фіксується і переноситься на unseen scenario. Окремо виконується абляція: без часової експоненти у формулі (3), без розрізнення типів зв'язків та без soft evidence.

Послідовність реалізації методу

Практична реалізація виконується у сім кроків. На першому кроці визначається початковий індикатор s та локальне часове вікно. Вікно не повинно охоплювати весь журнал: його задача полягає лише у формуванні початкової області, в якій ще зберігається причинний зв’язок із alert. На другому кроці eCAR-події перетворюються на вершини з уніфікованими атрибутами timestamp, hostname, object, action, actorID, objectID, principal і process context. На третьому кроці створюються орієнтовані ребра. Найсильнішим вважається зв’язок, коли objectID попередньої події стає actorID наступної, оскільки це безпосередньо відображає продовження дії тим самим системним об’єктом. Допоміжними є зв’язки за процесом, користувачем, вузлом і мережевою адресою.

На четвертому кроці виконується перетворення локального причинного графа в DAG. Якщо дві події мають взаємні або циклічні системні зв’язки, для байесівської мережі зберігається напрямок, що не суперечить часовому порядку, а інформація про зворотну залежність залишається атрибутом ребра. На п’ятому кроці задаються локальні умовні розподіли. Для першого запуску типам відношень призначаються параметри λ_r^0 , отримані з training-сценаріїв, після чого вони модифікуються часовою експонентою. Базова підтримка π_i визначається за типом події та її локальними ознаками, але не може самостійно включити подію до фінального ланцюга без причинного шляху до s.

На шостому кроці вводяться докази і виконується байесівський висновок. Початковий alert є жорстким доказом, а інші ознаки використовуються як soft evidence. У локальному DAG можливо застосовувати точний висновок за топологічним порядком, поки розмір підграфа залишається обмеженим. Якщо кількість вершин перевищує заданий бюджет, перед інференсом виконується структурне обрізання слабких ребер з $\lambda_{ij} < \lambda_{min}$. На сьомому кроці обчислюються p_i , формується V^* , а події сортуються за апостеріорною оцінкою. Разом із результатом зберігається коротке пояснення: значення p_i , найсильніший батьківський зв’язок, часовий інтервал до попередника та спостереження, яке найбільше змінило оцінку.

Підготовка даних OpTC до експерименту

Для відтворюваного експерименту сирі eCAR-записи не змішуються в один глобальний граф. Спочатку з ground truth виділяється конкретний red-team епізод із часовими межами та набором скомпрометованих вузлів. Далі до нього додається контрольований фон з тих самих host bucket і сусідніх часових інтервалів. Це важливо, оскільки випадковий benign фон з іншого дня може бути занадто легким для ранжування і не відображати реальні hard-negative події, які з’являються одночасно з атакою. У підграф включаються PROCESS, FILE, FLOW, SHELL, REGISTRY та інші типи, якщо вони причинно пов’язані з обраними actorID/objectID; тип події не використовується як автоматична мітка атаки.

Процес зіставлення з еталоном виконується після побудови графа. Для кожного описаного в ground truth кроку фіксуються відомі hostname, процес, команда, часовий інтервал та інші доступні ідентифікатори. Потім знаходяться eCAR-події, які одночасно задовольняють часову й об’єктну відповідність. Якщо один крок ground truth породжує декілька технічних записів, усі вони можуть бути позначені як релевантні до одного атакуючого фрагмента. Події, які не мають достатньої відповідності, не оголошуються автоматично benign: вони залишаються немаркованими і можуть використовуватися лише як фон для ранжування, але не для навчання параметрів як гарантовано негативні приклади. Такий підхід зменшує ризик помилкової розмітки через неповноту документації.

Таблиця 2. Параметри, що оцінюються тільки на training-сценаріях

Параметр	Зміст	Оцінювання	Фіксація для test
λ_r^0	Базова сила типу ребра	Підтримані причинні переходи	Так
σ_r	Часова чутливість	Квантиль Δt	Так
π_i	Підтримка типу події	Training evidence	Так
θ	Поріг формування V^*	NDCG@50 + Recall constraint	Так

Для оцінювання λ_r^0 не потрібно навчати окремих класифікатор. Параметр може визначатися як згладжена частка випадків, у яких зв’язок типу r з’єднує дві еталононо релевантні події серед усіх розглянутих зв’язків цього типу в training-сценаріях. Згладжування необхідне для рідкісних типів, інакше одиничний збіг дасть $\lambda_r^0=1$. Значення σ_r оцінюються окремо для process, file та network відношень, оскільки характерний часовий масштаб між породженням процесів і міжмережевими діями відрізняється. Усі параметри зберігаються перед відкриттям test ground truth.

Окремо перевіряється стійкість до неповних спостережень. У test-фрагменті послідовно приховується 10, 20 і 30 % м’яких доказів O, але самі еталонні події не видаляються з графа. Метод повинен зберігати високе ранжування події за рахунок причинних попередників, навіть якщо її локальний evidence відсутній. Друга стрес-умова полягає у додаванні в локальне вікно причинно близьких, але ground-truth-нерелевантних процесів з того самого host.

Наукова новизна, межі та очікуваний результат

Наукова новизна запропонованого підходу полягає у використанні байесівської мережі не для оцінювання загального стану компрометації вузлів, а для подієвого ранжування всередині локального provenance-фрагмента. Кожна спостережувана подія отримує апостеріорну оцінку належності до конкретного інциденту, а причинні залежності задаються безпосередньо зв’язками eCAR і їх часовою близькістю. Додаткова

вимога зв’язності з початковим alert відсікає локально підозрілі, але причинно незалежні події. У результаті аналітик отримує не бінарне рішення «атака/норма» і не прогноз наступної фази, а компактний упорядкований ланцюг доказів.

Метод має кілька обмежень. По-перше, побудова DAG за часовим порядком спрощує ситуації з паралельними процесами й циклічними системними взаємодіями. По-друге, якість λ_r^0 залежить від того, наскільки стабільно типи eCAR-зв’язків переносяться між сценаріями. По-третє, ground truth OpTC описує red-team активність, але не є автоматичною повною розміткою кожного фонового запису, тому процедуру зіставлення подій з еталоном необхідно документувати окремо.

Очікуваним практичним результатом є зменшення кількості подій, які аналітик переглядає після первинного alert, при збереженні більшості еталоонних атакуювальних дій у верхній частині ранжування. Додатковою перевагою є пояснюваність: для будь-якої вершини можна показати її p_i , батьківські події, типи причинних зв’язків і спостереження, що змінили апостеріорну оцінку. Такий формат придатний для інтеграції з SIEM як окремий шар post-alert investigation, який запускається після спрацювання правила або аналітичної моделі.

Висновки

Запропоновано метод ранжування причинно-пов’язаних подій багатокрокової комп’ютерної атаки на основі байесівської мережі. Метод формує локальний причинний DAG із спостережуваних подій, описує їх належність до атакуючого фрагмента бінарними випадковими змінними, використовує noisy-OR для поєднання декількох причинних попередників і виконує апостеріорне ранжування після введення підтвердженого індикатора та додаткових спостережень. Для перевірки підготовлено відтворюваний протокол на DARPA OpTC з leave-one-scenario-out поділом, базовими графовими методами та метриками ранжування, калібрування і скорочення графа. Така постановка формує окрему задачу графового аналізу, відмінну від класифікації атак, реконструкції прихованих етапів і прогнозування наступного стану.

Література

1. Kazeminajafabadi A., Imani M. Optimal monitoring and attack detection of networks modeled by Bayesian attack graphs. Cybersecurity. 2023. Vol. 6. Art. 22. DOI: 10.1186/s42400-023-00155-y.
2. Sahu A., Davis K. Inferring adversarial behaviour in cyber-physical power systems using a Bayesian attack graph approach. IET Cyber-Physical Systems: Theory & Applications. 2023. DOI: 10.1049/cps2.12047.
3. Cui M., Jiang Z., Li S., Ma C., Zhang K., Yang P., Feng H. MGDA: A provenance graph-based framework for threat detection and attack scenario reconstruction. Computer Networks. 2026. Vol. 274. Art. 111806. DOI: 10.1016/j.comnet.2025.111806.
4. Five Directions. Operationally Transparent Cyber (OpTC) Data Release and eCAR Model. DARPA CHASE. URL: <https://github.com/FiveDirections/OpTC-data> (дата звернення: 19.08.2026).
5. MITRE. MITRE ATT&CK: Enterprise Matrix. URL: <https://attack.mitre.org/matrices/enterprise/> (дата звернення: 19.08.2026).

УДК 004.056

Михайленко Г. О.

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ N8N

Державний університет інтелектуальних технологій і зв’язку

migeo9178@gmail.com

Анотація. Розглянуто можливості використання платформи n8n для автоматизації процесів у SOC. Визначено її роль як оркестраційного рівня між засобами виявлення загроз і процесами реагування, а також основні сценарії застосування: нормалізація, enrichment, маршрутизація та підтримка incident response. Окрему увагу приділено питанням безпеки платформи, обмеженням автоматизації та практичному досвіду її корпоративного використання.

Ключові слова: n8n, SOC, SOAR, автоматизація, оркестрація, incident response, security automation.

Сучасний центр моніторингу та реагування на кіберінциденти (SOC) функціонує в умовах одночасного використання значної кількості взаємопов’язаних засобів захисту, серед яких SIEM, EDR, IDS/IPS, сканери вразливостей, каталоги користувачів, системи інвентаризації активів та сервіси threat intelligence. За таких умов завдання SOC полягає не лише у виявленні потенційно небезпечної події, а й у швидкому формуванні достатнього контексту для її подальшого аналізу. Після отримання сповіщення аналітик повинен визначити критичність активу, ідентифікувати пов’язаного користувача, перевірити репутацію мережевих індикаторів, знайти пов’язані події в інших системах та зафіксувати результати проведеного аналізу.

Актуальність автоматизації таких операцій підтверджується результатами дослідження SANS 2024, відповідно до якого 59 % організацій використовують у SOC понад десять різних засобів безпеки. Найчастіше

автоматизація застосовується для реагування на фішингові атаки – 52 %, керування вразливостями – 43 % та збагачення даних – 42 %. Водночас 68 % респондентів визначили інженерні витрати на створення, інтеграцію та подальшу підтримку автоматизованих сценаріїв як одну з найбільш складних характеристик впровадження SOAR [1]. Таким чином, окремою проблемою стає не лише наявність засобів автоматизації, а й побудова гнучкого механізму взаємодії між уже наявними компонентами інформаційної безпеки.

Одним із можливих підходів до вирішення цього завдання є використання n8n як проміжного оркестраційного рівня між системами виявлення загроз та процесами реагування. n8n є універсальною low-code платформою автоматизації робочих процесів, яка дозволяє інтегрувати різні інформаційні системи за допомогою API, webhooks, готових модулів та програмного коду.

У роботі R. N. Mankame роль n8n у процесах кібербезпеки визначається саме як керування рухом інформації після формування security-сигналу: приймання події, нормалізація її структури, збагачення внутрішнім та зовнішнім контекстом, маршрутизація відповідно до заданих правил, виконання допоміжних операцій і фіксація результатів [2]. Отже, n8n у такій архітектурі не є засобом безпосереднього виявлення атак. Він не замінює SIEM, EDR або IDS/IPS і не виконує самостійний аналіз мережевого трафіку. Його призначення полягає у зв’язуванні результатів роботи різних засобів захисту в єдиний керований процес реагування.

Основний алгоритм використання n8n у кібербезпеці
Практичне використання n8n у SOC доцільно розглядати як послідовність операцій, які виконуються після отримання сповіщення від одного із засобів виявлення загроз. Основний алгоритм ОСНОВ такої взаємодії наведено на рис. 1.



Рисунок 1 – Сценарії використання n8n

Першим етапом є нормалізація сповіщень, отриманих від різних джерел. Оскільки SIEM, EDR, IDS/IPS та інші системи можуть використовувати різні назви полів, формати часових міток, рівні критичності та ідентифікатори об’єктів, n8n може приводити отримані дані до єдиної внутрішньої структури. Це дозволяє використовувати спільну логіку подальшої обробки незалежно від того, яка саме система сформувала початкове сповіщення.

Наступним етапом є збагачення події контекстною інформацією (enrichment). На цьому етапі до початкового alert можуть автоматично додаватися дані щодо критичності активу, ролі та привілеїв користувача, попередньої активності, наявності пов’язаних подій, а також репутації IP-адрес, доменів, URL або хешів файлів. Таким чином, окреме технічне сповіщення перетворюється на більш повний набір даних, придатний для прийняття рішення аналітиком.

Після збагачення виконується маршрутизація події відповідно до визначених правил. Наприклад, події з низьким рівнем ризику можуть автоматично реєструватися без подальшої ескалації, події з неоднозначними характеристиками – передаватися аналітику для ручної перевірки, а висококритичні події – негайно спрямовуватися відповідальній команді реагування. Такий підхід дозволяє зменшити кількість рутинних операцій та зосередити увагу аналітиків на подіях, що потребують експертної оцінки.

Окрему групу становлять сценарії операційної підтримки incident response. За допомогою n8n може бути автоматизоване створення ticket у системі керування інцидентами, повідомлення відповідальних осіб, збір додаткових артефактів, формування часової послідовності дій та передавання інформації між різними системами. У результаті n8n виконує роль координаційного компонента, який забезпечує послідовність виконання окремих етапів реагування.

Водночас не всі дії доцільно виконувати повністю автоматично. Для операцій, здатних вплинути на доступність інформаційних систем, може застосовуватися підхід human-in-the-loop. У такому випадку workflow автоматично збирає необхідний контекст і готує дію, однак перед блокуванням IP-адреси, облікового запису, ізоляцією робочої станції або виконанням іншої критичної операції процес призупиняється до отримання підтвердження від аналітика.

Необхідність такого обмеження автоматизації підтверджується результатами наукових досліджень SOAR-платформ. Bridges та співавтори провели контрольоване дослідження за участю 24 користувачів і шести комерційних SOAR-рішень. Отримані результати показали, що автоматизація здатна підвищити ефективність розслідування та зменшити кількість перемикань між різними інструментами. Водночас у частині сценаріїв

спостерігалось зниження точності та повноти сформованих ticket. Досвідчені аналітики також відзначали ризик надмірної автоматизації та віддавали перевагу системам, які підтримують процес прийняття рішення, але не повністю замінюють оператора [3].

Таким чином, під час використання n8n у SOC доцільно розмежовувати автоматизацію рутинних і критичних операцій. Детерміновані дії, зокрема нормалізація даних, отримання інформації з зовнішніх джерел, створення записів та надсилання повідомлень, можуть виконуватися автоматично. Натомість операції, які можуть призвести до блокування користувача, ізоляції вузла або порушення доступності сервісу, доцільно виконувати лише після підтвердження уповноваженим фахівцем.

За своїми функціональними можливостями n8n частково перетинається зі спеціалізованими SOAR-рішеннями, однак не є їх повноцінною заміною. Основною відмінністю є початкове призначення платформ: n8n є універсальним засобом workflow-оркестрації, тоді як SOAR-платформи створюються безпосередньо для автоматизації процесів security operations. Порівняння основних характеристик наведено в табл. 1.

Таблиця 1 – Порівняння n8n та спеціалізованої SOAR-платформи		
Критерій	n8n	Спеціалізований SOAR
Основне призначення	Універсальна workflow-оркестрація	Оркестрація та автоматизація реагування у SOC
Детектування загроз	Не є основною функцією; отримує готові події від зовнішніх систем	Переважно використовує сигнали SIEM, EDR, IDS/IPS та інших засобів
Case management	Реалізується через інтеграцію із зовнішньою системою або окремий workflow	Зазвичай є вбудованою складовою платформи
Інтеграції	API, webhooks, готові nodes, JavaScript/Python	Спеціалізовані security-конектори та playbooks
Human-in-the-loop	Реалізується за допомогою умов, пауз та підтверджень у workflow	Типовий механізм виконання playbook
Сфера застосування	SOC, IT-операції та бізнес-процеси	Переважно security operations

Доцільність використання n8n у SOC полягає не у заміні засобів виявлення загроз або повноцінної SOAR-платформи, а у створенні гнучкого оркестраційного рівня між наявними системами безпеки. Такий рівень дозволяє автоматизувати передачу та нормалізацію подій, їх збагачення контекстом, маршрутизацію, документування та окремі операції реагування, одночасно зберігаючи участь аналітика у прийнятті критичних рішень.

Практичні результати використання n8n

Практична доцільність використання n8n у процесах security automation підтверджується не лише можливістю побудови окремих workflow, а й прикладами його застосування у корпоративних середовищах. Одним із публічно описаних кейсів є використання платформи у Vodafone UK, де n8n застосовується для monitoring, автоматизованих перевірок та окремих SOAR-процесів у середовищі, що обробляє мільярди security events на місяць.

За даними корпоративного case study n8n, починаючи із серпня 2024 року у Vodafone було створено та введено в експлуатацію 33 workflow. Заявлений результат їх використання становить понад 5000 людино-днів заощадженого робочого часу та близько £2,2 млн уникнених витрат. У 2025 році також повідомлялося про подальший економічний ефект на рівні приблизно £300 тис. на місяць [4]. Один із реалізованих workflow виконує перевірку критичних потоків даних кожні п’ять хвилин, здійснює первинний triage та автоматично створює ticket для відповідальної команди у разі виявлення проблеми.

Наведені показники характеризують конкретне корпоративне впровадження і походять із case study, опублікованого постачальником платформи. Тому їх доцільно розглядати не як універсальну оцінку продуктивності n8n, а як практичний приклад того, як оркестрація повторюваних операцій може впливати на витрати часу та ресурсів у масштабовому SOC-середовищі.

Важливою особливістю кейсу Vodafone є те, що отриманий ефект пов’язаний не лише з кількістю створених workflow, а й з організацією їх життєвого циклу. Автоматизовані процеси були інтегровані у CI/CD-підхід із розділенням етапів розроблення, тестування та продуктивного використання. Для security automation така модель має принципове значення, оскільки навіть незначна зміна логіки workflow може вплинути на обробку великої кількості подій або ініціювати небажану дію в інтегрованій системі. Тому версіонування, тестування, централізоване журналювання та контроль змін повинні розглядатися як складові експлуатації автоматизованих сценаріїв, а не лише як допоміжні функції розроблення.

Безпека n8n

Зі збільшенням ролі n8n у процесах реагування зростає і критичність самої платформи. Оркестратор фактично стає привілейованим компонентом інфраструктури, оскільки може мати доступ до API різних систем, баз даних, файлової системи, webhook-ів, сервісних облікових записів та зовнішніх ресурсів. Унаслідок цього компрометація n8n потенційно створює не локальну, а міжсистемну загрозу, оскільки може надати зловмиснику доступ одночасно до декількох інтегрованих компонентів.

Офіційний механізм security audit n8n враховує низку ризиків, характерних для такого середовища. До них належать невикористані або надмірно привілейовані credentials, потенційно небезпечні SQL expressions, nodes із доступом до файлової системи, використання risky, community або custom nodes, недостатньо захищені webhook-и, відсутність окремих security settings, а також використання застарілої версії платформи [5].

Таким чином, продуктивне використання n8n у SOC повинно передбачати застосування принципу мінімальних привілеїв для service accounts, окреме керування секретами, захист webhook-ів, ізоляцію production-середовища, регулярне оновлення платформи та централізоване журналювання виконань. Крім того, критичні workflow доцільно розробляти і тестувати окремо від продуктивного середовища, особливо якщо вони можуть виконувати блокування, зміну конфігурації або інші дії, що впливають на доступність систем.

Використання n8n у security automation створює подвійний ефект: з одного боку, платформа зменшує кількість ручних операцій та спрощує взаємодію між засобами захисту, а з іншого – сама стає компонентом, для якого необхідно забезпечити належний рівень захисту та контроль змін.

Висновки. У результаті проведеного аналізу встановлено, що n8n доцільно використовувати в SOC як оркестраційний рівень між засобами виявлення загроз та процесами реагування. Платформа дозволяє автоматизувати нормалізацію сповіщень, їх збагачення контекстною інформацією, маршрутизацію та окремі операції incident response.

Також визначено, що n8n не є заміною SIEM, EDR, IDS/IPS або спеціалізованої SOAR-платформи, а виконує функцію зв’язування окремих засобів безпеки в єдиний керований процес. При цьому рутинні операції можуть автоматизуватися повністю, тоді як критичні дії доцільно виконувати із збереженням контролю аналітика.

Аналіз практичного кейсу Vodafone UK підтвердив можливість використання n8n у масштабному корпоративному SOC та показав потенціал автоматизації для зменшення витрат часу і ресурсів. Водночас встановлено, що сама платформа потребує належного захисту, оскільки має доступ до декількох інтегрованих систем та може бути критичним компонентом інфраструктури.

Література

1. Orlando M. The State of Automation in Security Operations: A SANS Survey. SANS Institute. 2024. URL: <https://www.sans.org/white-papers/state-automation-security-operations-sans-survey>.
2. Mankame R. N. n8n for Cybersecurity Automation: A Practical, Honest Exploration. Medium. 18.12.2025. URL: <https://medium.com/@cyrig/n8n-for-cybersecurity-automation-a-practical-honest-exploration-fecd681b32e8>.
3. Bridges R. A., Rice A. E., Oesch S. et al. Testing SOAR Tools in Use. Computers & Security. 2023. Vol. 129. Article 103201. DOI: 10.1016/j.cose.2023.103201.
4. n8n. Leveraging Automation in Cybersecurity: Vodafone Case Study. URL: <https://n8n.io/case-studies/vodafone/>.
5. n8n Docs. Security Audit. URL: <https://docs.n8n.io/hosting/securing/security-audit/>.

УДК 004(056.53):413.4)

¹Мохор В.В., ²Дорогий Я.Ю., ¹Ракович В.С., ^{1,3}Цуркан В.В.

ПОГЛЯД НА ПАРАДИГМУ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

¹Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України

²Донецький національний технічний університет

³Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
v.mokhor@gmail.com, yaroslav.dorohyi@donntu.edu.ua, covlad@ukr.net, v.v.tsurkan@gmail.com

Анотація. Проаналізовано заходи забезпечування непорушності надання об’єктами критичної інфраструктури життєво важливих функцій та/або послуг. Показано зосередженість заходів виявлення і реагування на кіберінцидентах, кібератаках, кіберзагрозах. Серед основних джерел інформації про них виокремлено працівників об’єктів критичної інфраструктури. Ефективність даної діяльності зведено до необхідності визначення парадигми повідомлення про події кібербезпеки. Так, буде враховано, по-перше, інтегрування України в європейський та євроатлантичний простори; по-друге, узгоджування вітчизняного законодавства з міжнародним, регіональним і національним. Це дозволить розробити механізм повідомлення про події кібербезпеки. І, забезпечити обізнаність працівників об’єктів критичної інфраструктури про те, що протягом якого проміжку часу та кому доводити до відома.

Ключові слова: об’єкт критичної інфраструктури, подія кібербезпеки, повідомлення про подію кібербезпеки, парадигма повідомлення, механізм повідомлення, погляд на парадигму.

Унеможливлення завдань шкоди життєво важливим національним інтересам досягається протидіянням запобіганню порушень функціонування об’єктів критичної інфраструктури. Така діяльність пов’язується насамперед з цінністю кожного з них для економіки, національної безпеки та оборони [1–3]. Вона орієнтована на забезпечування функційності, безперервності роботи, відновлюваності та стійкості об’єктів критичної інфраструктури. Тому станом надання ними життєво важливих функцій та/або послуг з прийнятними рівнем ризиків визначається кібербезпека [3]. На неї впливають як навмисні, так і ненавмисні події, настання яких може призводити до порушень, наприклад, систем електронних комунікацій, систем управління технологічними процесами, об’єкта критичної інфраструктури. Це спричиняє виникнення інцидентів кібербезпеки та, як наслідок, спонукає до своєчасного виявлення і реагування на них [3]. Реалізування зазначених заходів передбачається відповідним національним планом. Для цього на об’єктах критичної інфраструктури призначається відповідальна особа або створюється підрозділ. В обох випадках основними завданням є управління, координування, контролювання реалізованості вимог до кібербезпеки об’єктів критичної інфраструктури [1, 3, 4]. Насамперед стосовно обов’язковості інформування секторального органу про інциденти встановленим порядком. Задоволення цієї вимоги визначається обізнаністю працівників про те, що протягом якого проміжку часу та кому доводити до відома [1]. Цим обґрунтовується актуальність визначення і, як наслідок, викладання погляду на парадигму повідомлення про події кібербезпеки об’єктів критичної інфраструктури.

Прагненнями України до інтегрування в європейський та євроатлантичний простори розвивається діяльність забезпечування безпеки об’єктів критичної інфраструктури [2, 3]. Це пояснюється необхідністю узгоджування вітчизняного законодавства з міжнародним, регіональним і національним правом. Крім того, взаємодіянням національної системи захисту критичної інфраструктури з подібними міжнародними системами. Серед потенційним напрямів гармонізувань виокремлюються нормативні документи міжнародної організації зі стандартизації, Європейського союзу, Національного інституту стандартів і технологій [1, 4–6]. З одного боку, дане виокремлення дозволяє враховувати поточні тенденції розвитку вітчизняного законодавства у сфері кібербезпеки. Тоді як з іншого – імплементувати найкращі світові практики для виявлення і реагування на інциденти. Власне з огляду на [6], посадових осіб операторів, власників або розпорядників об’єктів критичної інфраструктури зобов’язано повідомляти встановленим порядком про кіберінциденти, кібератаки та кіберзагрози [6]. До того ж виконувати інші зобов’язання стосовно надання життєво важливих функцій та/або послуг. Це стосується і виявлення, реагування на інциденти кібербезпеки об’єктів критичної інфраструктури. Для цього встановлюються підстави, строки, порядок і звітність ужиття даних заходів. Тож оператори, власники або розпорядники об’єктів критичної інфраструктури повинні забезпечувати своєчасність їх виконання після отримання вимоги [7]. Її задоволення досягається за принципами забезпечення безперервності функціонування об’єктів критичної інфраструктури.

Відповідно до [7] виявлення і реагування на інциденти кібербезпеки окрім заходу є вимогою до операторів, власників, розпорядників об’єктів критичної інфраструктури. В останньому випадку нею встановлюються дії для зменшування наслідків настання інцидентів, запобігання реалізуванню загроз, відновлення сталого та надійного надання життєво важливих функцій та/або послуг [8]. Так, за Національним планом реагування на інциденти передусь підготовляння. У його межах передбачається вивчення і досліджування відомих кіберінцидентів, кібератак, кіберзагроз, а також розроблення відповідних методів і механізмів протидіяння. Завдяки цьому створюються організаційні, технічні, кадрові умови, зокрема, взаємодіяння з керівниками, підрозділами кіберзахисту. Протягом виявлення, аналізування, інформування про кіберінциденти отримується, обробляється і передається інформація про події. Вони можуть відноситися до одного з класів: кіберінцидент, кібератака, кіберзагроза. Повідомлення про них передбачено безперервно в режимі реального часу. Серед джерел виявлення кіберінцидентів, кібератак, кіберзагроз виокремлено суб’єктів національної системи реагування, забезпечування кібербезпеки та працівників. Тоді як протягом стримування, усунування наслідків та відновлення вживаються заходи зменшування негативного впливу на надання життєво важливих функцій та/або послуг. За результатами таких дій аналізується ефективність реагування на кіберінциденти, кібератаки або кіберзагрози [7, 8].

З огляду на [2, 3, 4, 7, 8], запорукою ефективності реалізування заходів виявлення і реагування на інциденти кібербезпеки об’єктів критичної інфраструктури є повідомлення про події. Для цього передбачається збирання і оброблення наявної інформації. Тож доцільно визначити потенційні джерела її отримання, наприклад [8], окрім суб’єктів національної системи реагування. Іншим важливим аспектом є обізнаність працівників об’єктів критичної інфраструктури стосовно їхніх дій у випадку виникання подій кібербезпеки. Оскільки кожен з них розглядається як одне з основних джерел інформації, яка може використовуватися при встановлюванні ознак належності подій до кіберінцидентів, кібератак, кіберзагроз [1, 8]. До того ж нині основна увага зосереджується на навчанні питанням реагування. Тому для ефективного його реалізування необхідно задовольнити потребу визначення основ повідомлення працівниками об’єктів критичної інфраструктури про події кібербезпеки. Насамперед йдеться про потенційні джерела інформації, діяльність, дії, правила, формат повідомлення. Загалом це дозволить визначити парадигму і, як наслідок, механізм повідомлення про події кібербезпеки. Такий погляд підтверджується настановами гармонізованого в Україні міжнародного стандарту ISO/IEC 27001 (додаток А, п. 6.8). Відповідно до нього організації повинні упроваджувати відповідний механізм при реалізуванні заходу звітування про події інформації безпеки. Крім того, ураховує узгодженість з найкращими світовими практиками на міжнародному, регіональному та національному рівнях [1, 5].

Висновки. Отже, запорукою ефективності реалізування заходів виявлення і реагування на інциденти є визначання основ повідомлення працівниками об’єктів критичної інфраструктури про події кібербезпеки. Це обумовлюється необхідністю протидіяння запобіганню порушень надання ними життєво важливих функцій та/або послуг. До того ж інтегруванням України в європейський і євроатлантичний простори та, як наслідок, узгоджуванням вітчизняного законодавства з міжнародним, регіональним і національним правом. Тому визначанням парадигми повідомлення про події кібербезпеки враховуватимуться найкращі світові практики. Тоді як її використання для розроблення відповідного механізму сприятиме обізнаності працівників об’єктів критичної інфраструктури про те, що протягом якого проміжку часу та кому доводити до відома. Насамперед йдеться про потенційні джерела інформації, діяльність, дії, правила, формат повідомлення. Крім того, дозволить задовольнити вимогу 6.8 додатку А ISO/IEC 27001 до системи управління інформаційною безпекою об’єкта критичної інфраструктури.

Література

1. Цуркан В., Ракович В. Механізм повідомлення про події кібербезпеки об’єктів критичної інфраструктури. *Кібербезпека : освіта, наука, техніка*. 2026. Том 4, № 32. Р. 1002–1014. DOI: <https://doi.org/10.28925/2663-4023.2026.32.1200>.

2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2021 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 14.08.2026).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 14.08.2026).

4. Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 № 518 : станом на 20 листоп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8> (дата звернення: 14.08.2026).

5. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) : Директива Європейського Парламенту і Ради (ЄС) від 14.12.2022 № 2022/2555. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text (дата звернення: 14.08.2026).

6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text> (дата звернення: 14.08.2026).

7. Про затвердження Порядку визначення підстав для надання вимог про реагування на кіберінциденти, кібератаки, кіберзагрози та надання звіту про результати вжитих заходів реагування : наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 24.06.2026 № 474. URL: <https://zakon.rada.gov.ua/laws/show/z1013-26#Text> (дата звернення: 14.08.2026).

8. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету міністрів України від 26.11.2025 № 1533: станом на 20 листоп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#n12> (дата звернення: 14.08.2026).

УДК 004.056.5:004.738.5:004.8

Сільвейструп О.Р.

СИСТЕМА ФІЛЬТРАЦІЇ HTTP-ТРАФІКУ ВЕБ-ДОДАТКІВ WAF З ВИКОРИСТАННЯМ ML

Державний університет інтелектуальних технологій і зв’язку
asilvejstruk@gmail.com

Анотація. Обґрунтовано доцільність застосування ансамблевих алгоритмів машинного навчання для проактивного захисту веб-додатків від кібератак прикладного рівня. Розроблено та програмно реалізовано архітектуру інтелектуального міжмережевого екрана (WAF), головною науково-практичною цінністю якої є імплементація механізму гібридної перехресної валідації. Поєднання ймовірнісних прогнозів ML-моделей (XGBoost, Random Forest, SVM, MLP) із детермінованими сигнатурними модифікаторами дозволило розв’язати проблему хибних спрацьовувань (FPR зведено до 0,34 %) зі збереженням високої стійкості до Zero-Day загроз. Натурне тестування розробленого прототипу підтвердило загальну точність класифікації мережевого трафіку 99,76 % при середній затримці обробки до 15 мс.

Ключові слова: Web Application Firewall, машинне навчання, кібербезпека, фільтрація трафіку, виявлення аномалій, ансамблеві методи, HTTP-запити.

Захист інформації та корпоративних веб-ресурсів є однією з найважливіших проблем сучасного інформаційного суспільства [1]. Інтенсивна цифровізація та масовий перехід до мікросервісної архітектури призвели до того, що веб-додатки стали основною мішенню для кіберзлочинців. Більшість успішних випадків витоків конфіденційних даних пов’язана з експлуатацією вразливостей саме на прикладному рівні (Layer 7 моделі OSI).

Традиційні міжмережеві екрани веб-додатків (WAF), що базуються виключно на негативній моделі безпеки та жорстких регулярних виразах (наприклад, OWASP Core Rule Set), наразі перебувають у технологічній кризі. Вони генерують значний відсоток хибних спрацьовувань (False Positives) при аналізі легітимного трафіку і залишаються критично вразливими до атак нульового дня (Zero-Day) та сучасних методів обфускації шкідливого коду. Це формує об’єктивну необхідність у переході від детермінованих алгоритмів до адаптивних засобів безпеки на основі штучного інтелекту.

Метою дослідження є проєктування, програмна реалізація та тестування інтелектуальної системи фільтрації HTTP-трафіку з використанням ансамблю алгоритмів машинного навчання та механізмів гібридної корекції рішень.

Запропонована система базується на гібридній архітектурі та імплементована як проміжне програмне забезпечення (Middleware). Процес інспекції кожного вхідного HTTP-запиту є суворо синхронізованим та поділяється на чотири послідовні фази:

- 1) Перевірка винятків та лімітування (Fast-Reject & Rate Limiting).
- 2) Нормалізація та екстракція ознак у 51-вимірний математичний вектор.
- 3) Інтелектуальна ML-Предикція за допомогою ансамблю класифікаторів.
- 4) Прийняття рішення (гібридна корекція) та транзакційне логування.

Архітектуру програмного забезпечення розробленої системи безпеки наведено на рис. 1.

Для якісної класифікації мережевого трафіку розроблено модуль екстракції, який перетворює неструктурований текст на 51-вимірний вектор. До цього простору ознак увійшли чотири основні категорії: розмірні характеристики (довжина URI-шляху, параметрів запиту та корисного навантаження), статистичні метрики (частота появи специфічних символів, таких як одинарні лапки, кутові дужки чи нуль-байти), лексичні маркери (бінарні прапорці наявності ключових слів атаки), а також контекстні ознаки (HTTP-методи та типи контенту).

Найважливішим етапом попередньої обробки є перетворення неструктурованого тексту мережевих пакетів у числовий формат. Окрім лексичних маркерів та розмірних характеристик, система обчислює інформаційну ентропію за Шенноном для URL-адреси та тіла запиту, оскільки обфускований код зломисників має значно вищий рівень ентропії порівняно з легітимним текстом. Розрахунок ентропії H виконується за формулою [2]:

$$H = - \sum_{i=1}^n p_i \log_2(p_i)$$

де p_i – ймовірність (відносна частота) появи i -го символу; n – загальна кількість унікальних символів.

Щоб уникнути проблеми дисбалансу класів (Class Imbalance) під час навчання ML-моделей, використано алгоритм синтетичного збільшення меншості класів – SMOTE [3]. Математично створення нового синтетичного зразка атаки X_{new} описується як:

$$x_{new} = x_i + \lambda \cdot (x_{rj} - x_i)$$

де x_i – базовий вектор ознак шкідливого HTTP-запиту; x_{zi} – один із k-найближчих сусідів; λ – випадкова величина [0,1].

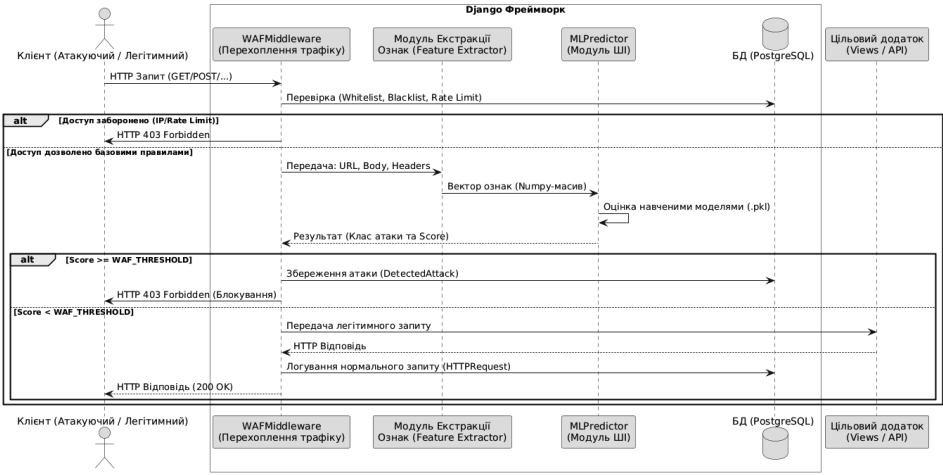


Рис. 1. Архітектура програмного забезпечення інтелектуального WAF

Для виявлення складних патернів кібератак використано ансамблевий підхід: алгоритм XGBoost (для SQLi та DDoS), Random Forest (для XSS), SVM з лінійним ядром (для Path Traversal) та багатoshаровий перцептрон (для RCE та SSRF). Для мінімізації хибних спрацьовувань впроваджено алгоритм гібридної оцінки, який комбінує ймовірнісні прогнози ML-моделей (Confidence Scores) із детермінованими правилами.

Логіку векторизації та гібридного аналізу наведено на рис. 2.

Ключовою інновацією розробленої архітектури є застосування механізму гібридної перехресної валідації. На відміну від класичних рішень, де вердикт виноситься виключно нейромережею, система застосовує зважений підхід. Кожна специфічна модель з ансамблю класифікаторів генерує первинну ймовірність атаки (Confidence Score). Далі система зв'язує цей результат із лексичними тригерами: якщо в запиті явно присутня сигнатура цільової атаки (наприклад, ключове слово для SQLi при високій оцінці моделі XGBoost), загальний бал штучно підвищується, гарантуючи миттєве блокування. Якщо ж спрацьовує сигнатура для іншого класу атак, оцінка радикально штрафується понижуючим коефіцієнтом. Цей підхід дозволяє чітко розмежовувати вектори загроз.

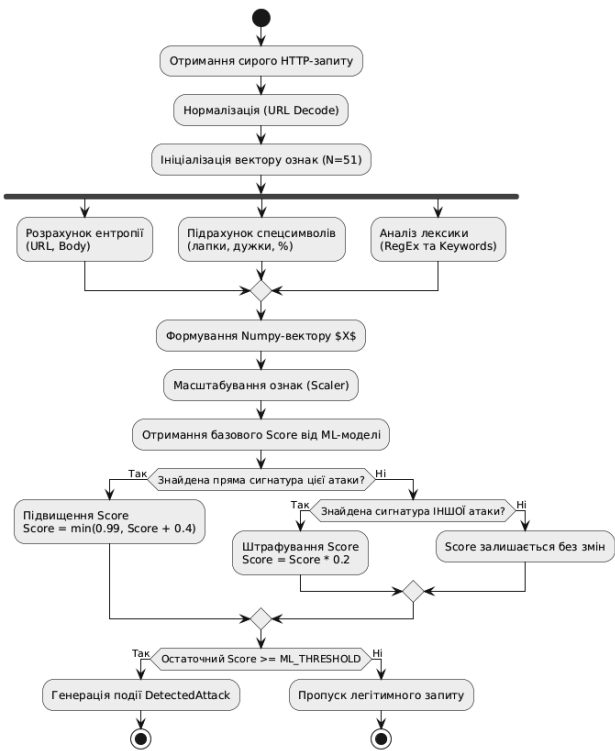


Рис. 2. Алгоритм векторизації та гібридного аналізу HTTP-запиту

Для перевірки ефективності розробленого інтелектуального ML-WAF у реальних експлуатаційних умовах проведено натурне тестування. WAF було інтегровано як Reverse-Proху для захисту цільового клієнт-серверного веб-додатка (онлайн-кінотеатру). Симуляція атак проводилася за допомогою розробленого багатопотокового fuzzer-агента, який згенерував вибірку обсягом 12 000 транзакцій. Вибірка включала як відомі вектори з публічних баз, так і згенеровані складні обфусковані атаки нульового дня (Zero-Day). Матрицю помилок (Confusion Matrix) системи наведено на рис. 3.

Аналіз матриці помилок свідчить про високу узагальнювальну здатність навчених моделей. Завдяки впровадженню гібридної корекції вдалося досягти нульового рівня пропусків для відомих критичних загроз. Загальна точність (Accuracy) системи становить 99,76%, що суттєво перевищує заявлені показники більшості традиційних систем (наприклад, ModSecurity з базовим набором правил CRS). При цьому рівень хибних блокувань легітимного трафіку (FPR) склав лише 0,34 %, а використання оптимізованих моделей машинного навчання дозволило утримувати середній час обробки одного запиту в межах 15 мс, що є критично важливим для високонавантажених веб-додатків.

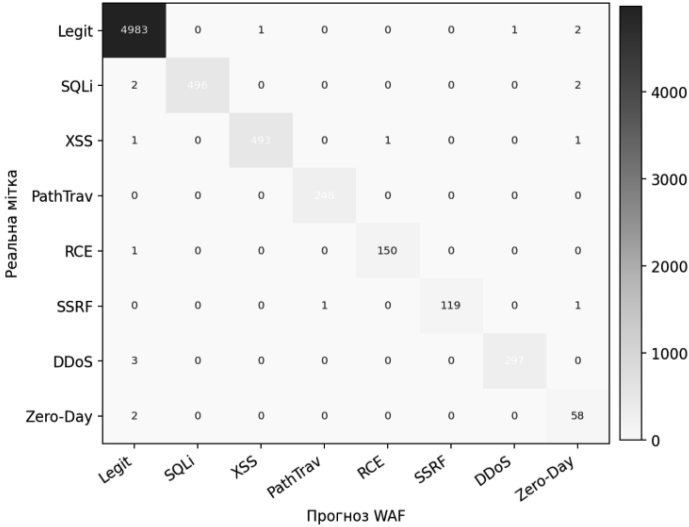


Рис. 3. Матриця помилок WAF на трафіку цільового веб-додатку

Висновки. Результати дослідження підтверджують ефективність запропонованого гібридного підходу. Розроблена інтелектуальна система WAF продемонструвала загальну точність (Accuracy) 99,76% та нульовий відсоток пропусків критичних загроз. Відсоток помилково заблокованих легітимних запитів (FPR) склав лише 0,34%, що значно перевищує показники класичних сигнатурних систем. Додатково вимірювання продуктивності при навантаженні 1500 RPS показало, що 99-й перцентиль (p99) затримки обробки становить 14,8 мс, що підтверджує готовність системи до використання у високонавантажених корпоративних інфраструктурах.

Література

- OWASP Top 10:2021 – The Ten Most Critical Web Application Security Risks [Електронний ресурс] / Open Worldwide Application Security Project. – Режим доступу: <https://owasp.org/Top10/> (дата звернення: 03.04.2026).
- The Role of Machine Learning in WAFs [Електронний ресурс] / Check Point Software Technologies. – 2024. – Режим доступу: <https://www.checkpoint.com/cyber-hub/network-security/what-is-a-web-application-firewall-waf/the-role-of-machine-learning-in-wafs/> (дата звернення: 03.04.2026).
- Chawla N. V. SMOTE: Synthetic Minority Over-sampling Technique / N. V. Chawla, K. W. Bowyer, L. O. Hall // Journal of Artificial Intelligence Research. – 2002. – Vol. 16. – P. 321-357. – Режим доступу: <https://arxiv.org/abs/1106.1813> (дата звернення: 03.04.2026).
- Chindrus C. Machine Learning-Based Multilabel Classification for Web Application Firewalls: A Comparative Study / C. Chindrus, C.-F. Caruntu // Electronics. – 2025. – Vol. 14, Iss. 21. – P. 4172. – Режим доступу: <https://doi.org/10.3390/electronics14214172> (дата звернення: 03.04.2026).

УДК 004.056

Горицький В.М.

БЕЗПЕКА ЗВ'ЯЗКУ ФІЗИЧНОГО РІВНЯ В МЕРЕЖАХ 5G/6G НА ОСНОВІ ЙМОВІРНІСНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Державний торговельно-економічний університет
gorytski@ukr.net

Анотація. Наднадійний зв'язок із низькою затримкою URLLC (Ultra-reliable low latency communication) як послуга, яку пропонують бездротові системи п'ятого та шостого покоління (5G/6G) є технологічною відповіддю на потреби різних критично важливих застосунків, які вимагають надійної передачі даних з низькою затримкою. Поєднання вимог до високої надійності та низької затримки у сценаріях використання URLLC створює проблему безпеки передачі даних URLLC як такої, що не може бути вирішена використанням звичайних складних криптографічних методів на основі секретного ключа. Розглянуто підхід з використання механізмів безпеки фізичного рівня (physical layer Security - PLS) як альтернативи класичним методам

криптографічної безпеки для URLLC. Запропоновано безпеку зв'язку фізичного рівня в мережах 5G/6G організовувати на основі ймовірнісних криптографічних перетворень, оснований на концепції каналу із відведенням («wire-tap channel»).

Ключові слова: наднадійний зв'язок із низькою затримкою, безпека зв'язку фізичного рівня, концепція каналу із відведенням, wire-tap channel, ймовірнісна криптографія.

Швидке розгортання систем бездротового зв'язку п'ятого та шостого поколінь прискорює розвиток сфер, де наднадійний зв'язок з низькою затримкою (URLLC) став ключовою технологією для критично важливих застосувань (медицина, автономне водіння, управління у режимі реального часу тощо). URLLC привносить значну новизну в 5G, запроваджуючи якісні відмінності від попереднього покоління мобільних послуг (4G, LTE), одночасно розширюючи функціональні можливості та виходячи за рамки додатків 5G нового покоління.

Сфера застосування наднадійного зв'язку із низькою затримкою (URLLC) постійно зростає і стає наріжним каменем кіберфізичних систем. Сервіс URLLC здатний забезпечити високу надійність (99,999%) і низьку затримку (≤ 1 мс) передачі сигналу для підтримки різноманітних критично важливих програм, таких як: промислова автоматизація (індустрія 5.0), автономне водіння (інтелектуальні транспортні системи), розумна мережа, тактильний Інтернет, інтелектуальні системи охорони здоров'я тощо.

Однак суворі вимоги URLLC, що характеризуються наскрізною затримкою менше 1 мс та надійністю понад 99,999%, створюють значні проблеми для традиційних криптографічних механізмів безпеки, які часто призводять до обчислювальних витрат та затримок зв'язку.

Таким чином, завдання полягає у всебічному дослідженні шляхів і механізмів захисту інформації при використанні мережевих технологій і технологій телекомунікацій на основі 5G/6G для широкого кола потреб і створенні рекомендацій щодо вибору ефективних і прийнятних технологій захисту даних. Як результат, кінцевою метою цього завдання є пропонування конструктивних підходів до вирішення безпекових питань комунікаційного підключення автомобілей до мереж на основі 5G.

Крім високої надійності передачі даних та малої затримки передачі даних, важливою проблемою є забезпечення безпеки передачі даних для URLLC. Це є наслідком того, що більшість критично важливих додатків 5G використовують службу URLLC для передачі конфіденційної та високопріоритетної керуючої інформації.

URLLC використовує для передачі даних короткі пакетні сигнали кінцевої довжини блоку (десятки – сотні біт), що дуже ускладнює (іноді і усуває можливість) використання звичайних складних криптографічних методів на основі секретного ключа.

Забезпечення інформаційної безпеки критичного короткопакетного зв'язку (SPC) у URLLC стає вирішальним з точки зору надійного та безпечного зв'язку.

Традиційно розробка схем посилення безпеки в бездротовому середовищі спирається на підходи, засновані на теорії інформації, де криптографічні методи застосовуються для запобігання витоку інформації та встановлення безпечного зв'язку в бездротових системах. Однак ці рішення для URLLC мають суттєві недоліки, так як вони створюють сильні обмеження та високі додаткові витрати для користувачів мереж загального користування, споживають додатковий час обробки, викликають накладні витрати на сигналізацію та підходять для сигналів з більшою довжиною блоку. З іншого боку, кінцева довжина блоку, ненульова ймовірність помилки декодування і суворі вимоги QoS URLLC створюють додаткове навантаження на розробку схем підвищення безпеки. Тому для передачі сигналу URLLC дуже бажані схеми безпеки низької складності замість складних криптографічних методів. Нові підходи до безпеки виходять із основ теорії інформації та зосереджуються на безпеці каналу розповсюдження радіосигналів і мають назву *безпека фізичного рівня (physical layer Security - PLS)* [1].

Розробка нових підходів для PLS, які можуть використовуватись для організації безпечного URLLC у 5G і майбутніх бездротових мережах шостого покоління (у 6G - Гіпернадійний Зв'язок із Низькою Затримкою (Hyper Reliable Low Latency Communication - HRLC)) на сьогодні є актуальною науковою задачею.

Ефективними методами вдосконалення PLS URLLC можуть бути підходи, побудовані на концепції каналу із відведенням («wire-tap channel»), запропонованій А.Вайнером (A.D.Wyner) [2] і розвинутий пізніше в інших роботах [3-5], де вона отримала назву кодовий захист, кодове зашумлення, *ймовірнісне криптографічне перетворення*. Суть її полягає в тому, що багатьом фізичним моделям несанкціонованого доступу до інформації в реальних інформаційно-комунікаційних системах (як провідних, так і безпроводних) може бути зіставлена математична модель, яка містить два канали: *основний* - від джерела інформації до одержувача і *відвідний (wire-tap)* - від джерела до незаконного користувача.

Вайнер припустив, що ідеальна секретність може бути досягнута в присутності підслухувачів, якщо якість каналу прослуховування стане гіршою, ніж якість законного каналу.

Запропонована схема представляє собою так званий погіршений широкомовний канал (ШК) з одним входом і двома виходами. Проте на відміну від звичайного завдання максимізації швидкості передачі до обох одержувачів, традиційної для ШК, тут ставиться завдання мінімізації кількості інформації, що отримується незаконним користувачем, при збереженні максимально можливої швидкості передачі інформації законному

користувачеві. З цією метою запропоновано здійснювати випадкове кодування на передачі і відповідне (невипадкове) декодування на прийомі. Нижче дано формальний опис моделі, показаної на рис. 1.

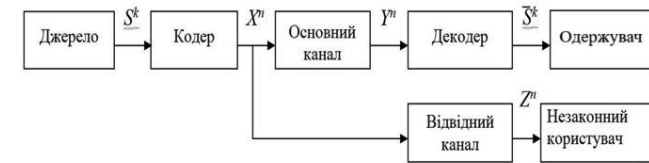


Рис. 1. Модель концепції «wire-tap channel»

Канал передачі інформації від джерела до одержувача називається *основним каналом*, канал відведення до незаконного користувача (аналітика) – *відвідним каналом*.

Джерело – пристрій, який в кожному одиницю часу формує один з символів, що належать дискретній множині S. На даному етапі обмежимося представленням джерела у вигляді послідовності незалежних, однаково розподілених випадкових величин, належних S. Позначимо ентропію джерела через H_S.

Основний канал – дискретний канал без пам'яті {X, p(y/x), Y} з вхідним алфавітом X, вихідним алфавітом Y і матрицею перехідної ймовірності |p(y/x)|.

Випадковий кодер – відображення k-блоків джерела s в n-блоки кодера x, тобто $x = f(s, t)$, де f – функція кодування, t – випадкове число. На кодуючу функцію накладається обмеження, що полягає в тому, що $f(s_i, t) \neq f(s_j, t')$ для будь-яких t, t' и $s_i \neq s_j$.

Декодер в основному каналі - невідповідне відображення n-блоків y в k-блоки s', $s' = \psi(y)$, де ψ – функція декодування.

Згідно концепції, джерело виробляє послідовність рівноймовірних та незалежних двійкових символів

$$S_1, S_2, \dots, S_i. \quad (1)$$

Кодер об'єднує вхідні символи в блоки по k символів

$$S^k = (S_1, S_2, \dots, S_k) \quad (2)$$

і кодує кожен блок у двійковий n-мірний вектор

$$X^n = (X_1, X_2, \dots, X_n), \quad (3)$$

який в основному каналі перетворюється на вектор

$$Y^n = (Y_1, Y_2, \dots, Y_n) \quad (4)$$

і надходить на декодер, де здійснюється його декодування у вектор

$$\hat{S}^k = (\hat{S}_1, \hat{S}_2, \dots, \hat{S}_k) \quad (5)$$

Послідовно з основним каналом включений відвідний канал (канал підслуховування «wire-tap channel»), на виході якого спостерігається вектор

$$Z^n = (Z_1, Z_2, \dots, Z_n) \quad (6)$$

У випадку, коли основний двійковий канал не має перешкод, а відвідний канал – дискретний симетричний канал з ймовірністю помилки p, тобто

$$Y^n = X^n, \text{ а } Z^n = X^n \oplus E^n \quad (7)$$

Де

$\oplus$ – покомпонентне підсумовування векторів за модулем два;

E^n – двійковий вектор помилок у відвідному каналі, які незалежні, ймовірність появи одиниці в кожній з позицій – p, а нуля – 1-p.

У такому випадку завдання імовірнісного кодування полягає у максимізації невизначеності

$$\Delta = k^{-1} H(S^k \vee Z^n) \quad (8)$$

в відвідному каналі щодо переданих S^k повідомлень під час спостереження Z^n .

Основними параметрами передачі в даній моделі є:

- швидкість передачі інформації – k/n ;
- ймовірність помилки на символ в основному каналі
-

$$P_e = \frac{1}{K} \sum_{i=1}^K p(s_i \neq s_{j'}); \tag{9}$$

- невизначеність інформації

$$\Delta = H(S^k \vee Z^n)/k. \tag{10}$$

Параметр Δ характеризує захищеність інформації відносно каналу відведення. Дійсно, використовуючи відоме співвідношення для кількості інформації, що передається по каналу [1], можна записати як (11)

$$I(S^k; Z^n) = H(S^k) - H(S^k | Z^n), \tag{11}$$

де

$H(S^k)$ – ентропія k -блоків джерела;

$H(S^k | Z^n)$ – умовна ентропія джерела при відомих n -блоках на виході каналу;

$I(S^k; Z^n)$ – середня взаємна інформація між k -блоками на вході і n -блоками на виході каналу.

Тоді вочевидь, що якщо $H(S^k | Z^n) = H(S^k)$, то $I(S^k; Z^n) = 0$ і інформація незаконному користувачеві не передається. Якщо $H(S^k | Z^n) = 0$, то $I(S^k; Z^n) = H(S^k)$ і незаконний користувач отримує повну інформацію від джерела. У проміжному випадку незаконний користувач отримує деяку кількість інформації, що відрізняється від нульової, але неповну.

Основний висновок, який встановлено в [2], полягає в доказі існування способу кодування-декодування для області кінцевих швидкостей передачі $0 \leq R \leq R_s$, при якому в каналі відведення може бути забезпечена висока захищеність $\Delta \rightarrow H_s$, якщо $n \rightarrow \infty$.

Конструктивні способи реалізації концепції «wire-tap channel» та відповідні неасимптотичні оцінки його ефективності були отримані в [4-7].

Сутність методу КЗ полягає в тому, що застосуванням спеціального надлишкового кодування, яке функціонально відображає випадкове кодування на основі кодової книги, вдається передавати в основному каналі (каналі законного одержувача) інформацію практично без помилок, а в каналі перехоплення («wire-tap channel») при цьому забезпечувати наближення ймовірності помилки до одиниці не ціною енергетичного придушення сигналів, що перехоплюються, а ціною ускладнення кодування і деякого погіршення якості каналу перехоплення порівняно з каналом одержувача (при такому підході передбачається знання незаконним користувачем такої ж апіорної сукупності відомостей, що і законним користувачем, тобто ніякі секретні дані тут не використовуються). Якщо основний канал досить високої якості, то надлишковість при такому кодуванні використовується не для підвищення достовірності передачі інформації, а навпаки, для виключення можливості перехоплення інформації каналом перехоплення (якість основного каналу при цьому практично не знижується або знижується незначно).

В фізично-просторовій моделі концепції «wire-tap channel» для *URLLC-одержувачів* вирішується завдання забезпечення некриптографічним шляхом захищеного обміну інформацією між джерелом і легальними отримувачами (по *основному каналу*) в межах *безпечної зони конфіденційності* при одночасній неспроможності отримання цієї інформації *незаконним користувачем* за межами *безпечної зони конфіденційності* (по *відвідному каналу*). Неспроможність отримання інформації *незаконним користувачем* за межами *безпечної зони конфіденційності* може бути оцінена по різним показникам і нормованим критеріям. Так як застосовуючи імовірісно-криптографічні перетворення, при тому ж співвідношенні сигнал/шум (без кодування) на вході приймача *незаконного користувача* можна отримати гіршу якість відтворення переданого повідомлення, критерієм якості каналу зв'язку (як *відвідного каналу*, так і *основного каналу*) може бути, наприклад, його пропускна здатність C . Розраховуючи пропускну здатність C для випадків застосування чи незастосування імовірісно-криптографічних перетворень даних, можливо оцінити виграш в розмірах (скорочення) зони інформаційної доступності для незаконного користувача. Відповідно, цей виграш буде залежати від параметрів блокового коду, структури його суміжних класів тощо.

У випадку *URLLC* модель джерела повідомлень, якими є короткі команди, може бути представлена у вигляді набору з T послідовностей $s_i = s_{i1}, s_{i2}, \dots, s_{ik}, \quad s_{ij} \in S, \quad i = 1, 2, \dots, T$, які мають довжину k . Послідовності джерела є рівноймовірними, тобто $p(s_i) = 1/T$.

Така модель може бути використана для опису безнадлишкового джерела, до якого можуть бути віднесені деякі джерела даних, а також надлишкових джерел, якщо їхній статистичний опис невідомий на приймальній стороні. Цією ж моделлю описуються і джерела детермінованих повідомлень, зокрема джерела команд, котрим передбачається кількість повідомлень невеликою, а структура відомою на приймальній стороні.

Тоді критерієм захищеності інформації у відвідному каналі буде виконання нерівності $P_{\text{пл}}(B) \leq P_{\text{пл/доп}}(B)$, де $P_{\text{пл/доп}}(B)$ - гранично допустима величина ймовірності правильного прийому блоку B . Ця величина має вибиратися близькою до ймовірності правильного вгадування переданого блоку.

Висновки. Швидке розгортання комунікаційних технологій п'ятого (5G) та шостого (6G) покоління перетворює більшість сучасних кіберфізичних систем на високопов'язані, керовані даними та критично важливі для безпеки екосистеми. Інтеграція наднадійного зв'язку з низькою затримкою (URLLC) в кіберфізичні системи значно підвищує їх ефективність. Однак ці досягнення одночасно збільшують вразливість інфраструктур кіберфізичних систем до складних кіберзагроз, включаючи підслуховування, спуфінг, глушіння, повторні атаки, атаки типу "сибіл" та "людина посередині". Отже, розробка ефективних механізмів безпеки, здатних відповідати суворим вимогам URLLC, стала критичним дослідницьким завданням.

Порівняльний аналіз показує, що механізми безпеки фізичного рівня (PLS) можуть значно підвищити конфіденційність в комунікаціях на основі URLLC, одночасно мінімізуючи накладні витрати на зв'язок. Серед досліджуваних підходів, механізми безпеки за допомогою IRS-Assisted Security, Massive MIMO Security, генерації ключів фізичного рівня та ймовірнісного захисту демонструють найбільший потенціал для майбутнього впровадження в середовищах 5G/6G. Отримані результати свідчать про те, що інформаційно-теоретична безпека може ефективно доповнювати традиційні криптографічні механізми та покращувати загальну стійкість підключених та автономних систем мобільності.

Ефективними методами вдосконалення PLS URLLC можуть бути підходи, побудовані на концепції каналу із відведенням («wire-tap channel»), які обмежують інформаційну доступність незаконних (несанкціонованих) користувачів до просторової безпечної зони конфіденційності, створеної шляхом імовірісно-криптографічних перетворень команд *URLLC*.

Література

1. Yongpeng Wu; Ashish Khisti; Chengshan Xiao; Giuseppe Caire; Kai-Kit Wong; Xiqi Gao «A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead». IEEE Journal on Selected Areas in Communications, Volume: 36 (2018), Issue: 4, pp 679 -695 <https://ieeexplore.ieee.org/document/8335290>
2. Wyner A.D. The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355-1387.
3. Csisz'ar I., K'ornier J. Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. –1978. – Vol. 24, № 3. – pp. 339–348, May 1978.
4. Коржик В. И., Яковлев В. А. Неасимптотические оценки эффективности кодового зашумления одного канала // Проблемы передачи информации. – 1981. – Т. 17, Вып. 4. – С. 11–18.
5. Коржик В.И., Горицкий В.М., Оценки эффективности методов кодового зашумления // Специальная техника средств связи. - Сер. ТПС. - Вып. 1. - 1983. - С. 74-83.
6. Горицкий В.М. Вероятностная криптография в системах защиты информации: кодовая защита // Электроника и связь. - Вып. 5. - 1998. - С. 140-145.
7. Коржик В.И., Горицкий В.М., МКИ НОЧК1, Способ активной защиты. - № 3133860; Заявл. 03.02.1986.

УДК 004.056.55

Дикий О.В., Соколов А.В.

ОЦІНЮВАННЯ ЛІНІЙНИХ ВЛАСТИВОСТЕЙ S-БЛОКІВ НА ОСНОВІ ЧЕТВІРКОВОЇ МОДЕЛІ АПРОКСИМАЦІЇ

Національний університет «Одеська юридична академія»
olegdykyj@gmail.com, radiosquid@gmail.com

Анотація. У роботі запропоновано підхід до оцінювання криптографічних S-блоків на основі четвіркової моделі, що доповнює традиційний бінарний аналіз. Розглянуто четвіркову таблицю лінійних апроксимацій (QLAT) та коефіцієнт четвіркової кореляції як засоби дослідження статистичних властивостей S-блоків. На відміну від класичної таблиці лінійних апроксимацій, запропонований підхід враховує розподіл результатів четвіркових лінійних форм за чотирма можливими значеннями та має спектральну інтерпретацію через перетворення Віленкіна–Крестенсона. Експериментальне дослідження S-блоків показало, що максимальна четвіркова кореляція не визначається однозначно класичною максимальною ймовірністю лінійної апроксимації. Зокрема, для S-блоків *Serpent*, які мають однакове значення класичного LAP, отримано суттєво різні значення четвіркової характеристики. Для випадково сформованих бієктивних S-блоків також встановлено слабкий статистичний взаємозв'язок між LAP та максимальною четвірковою кореляцією. Отримані результати свідчать про доцільність використання четвіркових характеристик як додаткового критерію комплексного оцінювання криптографічних S-блоків та створюють основу для розвитку четвіркового лінійного криптоаналізу багатораундових SPN-структур.

Ключові слова: S-блок, багатозначна логіка, четвіркова логіка, лінійний криптоаналіз, QLAT, четвіркова кореляція, SPN-структура.

$$p_r(a, b) = \frac{1}{|S|} |\{x: L_{a,b}(x) = r\}|, r \in \{0,1,2,3\}.$$

Таким чином, замість одного бінарного показника отримується вектор

$$p(a, b) = (p_0(a, b), p_1(a, b), p_2(a, b), p_3(a, b)),$$

який характеризує статистичну поведінку конкретної четвіркової лінійної апроксимації. Саме повний розподіл чотирьох значень є принциповою відмінністю QLAT від класичної LAT.

Для узагальненої кількісної оцінки сили четвіркової лінійної залежності вводиться коефіцієнт четвіркової кореляції

$$\gamma(a, b) = \sum_{r=0}^3 p_r(a, b) i^r,$$

де $i = \sqrt{-1}$. Модуль $|\gamma(a, b)|$ характеризує ступінь вираженості відповідної четвіркової лінійної залежності.

На основі цього коефіцієнта визначається максимальна четвіркова кореляція

$$\Gamma = \max_{(a,b) \neq (0,0)} |\gamma(a, b)|,$$

де максимум обчислюється для нетривіальних пар масок. Чим меншим є значення Γ , тим слабшими є найбільш виражені четвіркові лінійні залежності між входом і виходом S-блока, а отже, тим вищою є його стійкість до відповідного типу аналізу. Такий критерій доповнює традиційний LAP, а не замінює його.

Важливою властивістю запропонованого підходу є його зв'язок зі спектральним аналізом. Показано, що коефіцієнт четвіркової кореляції безпосередньо відповідає нормованому коефіцієнту перетворення Віленкіна–Крестенсона [7]. Це дозволяє розглядати четвірковий лінійний аналіз одночасно у ймовірнісній та спектральній формах.

Отже, четвіркове представлення дозволяє отримати додаткову характеристику S-блока, яка не зводиться безпосередньо до його класичних бінарних показників. Проведені дослідження показали, що S-блоки з однаковими або близькими значеннями класичної ймовірності лінійної апроксимації можуть мати суттєво різні значення четвіркової кореляції. Це свідчить про те, що четвірковий аналіз може виявляти статистичні властивості, які залишаються непомітними при використанні лише традиційного булевого представлення.

Для експериментальної перевірки запропонованого підходу було проведено порівняльне оцінювання криптографічних S-блоків за класичною максимальною ймовірністю лінійної апроксимації (LAP) та максимальною четвірковою кореляцією Γ . Дослідження охоплювало як випадково сформовані бієктивні S-блоки, так і S-блоки, що використовуються у відомих симетричних криптографічних алгоритмах.

Для практичних S-блоків отримано відносно невеликі значення Γ . Зокрема, для 8×8 S-блоків значення запропонованої характеристики становили близько 0.062–0.097 для досліджених S-блоків AES, Camellia, Kalyna, ARIA та SM4. При цьому отримані значення були нижчими за відповідні середні значення для випадково сформованих S-блоків аналогічного розміру. Це свідчить про те, що криптографічні S-блоки, оптимізовані за традиційними критеріями, загалом мають також сприятливі властивості з погляду четвіркового лінійного аналізу.

Водночас найбільш важливим результатом є те, що четвіркова характеристика не є простим дублюванням класичного LAP. Показовим прикладом є S-блок Serpent S2 [7]. У дослідженні він продемонстрував найбільше значення четвіркової кореляції серед розглянутих 4×4 S-блоків, хоча його класичні характеристики лінійного аналізу були такими самими, як у інших S-блоків Serpent (табл. 1).

Таблиця 1 – Порівняння класичної та четвіркової лінійних характеристик S-блоків Serpent

S-блок	Γ	LAP
S0	0.559	0.25
S1	0.559	0.25
S2	0.707	0.25
S3	0.530	0.25
S4	0.559	0.25
S5	0.559	0.25
S6	0.559	0.25
S7	0.515	0.25

Таким чином, S-блоки, які мають однакові або близькі характеристики у класичній бінарній моделі, можуть істотно відрізнятися за властивостями четвіркових лінійних апроксимацій.

Ще більш наочно слабкий статистичний взаємозв'язок між двома характеристиками демонструють результати для випадково сформованих бієктивних S-блоків. Для S-блока розміру 4×4 при однаковому значенні класичної LAP = 0.25 спостерігався діапазон значень четвіркової характеристики $0.450 \leq \Gamma \leq 0.790$.

Сучасні симетричні криптографічні алгоритми значною мірою ґрунтуються на використанні нелінійних перетворень, серед яких особливе місце займають таблиці підстановок (S-блоки). Саме S-блоки забезпечують нелінійність криптографічних перетворень та істотно впливають на стійкість алгоритмів до основних видів криптоаналітичних атак [1-3]. Тому розроблення та оцінювання криптографічних S-блоків є одним із важливих напрямів досліджень у галузі захисту інформації.

Для оцінювання якості S-блоків традиційно використовуються такі характеристики, як нелінійність, диференціальна рівномірність, лавинні властивості та стійкість до лінійного криптоаналізу. Зокрема, лінійний криптоаналіз ґрунтується на дослідженні статистичних залежностей між вхідними та вихідними значеннями S-блока. Класичним інструментом такого аналізу є таблиця лінійних апроксимацій (Linear Approximation Table, LAT), яка дозволяє визначати найбільш виражені лінійні залежності та оцінювати відповідну ймовірність лінійної апроксимації [4].

Водночас традиційні методи аналізу S-блоків переважно базуються на булевій моделі, у якій інформація подається у вигляді двійкових значень. Такий підхід є природним для більшості сучасних криптографічних алгоритмів, однак він не враховує можливості використання моделей на основі багатозначної логіки для дослідження статистичних та спектральних властивостей криптографічних перетворень. Дослідження функцій багатозначної логіки показує, що їхні властивості не завжди можуть бути безпосередньо визначені за характеристиками відповідних булевих компонентів [5].

У зв'язку з цим, перспективним напрямом є розширення відомих методів аналізу криптографічних перетворень на область функцій багатозначної логіки. Зокрема, використання четвіркової логіки дозволяє розглядати два біти як один елемент чотиризначного алфавіту та досліджувати S-блок з іншої математичної точки зору. Ми пропонуємо застосування четвіркової таблиці лінійних апроксимацій (Quaternary Linear Approximation Table, QLAT), а також відповідний коефіцієнт четвіркової кореляції, що забезпечують додаткову характеристику статистичних властивостей S-блоків.

Таким чином, поєднання класичних булевих критеріїв із характеристиками, отриманими на основі багатозначної логіки, може розглядатися як перспективний напрям удосконалення методів аналізу та проєктування криптографічних S-блоків.

Метою роботи є узагальнення та розвиток підходів до аналізу криптографічних S-блоків на основі функцій багатозначної логіки шляхом доповнення традиційних булевих характеристик четвірковими статистичними та спектральними показниками.

Для досягнення поставленої мети необхідно:

- розглянути обмеження традиційного булевого підходу до оцінювання лінійних властивостей S-блоків;
- сформувати четвіркову модель представлення криптографічних перетворень;
- розглянути можливість використання QLAT для визначення найбільш виражених четвіркових лінійних залежностей;
- дослідити взаємозв'язок четвіркової кореляції зі спектральними характеристиками функцій багатозначної логіки;
- визначити перспективи використання отриманих характеристик для комплексного оцінювання та подальшого проєктування криптографічних S-блоків.

Особливістю запропонованого підходу є те, що четвірковий аналіз не замінює традиційні методи оцінювання, а доповнює їх інформацією, яка може залишатися непомітною під час класичного бінарного аналізу.

Класичний аналіз лінійних властивостей S-блоків ґрунтується на булевому представленні, у якому вхідні та вихідні значення розглядаються як вектори над полем GF(2). Для заданих вхідної та вихідної масок досліджується відповідність між лінійними комбінаціями вхідних і вихідних бітів. Сукупність отриманих статистичних характеристик формується у вигляді таблиці лінійних апроксимацій (LAT), а максимальне відхилення відповідної ймовірності від 1/2 використовується для оцінювання стійкості S-блока до лінійного криптоаналізу.

У запропонованому підході розглядається можливість переходу від двозначного до чотиризначного представлення. При цьому двійкові пари розглядаються як елементи чотиризначного алфавіту, а операції над масками та лінійними формами визначаються у відповідній четвірковій алгебраїчній структурі. Такий перехід не змінює саме S-блок, а змінює математичну модель, у якій досліджуються його властивості.

Основним інструментом четвіркового аналізу є четвіркова таблиця лінійних апроксимацій (Quaternary Linear Approximation Table, QLAT). На відміну від класичної LAT, де для заданої лінійної апроксимації оцінюється ймовірність виконання одного з двох можливих співвідношень, QLAT враховує розподіл результату четвіркової лінійної форми за чотирма можливими значеннями. Таким чином, для кожної пари вхідної та вихідної масок формується повний розподіл чотирьох залишкових класів.

Для S-блока S , вхідної маски a та вихідної маски b розглянемо четвіркову лінійну форму

$$L_{a,b}(x) = \langle a, x \rangle_4 - \langle b, S(x) \rangle_4,$$

де $\langle \cdot, \cdot \rangle_4$ позначає скалярний добуток у четвірковій моделі. Для кожної пари масок визначається розподіл

Отже, два S-блока можуть мати однакову максимальну ймовірність лінійної апроксимації, але суттєво різну стійкість до четвіркових лінійних апроксимацій.

Для кількісної оцінки взаємозв'язку між LAP та Γ було також обчислено коефіцієнти кореляції Пірсона та Спірмена. Для досліджених груп випадкових S-блоків ці коефіцієнти виявилися невисокими: для 4×4 S-блоків вони становили відповідно 0.220 та 0.223, для більших S-блоків зменшувалися до 0.126 та 0.095, а для найбільших досліджених розмірів продовжували зменшуватися. Це підтверджує наявність слабого статистичного взаємозв'язку між Γ та класичним показником LAP.

Таким чином, результати експерименту показують, що використання лише класичної LAT не дозволяє повністю охарактеризувати лінійні властивості S-блоків. Четвіркова характеристика Γ надає додаткову інформацію, яка може бути використана під час порівняння та відбору криптографічних S-блоків. При цьому запропонований критерій доцільно розглядати не як заміну класичним криптографічним показникам, а як їх доповнення.

Отримані результати мають значення не лише для оцінювання окремих S-блоків, але й для аналізу багатораундових криптографічних конструкцій. Четвіркові лінійні апроксимації можуть послідовно комбінуватися між раундами SPN-мережі, утворюючи четвіркові лінійні траси (quaternary linear trails). Для такої траси загальна кореляція визначається взаємодією кореляцій окремих S-блоків та лінійного шару, що дозволяє переносити запропонований підхід від оцінювання окремого S-блока до аналізу повного криптографічного перетворення.

Таким чином, максимальна четвіркова кореляція S-блока може розглядатися як локальна характеристика, на основі якої здійснюється пошук найбільш виражених четвіркових лінійних трас у багатораундовій конструкції. Наявність сильної четвіркової апроксимації на рівні S-блока потенційно може призводити до формування нетривіальних лінійних залежностей на рівні всієї SPN-мережі. Це відкриває можливість розвитку четвіркового лінійного криптоаналізу як узагальнення традиційного підходу до багатозначної моделі.

Подальший розвиток цього підходу пов'язаний із побудовою практичних методів четвіркового лінійного криптоаналізу та дослідженням їх ефективності для багатораундових SPN-структур.

Висновки. У роботі розглянуто підхід до оцінювання криптографічних S-блоків на основі четвіркової моделі, що доповнює традиційний бінарний аналіз. Показано, що використання четвіркової таблиці лінійних апроксимацій (QLAT) та максимальної четвіркової кореляції Γ дозволяє отримати додаткову інформацію про лінійні властивості S-блоків, яка не завжди виявляється за допомогою класичної LAT.

Результати експериментального дослідження показали, що значення Γ не визначається однозначно класичною максимальною ймовірністю лінійної апроксимації. Зокрема, для S-блоків Serpent при однаковому значенні LAP=0.25 спостерігаються різні значення Γ , а для випадково сформованих 4×4 S-блоків при тому самому LAP значення Γ змінюються в широкому діапазоні. Це підтверджує доцільність використання четвіркової характеристики як додаткового критерію оцінювання.

Отже, поєднання класичних бінарних та четвіркових характеристик може забезпечити більш повне оцінювання лінійних властивостей криптографічних S-блоків. Перспективним напрямом подальших досліджень є використання четвіркових критеріїв не лише для аналізу, але й для пошуку та проектування нових S-блоків із заданими криптографічними властивостями.

Література

1. Karpinski M., Sokolov A., Tokkuliyea A., Radush V., Kazakova N., Shaikhanova A., Zagorodna N., Korchenko A. Development of High-Quality Cryptographic Constructions Based on Many-Valued Logic Affine Transformations. Electronics. 2025. Vol. 14, Issue 10. P. 1-22.
2. Cheng R., Zhou Y., Miao X., Hu J. Analysis of a New Improved AES S-Box Structure. International Conference on Security and Privacy in New Computing Environments. Cham : Springer Nature Switzerland, 2022. P. 109-125.
3. Соколов А.В., Ленков С.В., Радущ В.В. Криптографічні властивості S-блоків, що побудовані на основі теорії динамічного хаосу при представленні за допомогою функцій багатозначної логіки. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2025. №86. С. 79–87.
4. Matsui M. Linear Cryptanalysis Method for DES Cipher. Workshop on the Theory and Application of Cryptographic Techniques, 1993. Perugia, 9-12 May 1994. P. 386-397.
5. Kazakova N.F., Karpinski M., Sokolov A.V., Gancarczyk T. Nonlinearity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithms S-boxes. Procedia Computer Science. Vol. 192. P. 2731-2741.
6. Stanković R.S., Astola J., Moraga C. Representation of multiple-valued logic functions. Morgan & Claypool Publishers, 2012.
7. De Cannière C. Serpent. Encyclopedia of Cryptography, Security and Privacy, Cham. Springer Nature Switzerland, 2025. P. 2385-2386.

УДК 621.391.8:004.72

Царьов Р.Ю., Сідень С.В., Павлов А.С., Царьова А.Р.

ПОКАЗНИКИ ЯКОСТІ, ПЕРЕХІД ВІД МЕРЕЖ 5G ДО 6G

Державний університет інтелектуальних технологій і зв'язку
r-y.tsarov@suiit.edu.ua

Анотація. У роботі розглянуто питання щодо забезпечення показників якості у мережах 5G та 6G, проведено зіставлення нормативних значень показників якості, визначених у IMT-2020 та IMT-2030. Показано, що з тринадцяти мінімальних вимог визначених у IMT-2020 лише шість мають прямі числові відповідники серед характеристик IMT-2030, ще дві зіставляються частково, одна лише якісно, чотири відповідника не мають. Для затримки та надійності зіставлення часткове. Для оцінки факторів, що впливають на бюджет затримки у мережах 6G побудовано модель односторонньої затримки, визначено, що досяжність цільового значення затримки за стандартом IMT-2030 впирається в оброблення сигналу, а структура радіокадру має обмежений вплив.

Ключові слова: показники якості, 5G, 6G, затримка, надійність, час оброблення, скінчення довжина блоку, HARQ.

Рекомендація ITU-R M.2160-0 визначає для IMT-2030 затримку над радіоінтерфейсом у межах 0,1–1 мс і надійність від $1-10^{-5}$ до $1-10^{-7}$ [1]. Поширене уявлення пов'язує досяжність нижньої межі зі збільшенням відстані між піднесучими: коротший символ означає короткий інтервал передавання. Питання, яке лишається без відповіді, полягає в тому, яку частку бюджету цей інтервал насправді займає.

Зіставлення показників двох поколінь ускладнене різним статусом порівнюваних величин. Звіт ITU-R M.2410-0 містить тринадцять мінімальних вимог, невиконання яких закриває технології шлях до статусу IMT-2020 [2]. Характеристики IMT-2030 подано діапазонами, до яких додано застереження про рівний пріоритет усіх значень усередині діапазону та про їх неодночасну досяжність [1, п. 4]. За результатами відображення переліків шість вимог мають прямі числові відповідники, дві зіставляються частково, одна лише якісно, чотири відповідника не мають. Затримка й надійність потрапляють саме до часткових, оскільки нижні межі діапазонів IMT-2030 збігаються зі значеннями попереднього покоління.

Розрив між поколіннями видно й на рівні механізмів, якими якість обслуговування забезпечується в чинній архітектурі. Диференціацію сервісів у 5G реалізовано через ідентифікатор 5QI, кожному значенню якого відповідає бюджет затримки пакета, допустимий рівень помилок і рівень пріоритету. Виразених обмежень рамка не має: поряд зі стандартизованими значеннями специфікація допускає динамічні, тому будь-яку величину бюджету затримки формально задати можна. Обмеження виявляється в іншому місці. Найжорстке стандартизоване значення допустимого рівня помилок дорівнює 10^{-6} , а для критичних до затримки потоків 10^{-5} , тоді як верхня межа діапазону IMT-2030 становить 10^{-7} . Питання, отже, не в описі вимоги, а в здатності радіомережі її виконати, і саме аналізу цього й присвячена робота..

Мета роботи полягає в тому, щоб визначати, яка частина радіомережі обмежує досяжність цільового значення затримки 0,1 мс, і оцінити вартість підвищення надійності в каналі з завмираннями. Метод відрізняється від звичного тим, що час оброблення сигналу не добирається з фізичних міркувань, а береться з нормованих таблиць специфікації.

Односторонній бюджет радіоінтерфейсу представимо сумою очікування нагоди передавання, передавання міні-слота довжиною L символів, оброблення в терміналі та поширення сигналу на відстань d. Цикл повторної передачі містить оброблення двічі, у терміналі й у базовій станції; час оброблення в базовій станції не нормується, тому поданий через коефіцієнт κ :

$$T_{рад} = 1,5 \cdot L \cdot T_{сим} + T_{обр} + d/c; \quad THARQ = 2 \cdot L \cdot T_{сим} + T_{обр} \cdot (1 + \kappa), \quad (1)$$

де $T_{сим} = 1/(14 \cdot 2^n)$ мс – тривалість символу OFDM для конфігурації μ , якій відповідає відстань між піднесучими $\Delta f = 15 \cdot 2^n$ кГц.

Специфікація TS 38.214 задає мінімальний час оброблення PDSCH величиною N_1 і мінімальний час підготовки PUSCH величиною N_2 , обидві в символах, для двох класів оброблення [3]. Моделюємо напрямок «вгору», де нормованою величиною є N_2 ; вона перевищує N_1 для всіх значень і тому визначає бюджет. Значення зведено в таблиці 1.

Таблиця 1 – Час оброблення в терміналі за таблицями N ₁ і N ₂ з TS 38.214							
Δf, кГц	T _{сим} , мкс	N ₁ , симв.	N ₂ , симв.	T _{обр} , клас 1, мкс	N ₂ , клас 2	T _{обр} , клас 2, мкс	
15	71,429	8	10	714,3	5	357,1	
30	35,714	10	12	428,6	5,5	196,4	
60	17,857	17	23	410,7	11	196,4	
120	8,929	20	36	321,4	не визначено	—	
480	2,232	80	144	321,4	не визначено	—	
960	1,116	160	288	321,4	не визначено	—	

Таблиця 1 містить показує два факти, які й визначають подальший розрахунок. Клас оброблення 2, призначений для сервісів які вимагають низької затримки, але він визначений лише для інтервалів у 15, 30 і 60 кГц. Для 120 кГц і вище таких норм немає, тобто швидке оброблення в цих смугах не передбачене, і сервісам, яким потрібна затримка на рівні менше 1 мс на калах 120 МГц і більше, змушені використовувати більш повільний клас 1. Друге спостереження стосується Релізу 17: під час розширення на діапазон FR2-2 значення N₁ і N₂ для 480 і 960 кГц задано кратними до значення при 120 кГц з множниками 4 і 8. Ці множники дорівнюють відношенню відстаней між піднесучими, тому абсолютний час оброблення не змінюється зовсім і становить 321,4 мкс для всіх трьох варіантів. Отже нижня межа часу оброблення не є припущенням моделі, а зафіксована нормативно.

Розрахунок бюджету за виразом (1) наведено в таблиці 2. Відстань до терміналу прийнято 500, 200, 100 і 50 м відповідно до типового радіуса стільника для кожної смуги; її внесок не перевищує 0,32 % бюджету.

Таблиця 2 – Бюджет односторонньої затримки радіоінтерфейсу, мс									
Конфігурація	Δf, кГц	Клас	T _{вир}	T _{пер}	T _{обр}	T _{пош}	Разом	Ліміт	Запас
NR FR1	30	1	0,0357	0,0714	0,4286	0,0017	0,5374	1,0	1,86×
NR FR1	30	2	0,0357	0,0714	0,1964	0,0017	0,3052	1,0	3,28×
NR FR2	120	1	0,0089	0,0179	0,3214	0,0007	0,3489	1,0	2,87×
NR FR2-2	480	1	0,0022	0,0045	0,3214	0,0003	0,3285	0,5	1,52×
6G, кандидат	960	1	0,0011	0,0022	0,3214	0,0002	0,3249	0,1	0,31×

Останній рядок дає запас 0,31, тобто бюджет перевищує ліміт у 3,2 рази. Вимога щодо забезпечення затримки на рівні 0,1 мс в радімережі за нормованих часів оброблення недосяжна, і причина лежить поза структурою кадру: вирівнювання й передавання разом дають затримку у 0,0033 мс, тоді як оброблення – 0,3214 мс, тобто 98,9 % бюджету. Скорочення символу далі нічого не змінює, бо зменшує лише ту частину, яка вже становить одну сотню бюджету.

Звідси випливає результат, що суперечить вихідному очікуванню. Конфігурація з каналом у 30 кГц із класом оброблення 2 має запас 3,28 раза, тобто більший, ніж канал у 120 кГц із класом 1 (2,87). Зростання відстані між піднесучими тут погіршує становище, оскільки втрата доступу до швидкого оброблення коштує більше, ніж виграш від коротшого символу. Загальний вигляд залежності подано на рис. 1. Крива класу 1 виходить на горизонтальну ділянку вже після 120 кГц, а крива класу 2 обривається на 60 кГц, де закінчується область її визначення.

Зростання відстані між піднесучими обмежене й з іншого боку. Тривалість нормального циклічного префікса обернено пропорційна відстані між піднесучими, тому допустимий розкид затримки в каналі скорочується так само: 4,688 мкс і 1405 м за 15 кГц; 0,586 мкс і 176 м за 120 кГц; 0,073 мкс і лише 22 м за 960 кГц. Останнє значення менше за типовий середньоквадратичний розкид у зовнішніх середовищах, тому конфігурація 960 кГц залишається придатною для приміщень і коротких ліній. Навіть якби швидкодію оброблення вдалося підняти, твердження про досяжність затримки 0,1 мс потребувало б зазначення сценарію розгортання.

Наслідком стає несумісність двох цільових значень документу M.2160-0. Цикл повторної передачі за виразом (1) містить час оброблення двічі, тому за ліміту 0,1 мс і T_{обр} = 321,4 мкс жодна повторна передача в бюджет не вміщається за жодного розумного κ. Надійність тоді визначається помилкою першої спроби, і пара значень «0,1 мс» та «1–10⁻⁷» одночасно не виконується. Поряд зі схемою HARQ зі зворотним зв'язком розглянуто сліпі повтори, за яких К копій передаються підряд: вони витрачають більше ресурсу, зате не потребують часу на оброблення між спробами. Чергу описано моделлю M/D/1, оскільки передавання в радіокадрі детерміноване, а до сумарної ймовірності додано невідновну складову 10⁻⁶, що враховує помилки каналу керування та зворотного зв'язку і повторами не усувається. Результати за коефіцієнта використання ресурсу 0,5 і ймовірності помилки першої спроби 10⁻² наведено в таблиці 3.

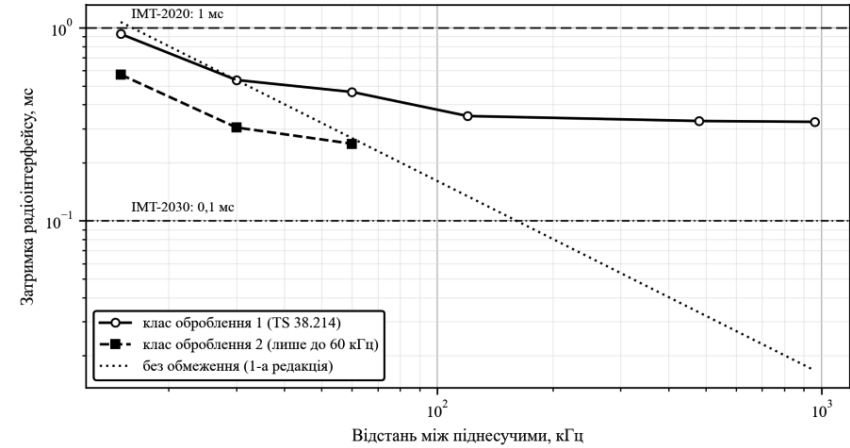


Рисунок 1 – Затримка радіоінтерфейсу залежно від відстані між піднесучими для двох класів оброблення

Таблиця 3 – Імовірність порушення часового ліміту доставки та гранична завантаженість							
Конфігурація	Клас	m*	HARQ	К	Сліпі повтори	ρ _{max}	Ціль сценарію
NR FR1, 30 кГц	1	0	1,00·10 ⁻²	3	2,79·10 ⁻⁴	0,36	1–10 ⁻⁵
NR FR1, 30 кГц	2	1	1,09·10 ⁻⁴	3	3,20·10 ⁻⁶	0,55	1–10 ⁻⁵
NR FR2, 120 кГц	1	0	1,00·10 ⁻²	3	2,00·10 ⁻⁶	0,88	1–10 ⁻⁵
NR FR2-2, 480 кГц	1	0	1,00·10 ⁻²	4	1,01·10 ⁻⁶	недосяжна	1–10 ⁻⁶
6G, 960 кГц	1	—	1,00	4	не вміщається	недосяжна	1–10 ⁻⁷

Значення m* позначає оптимальну кількість повторів HARQ, К – найменшу кількість сліпих повторів, за якої залишкова помилка не перевищує цілі сценарію, ρ_{max} – граничну завантаженість, за якої ця ціль ще виконується. Схема сліпих повторів працює там, де HARQ не встигає: за 120 кГц вона дає 2,00·10⁻⁶ проти 10⁻², бо жоден повтор із підтвердженням у бюджет не вміщається. Для 480 кГц результат 1,01·10⁻⁶ упирається в саму невідновну складову, тобто нижня межа діапазону надійності IMT-2030 лежить на рівні залишкових помилок сигналізації. Для 960 кГц чотири сліпі повтори в бюджет не вміщаються, і ціль не досягається за жодного навантаження.

Отриманий результат для 30 кГц узгоджується з висновком самооцінки 3GPP, за яким радімережа NR задовольняє вимоги IMT-2020 для сценарію URLLC [4]. Рядок із класом оброблення 1 відповідає загальнодоступному режиму й вимогу не виконує, тоді як самооцінка спиралася на клас 2 та агрегування передач без зворотного зв'язку; відповідний рядок дає 3,20·10⁻⁶ і вимогу задовольняє, тому суперечності немає.

Окремого зауваження потребує вартість надійності. Оцінка за нормальною апроксимацією для скінченної довжини блоку [5; 6] дає для каналу з адитивним білим гаусовим шумом приріст у 0,29–0,38 дБ під час переходу від 1–10⁻⁵ до 1–10⁻⁷, звідки в літературі й походить теза про дешевизну цієї вимоги. Проте документ M.2410-0 нормує надійність на межі покриття [2, п. 4.10], тобто в каналі із завмираннями. Для релієвського каналу з рознесенням порядку L потрібний запас середнього відношення сигнал/шум над пороговим дорівнює

$$\gamma_{\text{сер}} / \gamma_{\text{пор}} = (1 / (L! \cdot \epsilon))^{(1/L)}, \tag{2}$$

звідки те саме посилення вимоги коштує 20 дБ без рознесення, 10 дБ за L = 2 і 5 дБ за L = 4. Сумарне потрібне середнє відношення сигнал/шум для блоку 256 канальних інтервалів за L = 4 дорівнює 10,34 дБ для 1–10⁻⁵ і 15,63 дБ для 1–10⁻⁷, тоді як оцінка лише за гаусовим каналом дала б 1,29 і 1,58 дБ. Вартість надійності визначається доступним порядком рознесення.

Межі застосовності отриманих оцінок окреслимо прямо. Значення N₁ і N₂ нормують оброблення в терміналі, тоді як тривалість оброблення в базовій станції специфікаціями не задана і входить у розрахунок через коефіцієнт κ; за κ = 0,5 цикл повторної передачі для 120 кГц скорочується до 0,518 мс, за κ = 2 зростає до 1,000 мс, проте на висновок щодо 960 кГц це не впливає. Модель черги припускає пуассонівський вхідний потік, що для періодичного трафіку промислового керування є консервативним припущенням, а хвіст часу очікування взято як оцінку зверху. Незалежність спроб повторної передачі виконується лише за наявності частотного або часового рознесення між ними. Експериментальна перевірка потребує вимірювань на діючій мережі 5G автономної архітектури, а для 480 і 960 кГц ускладнена недоступністю комерційного обладнання FR2-2.

Висновки. Досяжність цільового значення затримки IMT-2030 впирається в оброблення сигналу; структура радіокадру має не значний вплив. За нормованими значеннями визначеними у TS 38.214 бюджет затримка для каналу у 960 кГц становить 0,325 мс проти цільових 0,1 мс, і 98,9 % його припадає на оброблення, абсолютна тривалість якого визначена Релізом 17 на рівні 321,4 мкс для всіх значень μ від 120 кГц. Клас оброблення 2 визначений лише до 60 кГц, через що збільшення відстані між піднесучими саме собою затримки не зменшує: 30 кГц зі швидким класом дає більший запас, ніж 120 кГц із повільним. Оскільки цикл повторної передачі містить оброблення двічі, цільові значення 0,1 мс і $1-10^{-7}$ одночасно не виконуються. Практичний висновок роботи полягає в тому, що для мереж 6G необхідно поширити швидкий клас оброблення на більш високочастотні канали; без цього подальше скорочення символу виграшу не дає і досягнення заявлених показників якості неможливо.

Література

1. Framework and overall objectives of the future development of IMT for 2030 and beyond : Recommendation ITU-R M.2160-0. Geneva : ITU, 2023. URL: <https://www.itu.int/rec/R-REC-M.2160/en>.
2. Minimum requirements related to technical performance for IMT-2020 radio interface(s) : Report ITU-R M.2410-0. Geneva : ITU, 2017. URL: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf.
3. 3GPP TS 38.214. NR; Physical layer procedures for data. Sophia Antipolis : 3GPP, 2025.
4. 3GPP TR 37.910. Study on self evaluation towards IMT-2020 submission. Sophia Antipolis : 3GPP, 2019.
5. Polyanskiy Y., Poor H. V., Verdú S. Channel Coding Rate in the Finite Blocklength Regime. IEEE Transactions on Information Theory. 2010. Vol. 56, No. 5. P. 2307–2359. DOI: 10.1109/TIT.2010.2043769.
6. Durisi G., Koch T., Popovski P. Toward Massive, Ultrareliable, and Low-Latency Wireless Communication with Short Packets. Proceedings of the IEEE. 2016. Vol. 104, No. 9. P. 1711–1726. DOI: 10.1109/JPROC.2016.2537298.
7. First 6G RAN study approved. 3GPP News. 14.06.2026. URL: <https://www.3gpp.org/news-events/3gpp-news/6g-38914>.
8. Горохов О. С. Удосконалення управління радіочастотними ресурсами в сегментованій мережі радіодоступу 5G. Наукові записки Державного університету інформаційно-комунікаційних технологій. 2026. № 1. С. 80–87. DOI: 10.31673/2786-8362.2026.018042.
9. Захаржевський А. Г. Розробка системної моделі якості обслуговування у інфокомунікаційних мережах зв’язку для забезпечення низької затримки трафіку. Телекомунікаційні та інформаційні технології. 2022. № 3. С. 40–48.
10. IMT-2030: Technical requirements for the 6G future. ITU Hub. 17.03.2026. URL: <https://www.itu.int/hub/2026/03/imt-2030-technical-requirements-for-the-6g-future/>.
11. Bennis M., Debbah M., Poor H. V. Ultrareliable and Low-Latency Wireless Communication: Tail, Risk, and Scale. Proceedings of the IEEE. 2018. Vol. 106, No. 10. P. 1834–1853. DOI: 10.1109/JPROC.2018.2867029.

УДК 004.75:621.39

Царьов Р.Ю., Царьова А.Р., Андрухів Т.В., Міщенко Д.С.

ВИБІР КІЛЬКОСТІ ТОЧОК РОЗПОДІЛУ КАБЕЛЬНОЇ СИСТЕМИ ДЛЯ СЕНСОРНОГО СЕГМЕНТА ІНТЕРНЕТУ РЕЧЕЙ

Державний університет інтелектуальних технологій і зв’язку
r-y.tsarov@suitt.edu.ua

Анотація. У роботі розглянуто вибір кількості точок розподілу горизонтальної підсистеми структурованої кабельної системи, що обслуговує сенсорний сегмент Інтернету речей у промислових будівлях великої площі. Показано, що обмеження стаціонарної лінії у 90 м виводить задачу з внутрішнього оптимуму на межу допустимої області, після чого класичний вираз неперервного наближення для оптимальної кількості вузлів обслуговування втрачає силу, а рішення визначається геометрією плану приміщення.

Ключові слова: структуровані кабельні системи, Інтернет речей, точка розподілу, кутовий розв’язок, однопарний Ethernet, 10BASE-T1L, неперервне наближення.

ДСТУ ISO/IEC 11801-1:2018 обмежує канал горизонтальної підсистеми ста метрами, з яких на стаціонарну лінію припадає 90 м [1]. Цифра має конкретне походження: її отримали з бюджету загасання чотирипарного каналу для офісної будівлі, де робочі місця стоять щільно й відстань до поверхового розподільника рідко перевищує кілька десятків метрів. Для сучасних виробничих приміщень цього виявляється недостатньо. Довжина стаціонарної лінії у 90 м дозволяє покривати площу приблизно у 25000 м², натомість площі типових виробничих корпусів в декілька разів більше. Клас застосувань, до якого належить сегмент,

описано в ISO/IEC 11801-6:2017 [8]: це кабельні системи розподілених інженерних служб будівлі, більшість пристроїв яких живиться дистанційно, тому радіоканал питання траси не знімає. Проектувальник, підчас планування розташування розподільники в приміщенні площею кілька десятків тисяч квадратних метрів, керується радіусом покриття, а не кількістю портів або економічними показниками. Кількість точок розподілу задана ззовні, і економічні показники враховуються після того, як ця кількість зафіксована. Таким чином, задача вибору, яка в офісній будівлі має внутрішній розв’язок, у виробничих приміщення виходить. Наявні порівняльні огляди міжнародних і національних стандартів кабельних систем, зокрема проведені в [11], критерію вибору структури не розглядають, оскільки це лежить поза предметом самих стандартів.

Задача належить до класу задач розміщення. В [2] продемонстровано, що для широкого класу таких задач цільова функція чутливіша до щільності розміщення вузлів обслуговування, ніж до їхніх точних координат. У роботі [3] систематизовано апарат неперервних наближень, а в [4] запропонували процедуру переведення неперервного розв’язку в дискретний набір позицій. Відома з цієї літератури залежність оптимальної кількості вузлів обслуговування виду степеня дві третини від добутку кількості клієнтів на корінь із площі виведена для необмеженої області. Питання, яке лишається без відповіді, полягає в тому, чи застосовна вона взагалі, коли довжина лінії обмежена нормативом.

Мета роботи полягає в тому, щоб описати цей граничний режим формально, отримати для нього цілочислову корекцію нижньої межі й оцінити, які проєктні рішення в такому режимі впливають на вартість.

Нехай N сенсорних вузлів розподілені по прямокутному приміщенню розмірами W × L та площею A рівномірно, а обслуговують їх k точок розподілу. Кабель не йде до вузла по прямій: він прокладений у лотках, а лотки прокладають уздовж будівельних осей, тому відстань вимірюється манхеттенською метрикою. Для зони розмірами w × l з точкою розподілу в центрі середня манхеттенська відстань до рівномірно розподіленого вузла дорівнює (w + l)/4, а максимальна, до кута зони, дорівнює (w + l)/2. Кожна лінія має ще вертикальний спуск h від лотка до пристрою та запас на монтаж β, який покриває вигини траси, обхід технологічного обладнання й похибку обміру. Сумарна довжина горизонтального кабелю та приведена до його погонної вартості вартість інфраструктури дорівнюють

$$L_k(k) = \beta \cdot N \cdot ((w + l)/4 + h); \quad C(k)/c_L = r \cdot L_k(k) + \varphi \cdot M(k) + \gamma(k) \cdot k + N \cdot (\tau + \pi), \tag{1}$$

де r – відношення погонної вартості застосованого кабелю до кабелю категорії 6A; φ – те саме для магістрального кабелю; M(k) – довжина магістралі від центральної апаратної до центрів зон; γ(k) – вартість однієї точки розподілу; τ – вартість термінального адаптера на вузол; π – вартість порту комутатора. Останній доданок від k не залежить, оскільки портів завжди N, проте він входить до бази, від якої рахуються відсотки економії, і нижче буде показано, наскільки вибір цієї бази змінює висновки. Прирівнявши похідну до нуля при сталій γ, дістаємо класичний вигляд оптимуму, поряд з яким запишемо умову досяжності найдалшого вузла зони:

$$k^* = (r \cdot \beta \cdot N \cdot \sqrt{A} / (4\gamma))^{2/3}; \quad \beta \cdot ((w + l)/2 + h) \leq D_{max} \tag{2}$$

Коли друга умова активна, задача має кутовий розв’язок: мінімум лежить на межі допустимої області, вираз для k* до нього не застосовний, і кількість точок розподілу диктується геометрією плану. Практичний наслідок полягає в тому, що обчислення k* у такому разі дає число, яке не можна реалізувати.

Неперервне наближення дає тут ще одну похибку, вже суто арифметичну. Підстановка квадратної зони в умову досяжності веде до оцінки $k \geq [A/(D_{max}/\beta - h)^2]$, тоді як реальний план ділиться на m × n прямокутних зон. Допустимі значення k обмежені добутками цілих чисел, а сума сторін зони визначається найкращим розкладом

$$s(k) = \min\{ W/m + L/n : m \cdot n = k, m, n \in \mathbb{N} \}. \tag{3}$$

Функція s(k) немонотонна, і для проєктування це має прямий наслідок. Для витягнутого плану прості значення k можна розставити тільки в один ряд, а ряд вузьких смуг має більший периметр зони за компактнішу сітку. Тому збільшення кількості точок розподілу може погіршити покриття.

Розрахунок виконано для одноповерхового виробничого корпусу з розмірами 300 × 120 м за планом, площею A = 36 000 м², з N = 360 сенсорно-виконавчими вузлами, що відповідає сітці приблизно 10 × 10 м. Прийнято h = 6 м, β = 1,15, φ = 1,0. Результати розбиття плану зведено в таблиці 1.

Таблиця 1 – Цілочислові розбиття плану 300 × 120 м

k	m × n	s(k), м	Найдовша лінія, м	Lk(k), м	Допустимо за (2)
2	2 × 1	270,0	162,1	30 429	ні
4	4 × 1	195,0	119,0	22 666	ні
6	3 × 2	160,0	98,9	19 044	ні
7	7 × 1	162,9	100,5	19 340	ні
8	4 × 2	135,0	84,5	16 456	так
10	5 × 2	120,0	75,9	14 904	так
12	6 × 2	110,0	70,1	13 869	так

Умова досяжності виконується починаючи з $k = 8$: розбиття 4×2 дає зони 75×60 м і найдовшу лінію 84,5 м. Найкраще розбиття при $k = 6$ дає вже 98,9 м і в норматив не вкладається. Квадратна ідеалізація тієї самої умови дає $36\,000/(90/1,15 - 6)^2 = 6,89$, тобто сім точок, і знижує потребу на одиницю. Рядок $k = 7$ ілюструє немонотонність $s(k)$: сім точок покривають зону гірше, ніж шість, бо сім розкладається лише як 7×1 .

Отриманий розв’язок далі використано для порівняння трьох архітектур, які по-різному поводяться з обмеженням довжини. Варіант А зберігає обмеження: канали категорії 6А від повних поверхових апаратних, $D_{\max} = 90$ м, $r = 1$, вартість вузла $\gamma_f = 3000$ еквівалентних метрів кабелю. Варіант В обмеження знімає: однопарні канали 10BASE-T1L за IEEE Std 802.3cg-2019 [5] допускають лінію до 1000 м, а ANSI/TIA-568.5 нормує канал 400 м [6]; прийнято $r = 0,55$ і термінальний адаптер $\tau = 15$ на вузол. Варіант С обмеження зберігає й здешевлює його виконання: одна апаратна, волоконна магістраль до зонних розподільників вартістю $\gamma_z = 600$ і короткі мідні відгалуження.

Вартість вузла розподілу задано покомпонентно. Повна апаратна $\gamma_f = 3000$ складається з будівельної підготовки приміщення 1000, джерела безперебійного живлення 700, розподільчого щита і ввідної лінії 500, шафи 19” 400, заземлення й вентиляції 400. Зонний розподільник $\gamma_z = 600$ вкпочає настіну шафу IP54 250, польовий комутатор із живленням від магістралі 200, кріплення та вводи 150. Місткість шафи скінченна, тому вартість вузла описано східчаюю функцією $\gamma(k) = \gamma_0 \cdot \lceil N/(k \cdot r_{\text{ш}}) \rceil$ з $r_{\text{ш}} = 96$ портів для апаратної та 48 для зонної шафи. Ця форма дозволяє зосереджувати вузли, проте штрафує таке зосередження рівно на вартість додаткового конструктива. Результати розрахунку наведено в таблиці 2 і на рисунку 1.

Варіант А працює на обмеженні. Варіант В має мінімум при $k = 4$, тоді як при інших значення k виникає необхідність у додаткових шафах для розміщення портів, що знижає отриману економію на мінімізації довжини кабелю. Варіант С дає найнижчу вартість. Контрольний рядок (табл. 2) показує, що варіант С поступається варіанту А на 2,1 % вартості за умов, що $\gamma_z = \gamma_f$. Тобто перевага варіанта С цілком визначається співвідношенням γ_z/γ_f і втрачається у разі його погіршення. Варіант В поводитьсь так само чутливо, тільки щодо іншого параметра: якщо враховувати лише вартість кабелю й точок розподілу, і не враховувати вартість портів та адаптерів, його ефективність зросте з 23 до 40 %. Таким чином вибір того, які показники враховуються при визначенні загальної вартості має більший вплив ніж вибір способу реалізації самого фізичного рівня.

Таблиця 2 – Приведена вартість трьох архітектур, C/cL

Варіант	Механізм	копт	C/cL	До варіанта А	Зона +5 %
А	обмеження збережене	8	45 856	—	відсутня
В	обмеження знято	4	35 267	−23 %	відсутня
С	вузол здешевлено	10	27 477	−40 %	$k = 8 \dots 14$
С (контроль)	$\gamma_z = \gamma_f$	8	46 822	+2,1 %	відсутня

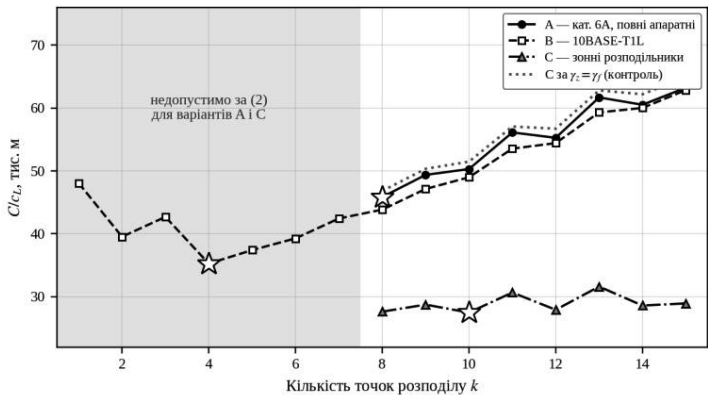


Рисунок 1 – Приведена вартість трьох архітектур залежно від кількості точок розподілу

Чутливість до решти параметрів перевірено варіюванням кожного окремо. Варіант В випереджає С, якщо погонна вартість однопарного кабелю падає нижче 0,21 від кабелю категорії 6А або якщо вартість повної апаратної опускається до 1000 еквівалентних метрів; в останньому випадку різниця становить 0,8 % і лежить у межах похибки моделі. Варіант С поступається, якщо вартість зонного розподільника перевищує 1556 еквівалентних метрів. Окремо діє тепловий режим кабельного пучка. Під навантаженням кабелі РоЕ типу 4, для якого IEEE Std 802.3bt-2018 відводить на канал до 18,7 Вт [9], розмір пучка обмежений нагріванням; аналітичні моделі теплового опору пучка однакових кабелів [10] дають цю межу в замкненій формі. За гранично допустимого розміру пучка 24 кабелі умова $k \geq 15$ підвищує вартість варіанта А на 38 %, а варіанта С лише на 5 %, оскільки в другому випадку мідні відгалуження коротші й пучок біля вузла тонший.

Пропускна здатність 10 Мбіт/с у варіанті В перевірена окремо. За чотирьох точок розподілу на одну припадає 90 вузлів, і за середньої інтенсивності 100 кбіт/с на вузол сукупний трафік становить 9 Мбіт/с.

Обмеженням є затримка: серіалізація кадру 256 байтів забирає 204,8 мкс і лишає в циклі 1 мс запас близько п’яти разів, тоді як повнорозмірний кадр 1518 байтів займає 1214 мкс і в такий цикл не вкладається. Змішування телеметрії з об’ємними передачами в сегменті з жорстким циклом вимагає механізму переривання кадрів, визначеного для однопарних сегментів у IEEE Std 802.3de-2022 [7].

Висновки. Обмеження досяжності виводить задачу вибору кількості точок розподілу з внутрішнього оптимуму на межу допустимої області, і в цьому режимі класичний вираз неперервного наближення до розв’язку не застосовний. Для промислових будівель площею в кілька десятків тисяч квадратних метрів такий режим є типовим. Квадратна ідеалізація умови досяжності знижує нижню межу для витягнутого плану: у розглянутому прикладі вона дає сім точок розподілу проти восьми за цілочисловим розбиттям, а немонотонність $s(k)$ додатково виключає прості значення k . Вартість вузла розподілу доцільно описувати східчаюю функцією, оскільки саме вона зміщує оптимум архітектур із малою кількістю точок розподілу. Різниця між трьома розглянутими архітектурами становить від 23 до 40 %, проте кожна з цих величин простежується до одного вартісного припущення: контрольний розрахунок при рівних вартостях вузла показує, що волоконний варіант поступається базовому на 2,1 %, а звуження вартісної бази піднімає розрахункову економію однопарного варіанта з 23 до 40 %. Практичний висновок полягає в тому, що вартість вузла розподілу й те, які показники вартості враховуються в проєкті, впливають на підсумок сильніше за вибір способу реалізації фізичного рівня, і саме їх у проєкті доцільно брати до уваги.

Література

1. ДСТУ ISO/IEC 11801-1:2018. Інформаційні технології. Кабельні системи загальної призначеності для приміщень користувачів. Частина 1. Загальні вимоги (ISO/IEC 11801-1:2017, IDT). Київ : ДП «УкрНДНЦ», 2018.

2. Newell G. F. Scheduling, location, transportation, and continuum mechanics: some simple approximations to optimization problems. SIAM Journal on Applied Mathematics. 1973. Vol. 25, No. 3. P. 346–360. DOI: 10.1137/0125037.

3. Daganzo C. F. Logistics Systems Analysis. 4th ed. Berlin ; Heidelberg : Springer, 2005. XVII, 296 p. DOI: 10.1007/3-540-27516-9.

4. Ouyang Y., Daganzo C. F. Discretization and validation of the continuum approximation scheme for terminal system design. Transportation Science. 2006. Vol. 40, No. 1. P. 89–98. DOI: 10.1287/trsc.1040.0110.

5. IEEE Std 802.3cg-2019. IEEE Standard for Ethernet. Amendment 5: 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors. New York : IEEE, 2020. DOI: 10.1109/IEEEESTD.2020.8982251.

6. ANSI/TIA-568.5:2022. Balanced Single Twisted-pair Telecommunications Cabling and Components Standard. Arlington : Telecommunications Industry Association, 2022.

7. IEEE Std 802.3de-2022. IEEE Standard for Ethernet. Amendment: Enhancements to the MAC Merge Function and the Time Synchronization Service Interface for Point-to-Point 10 Mb/s Single Pair Ethernet. New York : IEEE, 2022.

8. ISO/IEC 11801-6:2017. Information technology. Generic cabling for customer premises. Part 6: Distributed building services. Geneva : ISO/IEC, 2017. 37 p.

9. IEEE Std 802.3bt-2018. IEEE Standard for Ethernet. Amendment 2: Physical Layer and Management Parameters for Power over Ethernet over 4 pairs. New York : IEEE, 2019. DOI: 10.1109/IEEEESTD.2019.8632920.

10. Henke A., Frei S. Analytical thermal cable model for bundles of identical single wire cables. IEEE Transactions on Power Delivery. 2023. Vol. 38, No. 5. P. 3107–3116. DOI: 10.1109/TPWRD.2023.3272837.

11. Мадінов М., Руденко Н. Стандарти як основа інформаційно-комунікаційних технологій: дослідження міжнародних стандартів комунікаційних систем. Сучасний стан наукових досліджень та технологій в промисловості. 2024. № 4(30). С. 153–164. DOI: 10.30837/2522-9818.2024.4.153.

УДК 004.056.55:681.518.54

Іщенко А. Д., Русаловський В. Б., Калюжний Л. В., Рущенко О. В.

МЕХАНІЗМ АВТЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ ПЛАГІНА MOSQUITTO-AUTH-PLUGIN У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ З ТОПОЛОГІЄЮ MESH

Державний університет інтелектуальних технологій і зв'язку, м. Одеса
artem.ischchenko@gmail.com, it.dbo.od@gmail.com, leonid.kalyuzhnyy@gmail.com, rushenko64@gmail.com

Анотація. Розглянуто практичний підхід до організації автентифікації та розмежування доступу в бездротових сенсорних мережах з топологією Mesh на основі брокера повідомлень Eclipse Mosquitto та плагіна автентифікації mosquitto-auth-plugin. Описано функціональні можливості плагіна, підтримувані бекенди зберігання облікових даних (MySQL, PostgreSQL, Redis, LDAP, HTTP, CDB) та механізм списків контролю доступу (ACL), що дозволяє ґранулярно керувати правами публікації та підписки на рівні MQTT-топиків. Проаналізовано архітектурні переваги рішення для сенсорних вузлів з обмеженими енергетичними та

обчислювальними ресурсами, а також окреслено перспективні напрями подальшого розвитку та практичного застосування плагіна у промислових IoT-системах, «розумних» містах та системах екологічного моніторингу.

Ключові слова: бездротові сенсорні мережі, Mesh-топологія, MQTT, mosquito-auth-plugin, автентифікація, ACL, контроль доступу, IoT.

Бездротові сенсорні мережі (БСМ) з Mesh-топологією широко застосовуються в системах «Інтернету речей» (IoT), промисловій автоматизації, «розумних» містах та медичному моніторингу. Децентралізована природа Mesh-архітектури забезпечує відмовостійкість і масштабованість, проте водночас породжує суттєві виклики у сфері інформаційної безпеки [1].

Протокол MQTT (Message Queuing Telemetry Transport) став де-факто стандартом для IoT-комунікацій завдяки своїй легковаговості та моделі публікації/підписки. Однак базова специфікація MQTT не передбачає надійних механізмів автентифікації та авторизації, покладаючись на прикладний рівень безпеки [2]. Це відкриває простір для дослідження спеціалізованих рішень із контролем доступу на рівні брокера повідомлень, придатних для вузлів з обмеженими обчислювальними та енергетичними ресурсами.

Додатково ускладнює ситуацію Mesh-топологія: на відміну від мереж із фіксованою зірковою структурою, тут вузли можуть динамічно змінювати маршрути, а кількість активних з'єднань з брокером змінюється в часі. Це висуває вимоги не лише до ефективності одиної операції автентифікації, а й до масштабованості рішення при одночасному підключенні великої кількості вузлів.

Сенсорні вузли, як правило, мають жорсткі обмеження за обчислювальною потужністю, обсягом пам'яті та ємністю акумулятора, що робить традиційні важковагові механізми автентифікації (наприклад, повне рукописання TLS/SSL) малоприматними для щоденної експлуатації [3]. Разом з тим базова специфікація MQTT передає облікові дані у відкритому вигляді, що є неприйнятним для захищених систем. Постає задача обрати та практично реалізувати механізм автентифікації й авторизації, який інтегрується безпосередньо в інфраструктуру MQTT-брокера, не вимагає суттєвої модифікації клієнтської частини на сенсорних вузлах і забезпечує гранулярне розмежування прав доступу до MQTT-топиків.

Серед практичних реалізацій автентифікації для MQTT виокремлюється відкрита бібліотека mosquito-auth-plugin, яка розширює брокер Eclipse Mosquitto підтримкою множинних бекендів зберігання облікових даних – MySQL, PostgreSQL, Redis, LDAP, HTTP та CDB [4]. Така багатоваріантність дозволяє інтегрувати плагін у вже наявну корпоративну інфраструктуру безпеки без потреби розгортання окремого сервера автентифікації.

Плагін забезпечує зберігання паролів у хешованому вигляді, що суттєво підвищує стійкість до атак за словником та до витоків бази даних. Автентифікація виконується на стороні брокера під час обробки пакета MQTT CONNECT: надані клієнтом ідентифікатор і пароль зрівнюються з відповідним записом у підключеному бекенді, після чого з'єднання або приймається, або відхиляється.

Другою ключовою функцією плагіна є механізм списків контролю доступу (Access Control List, ACL), який дозволяє гранулярно керувати правами на публікацію (PUB) та підписку (SUB) для кожного MQTT-топіку окремо для кожного користувача. Правила ACL зберігаються в тому ж бекенді, що й облікові дані, і можуть використовувати маски топиків (наприклад, wsn/zone_A/#), що дозволяє задавати політики доступу як для окремих вузлів, так і для цілих сегментів мережі.

Важливою практичною особливістю плагіна є підтримка кешування результатів перевірки, що дозволяє суттєво знизити навантаження на базу даних бекенда в мережах з великою кількістю одночасних підключень і частими операціями публікації/підписки. Крім того, плагін підтримує позначення окремих облікових записів як суперкористувачів (superusers) – типово це шлюзові вузли або сервери агрегації, яким надається необмежений доступ до всіх топиків без додаткової перевірки ACL, що спрощує адміністрування мережі.

У типовій конфігурації для Mesh-мережі брокер Mosquitto з плагіном mosquito-auth-plugin розгортається на шлюзовому вузлі або окремому сервері й одночасно використовує два сховища даних: швидке кешування сесійних та ACL-рішень (наприклад, засобами Redis) і надійне довгострокове зберігання облікових записів та правил доступу (наприклад, у реляційній базі PostgreSQL). Така гетерогенна конфігурація дозволяє поєднати швидкодію оперативної перевірки з надійністю зберігання політик безпеки.

Ієрархічна структура MQTT-топиків природно відображається на топологію сенсорної мережі. Наприклад, для окремого вузла у певній зоні мережі топик може мати вигляд wsn/<zone_id>/<node_id>/<data_type>, що дозволяє задати гранулярні правила: кінцевий вузол отримує право публікації виключно на власний топик, тоді як агрегатор зони – право підписки на весь сегмент цієї зони та право публікації узагальнених даних до центральної системи. Таким чином, у разі компрометації окремого сенсорного вузла зловмисник отримує доступ лише до даних цього вузла, не маючи можливості перехопити трафік сусідніх пристроїв чи втрутитись у роботу інших сегментів мережі.

Адміністрування системи здійснюється централізовано: додавання нового вузла, зміна його прав доступу або повна ізоляція скомпрометованого пристрою виконуються шляхом редагування відповідних записів у бекенді зберігання, без потреби втручання у програмне забезпечення інших вузлів мережі. Ізоляція вузла з активною сесією додатково підсилюється примусовим розривом з'єднання з боку брокера через обліковий запис суперкористувача.

Розглянутий підхід на основі mosquito-auth-plugin має ряд практичних переваг, що визначають перспективи його подальшого застосування. По-перше, використання Mosquitto як брокера дозволяє розгорнути

систему на широкому спектрі апаратного забезпечення – від одноплатних комп'ютерів до промислових серверів – без зміни клієнтської частини сенсорних вузлів. По-друге, гнучка конфігурація бекендів спрощує інтеграцію з існуючою корпоративною інфраструктурою безпеки, зокрема з корпоративними каталогами LDAP та наявними базами даних.

Перспективним напрямом є застосування розглянутого рішення у промислових системах IoT, де кількість вузлів і сегментів мережі постійно зростає, а вимоги до розмежування доступу між виробничими дільницями є критичними. Аналогічно підхід є придатним для систем екологічного моніторингу та інфраструктури «розумних» міст, де сенсорні вузли розосереджені територіально, а централізоване управління правами доступу через ACL дозволяє оперативно реагувати на інциденти безпеки без фізичного втручання в мережу.

Подальшого розвитку потребує питання підвищення відмовостійкості рішення, оскільки модель MQTT-брокера передбачає наявність центральної точки, потенційно вразливої до відмови; перспективним є перехід до кластерних конфігурацій брокера з реплікацією даних автентифікації. Окремим напрямом є посилення захисту самого сховища облікових даних, зокрема через застосування апаратних модулів безпеки (HSM) для зберігання ключової інформації брокера, а також дослідження можливості інтеграції плагіна з сучасними хмарними IoT-платформами (AWS IoT Core, Azure IoT Hub, HiveMQ), що підтримують протокол MQTT «з коробки» [5].

Порівняно з альтернативними спеціалізованими протоколами для обмежених IoT-пристроїв, такими як стандартизований IETF протокол EDHOC (RFC 9528) [6], розглянутий підхід не потребує розгортання окремого CoAP/OSCORE-стека та сервера авторизації, що робить його практичнішим варіантом для проєктів, де вже використовується MQTT-інфраструктура або хмарні IoT-платформи з вбудованою підтримкою цього протоколу.

Висновки. У роботі розглянуто практичне застосування плагіна mosquito-auth-plugin для організації автентифікації та контролю доступу в бездротових сенсорних мережах з Mesh-топологією. Показано, що інтеграція плагіна з бекендами зберігання типу Redis/PostgreSQL дозволяє реалізувати гранулярний ACL-контроль на рівні MQTT-топиків без суттєвих змін у програмному забезпеченні сенсорних вузлів, а підтримка кешування ACL-рішень і механізму суперкористувачів забезпечує масштабованість рішення для мереж з великою кількістю вузлів.

Практична цінність розглянутого підходу полягає у можливості побудови готового до впровадження програмного стека на основі відкритого програмного забезпечення та стандартних протоколів, що суттєво знижує бар'єр входу для промислового застосування. Перспективними напрямками подальших досліджень визначено підвищення відмовостійкості брокера через кластерні конфігурації, посилення захисту сховища облікових даних апаратними засобами та інтеграцію рішення з хмарними IoT-платформами.

Література

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393–422. [https://doi.org/10.1016/S1389-1286\(01\)00302-4](https://doi.org/10.1016/S1389-1286(01)00302-4)
2. Hankerson, D., Menezes, A., & Vanstone, S. (2004). Guide to elliptic curve cryptography. Springer. <https://doi.org/10.1007/b97644>
3. Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294–1312. <https://doi.org/10.1109/COMST.2015.2388550>
4. Kuroei. (2016). mosquito-auth-plugin. GitHub. <https://github.com/kuroei/mosquito-auth-plugin>
5. Light, R. A. (2017). Mosquitto: server and client implementation of the MQTT protocol. Journal of Open Source Software, 2(13), 265. <https://doi.org/10.21105/joss.00265>
6. Selander, G., Mattsson, J., Palombini, F., & Seitz, L. (2023). Ephemeral Diffie-Hellman over COSE (EDHOC). IETF RFC 9528. <https://doi.org/10.17487/RFC9528>

УДК 004.738.5:004.056

Русаловський В.Б., Калюжний Л.В., Іщенко А.Д., Воронюк Д.В.

КОМПЛЕКСНА СИСТЕМА МОНІТОРИНГУ ТА АДАПТИВНОЇ ФІЛЬТРАЦІЇ НЕБЕЗПЕЧНОГО КОНТЕНТУ ДЛЯ КІБЕРЗАХИСТУ ДІТЕЙ У ЗАКЛАДАХ ОСВІТИ

Державний університет інтелектуальних технологій і зв'язку, м. Одеса

it.ddo.od@gmail.com, leonid.kalyuzhnyy@gmail.com, artem.ischchenko@gmail.com, itlab.stem@gmail.com

Анотація. Розглянуто підхід до побудови комплексної системи моніторингу та адаптивної фільтрації небезпечного і нецільового контенту для захисту дітей у мережі Інтернет, розробленої на

виконання методичних рекомендацій наказу МОН України № 103. На відміну від поширених засобів DNS-фільтрації, система контролює не лише браузерний трафік, а й усі застосунки та мережеві з'єднання на рівні операційної системи, що ускладнює стандартні способи обходу захисту. Наведено порівняння основних класів засобів фільтрації, архітектуру системи та структуру багаторівневого каскаду правил, оптимізованого під обмежені апаратні ресурси шкільного обладнання. Система не передбачає збирання чи зберігання персональних даних учнів. Підхід реалізовано у програмному комплексі SafeGate, пілотне впровадження якого підготовлено у закладах освіти м. Одеси.

Ключові слова: кіберзахист дітей, контентна фільтрація, моніторинг, заклади освіти, безпечний Інтернет, персональні дані.

Цифровізація освіти зробила Інтернет повсякденним робочим середовищем школяра, водночас відкривши дітям прямий доступ до контенту, здатного завдати їм фізичного та психічного розвитку: матеріалів із насильством, екстремістськими ідеями, контенту для дорослих, пропаганди наркотиків та азартних ігор. Обмеження поширення такої інформації серед дітей прямо передбачене статтею 42 Закону України «Про медіа» [1].

Для закладів освіти вимоги конкретизовано методичними рекомендаціями щодо фільтрації доступу до мережі Інтернет та протидії шкідливому контенту, затвердженими наказом МОН України № 103 від 26.01.2026 [2]. Таким чином, школи опинилися перед необхідністю впровадити технічні засоби контентної фільтрації, і питання полягає в тому, якими саме засобами цю вимогу можна виконати ефективно та законно.

Поширені сьогодні рішення зосереджені переважно на фільтрації веб-трафіку: DNS-фільтри, налаштування безпечного пошуку, браузерні розширення та проксі-сервери [3].

Досвід їх експлуатації виявляє два принципові недоліки.

По-перше, такі засоби контролюють лише браузер, тоді як значна частина трафіку сучасного комп'ютера генерується месенджерами, ігровими клієнтами та іншими застосунками, що взаємодіють з мережею напряду.

По-друге, захист на рівні DNS або браузера обходиться стандартними прийомами, добре відомими підліткам: зміною DNS-сервера, використанням VPN-сервісів або шифрованих DNS-протоколів.

Окремою проблемою залишається обмежена продуктивність шкільних комп'ютерів, на яких ресурсоемні засоби аналізу контенту [4] працюють незадовільно. Узагальнене порівняння основних класів засобів фільтрації за критеріями, суттєвими для закладу освіти, наведено в табл. 1.

У межах науково-дослідної роботи кафедри інженерії програмного забезпечення ДУІТЗ розроблено підхід, у якому контроль переноситься з рівня окремого браузера на рівень операційної системи.

Система охоплює всі встановлені застосунки та всі мережеві з'єднання комп'ютера, тому зміна DNS-сервера чи використання VPN не виводить трафік з-під контролю: фільтрація відбувається до того, як з'єднання залишає пристрій.

Архітектура системи складається з чотирьох взаємопов'язаних модулів: моніторингу, адаптивної фільтрації, централізованого управління та звітності (рис. 1).

Фільтрація побудована за багаторівневим принципом (рис. 2).

Швидкі рівні – чорні та білі списки ресурсів і категорійні правила – відсікають основну масу небажаних звернень з мінімальними витратами обчислювальної потужності.

Складніші рівні аналізу застосовуються лише до звернень, які не вдалося класифікувати швидкими правилами. Такий каскад дає змогу ефективно розпізнавати загрози на обмежених апаратних ресурсах, характерних для комп'ютерних класів українських шкіл.

Таблиця 1 – Порівняння класів засобів фільтрації доступу до мережі Інтернет у закладах освіти

Критерій	DNS-фільтрація	Браузерні засоби	Проксі-сервер	SafeGate (рівень ОС)
Точка перехоплення	DNS-запити на резолвері	WebRequest API браузера	HTTP(S)-сесії на шлюзі	Сокет-з'єднання в ядрі ОС
Охоплення застосунків	Ті, що йдуть через системний резолвер	Один браузер	Ті, що враховують системний проксі	Усі процеси
Обхід	DoH або зміна DNS адаптера	Вимкнення розширення, портативний браузер	Зняття проксі в налаштуваннях	Зупинка служби (права адміністратора)
Додаткове обладнання	Не потрібне	Не потрібне	Виділений сервер або шлюз	Не потрібне

Критерій	DNS-фільтрація	Браузерні засоби	Проксі-сервер	SafeGate (рівень ОС)
Дані, що зберігаються	Журнал усіх DNS-запитів у постачальника	Історія URL у розширенні	Повний лог URL і станцій	Факт звернення до забороненої категорії, час, клас
Точка перехоплення	DNS-запити на резолвері	WebRequest API браузера	HTTP(S)-сесії на шлюзі	Сокет-з'єднання в ядрі ОС
Охоплення застосунків	Ті, що йдуть через системний резолвер	Один браузер	Ті, що враховують системний проксі	Усі процеси

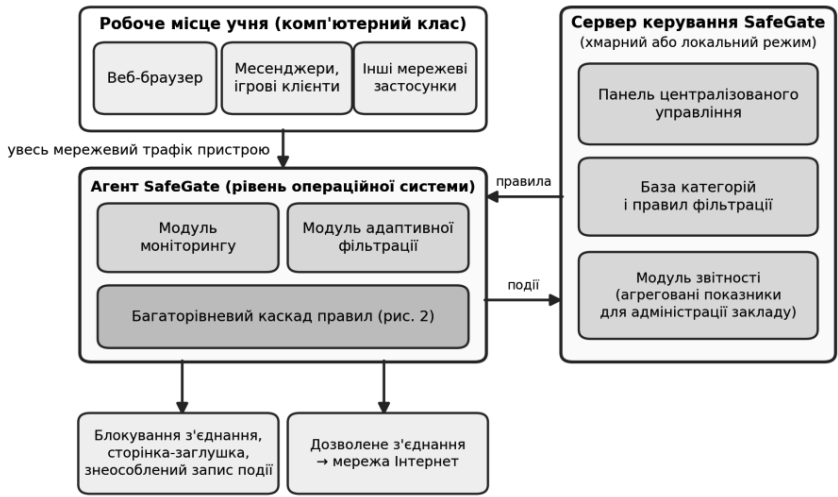


Рисунок 1 – Архітектура системи моніторингу та адаптивної фільтрації контенту

Характеристики рівнів каскаду наведено в таблиці 2.

Адаптивність системи полягає у коригуванні правил фільтрації за результатами моніторингу без втручання у програмне забезпечення робочих місць: правила оновлюються централізовано з панелі адміністратора, а профілі фільтрації диференціюються за віковими групами та призначенням комп'ютерного класу.



Рисунок 2 – Каскад багаторівневої фільтрації мережевого звернення

Таблиця 2 – Рівні каскаду фільтрації

Рівень	Метод класифікації	Вхідні дані	Обчислювальні витрати	Джерело правил
1	Списки дозволених і заборонених ресурсів	Доменне ім'я, мережева адреса	Мінімальна	Локальна база, синхронізована із сервером

Рівень	Метод класифікації	Вхідні дані	Обчислювальні витрати	Джерело правил
2	Категорійні правила	Категорія ресурсу, профіль вікової групи	Низька	Категорійна база сервера керування
3	Евристичний аналіз запиту	Ознаки URL, метадані з'єднання, репутація вузла	Середня	Набір евристик, оновлюється централізовано
4	Контентний аналіз	Текстовий і графічний вміст сторінки	Висока	Моделі класифікації контенту

Принциповою вимогою до системи є захист приватності учнів. Система не збирає і не зберігає персональних даних дітей, не відстежує їхні приватні файли та листування – оброблюються лише факти звернень до заборонених категорій ресурсів, необхідні для звітності перед адміністрацією закладу. Відповідність системи основним нормативним вимогам подано в табл. 3, а також узгоджується зі Стратегією кібербезпеки України [8].

Таблиця 3 – Відповідність системи нормативним вимогам

Вимога	Нормативне джерело	Реалізація в системі
Обмеження доступу неповнолітніх до шкідливого контенту	Стаття 42 Закону України «Про медіа» [1]	Категорійне блокування визначених груп ресурсів на рівні операційної системи
Наявність технічних засобів фільтрації в закладі освіти	Наказ МОН України № 103 [2]	Агент на кожному робочому місці та єдина політика фільтрації закладу
Мінімізація обробки даних неповнолітніх	Закон України № 2297-VI [5], Регламент (ЄС) 2016/679	Обробляються лише знеособлені факти звернень до заборонених категорій
Невтручання в приватне життя дитини	Конвенція ООН про права дитини [6]	Не аналізуються листування, приватні файли та зміст дозволених ресурсів
Протидія матеріалам сексуального насильства над дітьми	Директива 2011/93/ЄС [7]	Безумовне блокування відповідної категорії незалежно від профілю користувача

Підхід реалізовано у програмному комплексі SafeGate, що підтримує як хмарний, так і локальний режими розгортання – останній важливий для закладів з нестабільним інтернет-з'єднанням. Розгортання не потребує заміни наявного обладнання. У межах НДР, погодженої з Департаментом освіти та науки, підготовлено пілотне впровадження системи у двох ліцеях м. Одеси: проведення аудиту ІТ-інфраструктури закладів, налаштування фільтрації у реальній мережі та навчання персоналу заплановано на перший етап дослідження, а зворотний зв'язок користувачів буде використано для коригування правил і параметрів системи. Під час пілотних випробувань передбачено оцінити точність фільтрації (частку хибних блокувань і пропущених звернень), накладні витрати на обчислювальні ресурси робочої станції, затримку встановлення з'єднання, а також стійкість захисту до типових способів обходу.

Висновки. Виконання вимог наказу МОН України № 103 засобами, що фільтрують лише браузерний трафік, не забезпечує реального захисту: такі засоби обходяться стандартними прийомами і не охоплюють трафік застосунків. Запропонована система SafeGate для моніторингу та адаптивної фільтрації небезпечного і нецільового контенту для захисту дітей у мережі Інтернет переносить контроль на рівень операційної системи, поєднує багаторівневу фільтрацію з централізованим управлінням і при цьому не збирає персональних даних учнів. SafeGate – комплекс, що готується до пілотних випробувань в одеських закладах освіти, за результатами яких буде оцінено точність і продуктивність фільтрації та сформовано методичні рекомендації.

Література

1. Про медіа: Закон України від 13.12.2022 № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20>
2. Про затвердження методичних рекомендацій щодо способів фільтрації доступу до мережі Інтернет та протидії шкідливому контенту в закладах освіти: наказ МОН України від 26.01.2026 № 103.
3. Gómez Hidalgo, J. M., Puertas Sanz, E., Carrero García, F., & De Buenaga Rodríguez, M. (2009). Web content filtering. *Advances in Computers*, 76, 257–306. [https://doi.org/10.1016/S0065-2458\(09\)01007-9](https://doi.org/10.1016/S0065-2458(09)01007-9)
4. Hammami, M., Chahir, Y., & Chen, L. (2006). WebGuard: A Web filtering engine combining textual, structural, and visual content-based analysis. *IEEE Transactions on Knowledge and Data Engineering*, 18(2), 272–284. <https://doi.org/10.1109/TKDE.2006.34>
5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>

6. Конвенція ООН про права дитини від 20.11.1989 (ратифікована Постановою ВР України від 27.02.1991 № 789-ХІІ).
7. Директива 2011/93/ЄС Європейського Парламенту і Ради від 13.12.2011 про боротьбу із сексуальним насильством над дітьми та дитячою порнографією.
8. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021.

УДК 004.056:004.7

Кривченко А.А., Кривченко Ю.В.

РЕАЛІЗАЦІЯ ПРОГРАМНОЇ МОДЕЛІ АНАЛІЗУ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

ВСП «Одеський технічний фаховий коледж Одеського Національного технологічного університету»
Nastya.otk.2014@gmail.com

Анотація. Виконано аналіз та програмну реалізацію моделі оцінювання захищеності комп'ютерних мереж у середовищі Embarcadero C++Builder. Розглянуто вплив зовнішніх і внутрішніх загроз, технічних відмов та порушень працездатності окремих вузлів на загальний стан мережевої інфраструктури. Запропоновано комплексний підхід до оцінювання стійкості мережі, що враховує показники захищеності, надійності та живучості. Реалізовано алгоритми розрахунку часткових та інтегрального показників, механізми валідації вхідних даних, візуалізації результатів, формування рекомендацій і прогнозування деградації технічного стану мережі. Проведене тестування підтвердило коректність обчислювальних алгоритмів та можливість практичного використання розробленої моделі як інструменту підтримки прийняття рішень під час адміністрування й модернізації комп'ютерних мереж.

Ключові слова: комп'ютерна мережа, інформаційна безпека, захищеність, стійкість, надійність, живучість, програмна модель, C++Builder, прогнозування.

Сучасні комп'ютерні мережі функціонують в умовах постійного впливу зовнішніх і внутрішніх дестабілізуючих факторів. До них належать мережеві атаки, шкідливе програмне забезпечення, несанкціонований доступ, помилки персоналу, технічні несправності обладнання, порушення каналів зв'язку та відмови окремих елементів мережевої інфраструктури. За таких умов забезпечення інформаційної безпеки не може обмежуватися лише виявленням окремих вразливостей. Необхідним є комплексне оцінювання здатності мережі зберігати функціональність під впливом різних типів загроз та відмов.

Поширені засоби аналізу захищеності, зокрема Nmap, Nessus та OpenVAS, ефективно вирішують завдання пошуку відкритих портів, аналізу конфігурацій, ідентифікації активних сервісів і виявлення відомих вразливостей. Водночас результат їхньої роботи переважно характеризує поточний технічний стан окремих елементів мережі та не завжди дає змогу сформувати узагальнену кількісну оцінку працездатності мережевої інфраструктури в цілому. Тому актуальним є використання математичних і програмних моделей, які дозволяють агрегувати часткові характеристики та формувати інтегральний показник стану системи.

У межах роботи запропоновано програмну модель комплексного аналізу захищеності комп'ютерної мережі, в основу якої покладено оцінювання трьох взаємопов'язаних характеристик: захищеності, надійності та живучості.

Показник захищеності характеризує здатність засобів інформаційного захисту протидіяти зовнішнім і внутрішнім загрозам. Під час його визначення враховуються ймовірності успішної реалізації відповідних атак та ефективність застосованих механізмів захисту.

Показник надійності визначає ймовірність безвідмовного функціонування технічних засобів мережі протягом заданого періоду. На відміну від статичної оцінки, у розробленій моделі реалізовано ітеративний механізм накопичення відмов. Це дає змогу послідовно враховувати декілька подій, пов'язаних із несправністю серверів, комутаторів, каналів зв'язку та інших елементів мережевої інфраструктури.

Показник живучості характеризує здатність мережі продовжувати виконання критичних функцій після виходу з ладу частини її компонентів або успішної реалізації деструктивного впливу. На його значення впливають резервування каналів зв'язку, дублювання обладнання, застосування RAID-масивів, кластеризації та інших механізмів забезпечення безперервності функціонування.

Для формування комплексної оцінки використовується мультиплікативна модель. Інтегральний показник стійкості комп'ютерної мережі визначається як

$$S = K_{\text{зах}} \cdot K_{\text{над}} \cdot K_{\text{жив}}$$

де **K_{зах}** — коефіцієнт захищеності мережі; **K_{над}** — коефіцієнт надійності; **K_{жив}** — коефіцієнт живучості

Використання мультиплікативної залежності обумовлено необхідністю врахування критичного впливу кожного окремого показника на стан системи. За такого підходу суттєве зниження одного з коефіцієнтів автоматично призводить до зменшення інтегрального показника, навіть якщо інші характеристики мають високі значення. Це дозволяє уникнути ситуації, коли високий рівень технічної надійності штучно компенсує критично низький рівень інформаційного захисту або живучості.

Програмну реалізацію моделі виконано мовою C++ у середовищі Embarcadero C++Builder із використанням бібліотеки VCL. Вибір даного середовища забезпечив можливість поєднання обчислювального ядра з графічним інтерфейсом та засобами оперативної візуалізації результатів.

Архітектуру програмного застосунку побудовано за модульним принципом. До її складу входять модуль введення та валідації вихідних даних, обчислювальне ядро, модуль візуалізації, а також блок аналітичної обробки та прогнозування. Такий підхід забезпечує логічне розмежування функцій програмного забезпечення та створює можливості для його подальшого розширення.

Обчислювальний алгоритм передбачає послідовне виконання етапів введення початкових параметрів, перевірки їх коректності, визначення часткових коефіцієнтів, розрахунку інтегрального показника та інтерпретації отриманого результату. Для ймовірнісних параметрів передбачено контроль допустимого діапазону від 0 до 1. Обробка помилкових значень та некоректного введення реалізована із застосуванням механізмів обробки виняткових ситуацій.

Особливістю програмної моделі є реалізація ітеративного алгоритму оцінки надійності. Після введення кожної нової події відмови значення відповідного коефіцієнта перераховується з урахуванням попередніх подій. Передбачено також функцію Undo, яка дає можливість відновити попередній стан розрахунку у разі помилкового введення даних. Такий механізм забезпечує моделювання накопичувального впливу несправностей на загальну працездатність мережі.

Для спрощення інтерпретації результатів у застосунку використано графічну та кольорову індикацію. Часткові показники відображаються на гістограмі, що дозволяє візуально визначити найменший із них та локалізувати потенційне «вузьке місце» мережевої інфраструктури. Інтегральна оцінка супроводжується кольоровим індикатором типу «світлофор»: зелений колір відповідає оптимальному стану, жовтий сигналізує про необхідність додаткової уваги, а червоний — про критичний рівень стійкості.

Важливою складовою програмного забезпечення є модуль підтримки прийняття рішень. На основі порівняльного аналізу часткових коефіцієнтів програма визначає параметр, який найбільше впливає на зниження загального рівня стійкості, та формує відповідні рекомендації. Залежно від отриманих результатів такими рекомендаціями можуть бути посилення засобів інформаційного захисту, оновлення антивірусного програмного забезпечення, модернізація мережевого обладнання, впровадження резервування або створення додаткових засобів резервного копіювання.

Додатково реалізовано прогнозний модуль Aging Forecast, призначений для оцінювання зміни технічного стану мережі в часі. Модель враховує природне зниження надійності обладнання та дає змогу розрахувати прогнозне значення комплексного показника стійкості. Це дозволяє використовувати програму не лише для аналізу поточного стану інфраструктури, а й для планування її профілактичного обслуговування та модернізації.

Перевірку коректності розробленої моделі проведено із використанням контрольних наборів вхідних даних. Під час тестування перевірялися розрахунки часткових показників, ітеративний алгоритм оцінювання надійності, робота механізму скасування останньої операції, комплексний розрахунок стійкості, функції прогнозування, візуалізації та автоматичного формування рекомендацій.

Порівняння програмних результатів із контрольними ручними розрахунками засвідчило їх збіг до третього знака після коми. Зокрема, для набору значень $(K_{\{z\}}=0_{\{, \}}95)$, $(K_{\{nad\}}=0_{\{, \}}95)$ та $(K_{\{giv\}}=0_{\{, \}}90)$ отримано інтегральний показник $(S=0_{\{, \}}812)$, що відповідає оптимальному стану мережі. Для значень 0,80; 0,80 та 0,85 отримано $(S=0_{\{, \}}544)$, що сигналізує про необхідність підвищеної уваги. У критичному сценарії при значеннях 0,60; 0,70 та 0,65 інтегральний коефіцієнт становив $(S=0_{\{, \}}273)$, а система сформуvala попередження про критичний стан.

Результати тестування підтвердили правильність реалізації математичної моделі, коректність алгоритмів прийняття рішень та відповідність програмних результатів розрахунковим значенням. Введення некоректних параметрів не призводить до аварійного завершення роботи програми завдяки застосованим механізмам валідації та обробки виняткових ситуацій.

Висновки. Розроблена програмна модель забезпечує перехід від локального аналізу окремих вразливостей до комплексної кількісної оцінки стану комп'ютерної мережі. Поєднання показників захищеності, надійності та живучості дозволяє врахувати як інформаційні загрози, так і технічний стан мережевої інфраструктури. Реалізований програмний застосунок автоматизує виконання розрахунків, забезпечує візуалізацію результатів, виявлення критичних параметрів, формування рекомендацій та прогнозування зміни стану мережі.

Практичне значення отриманих результатів полягає у можливості використання розробленого програмного забезпечення системними адміністраторами та фахівцями з інформаційної безпеки як інструменту підтримки прийняття рішень. Застосування моделі дозволяє оперативно визначати слабкі елементи мережевої інфраструктури, оцінювати наслідки потенційних відмов та атак, обґрунтовувати необхідність модернізації

обладнання й засобів захисту, а також планувати профілактичні заходи з урахуванням прогнозованого зниження надійності системи.

Література

1. Колосов А. М., Колосова К. А. Управление стійкістю підприємства: монографія. Старобільськ: Вид. ЛНУ імені Тараса Шевченка, 2016. 336 с.
2. Собчук В. В., Барабаш О. В., Основи забезпечення функціональної стійкості інформаційних систем підприємств в умовах впливу дестабілізуючих факторів: монографія. Київ: Міленіум, 2022. 272 с.
3. В'юніков, О. О. Дослідження методів підвищення надійності комп'ютерних систем у критично важливих інфраструктурах – Хмельницький: ХНТУ, 2025. – 118 с.
4. Ланде Д.В., Субач І.Ю. Візуалізація та аналіз мережевих структур. Навчальний посібник. – К.: ІСЗІ КПІ ім. Ігоря Сікорського, 2020. – 79 с.

УДК 004.056.53:005.334

Бакалинський О.О.

АКСІОМАТИЧНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ КРИТИЧНИХ ФУНКЦІЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

*Інститут проблем моделювання в енергетиці ІПМЕ ім. Г.Пухова НАН України
baov1970@gmail.com*

Анотація. У роботі запропоновано аксіоматичний підхід до формалізації критичних функцій критичної інфраструктури. Показано, що попри широке використання поняття критичної функції в концепціях операційної стійкості, воно залишається переважно нормативною категорією без формального математичного визначення. Сформульовано базові визначення функції та критичної функції, побудовано аксіоматичну основу з шести аксіом, доведено теорему про мінімальну структуру критичної функції та запропоновано її узагальнену формальну модель. Введено показник системної значущості критичної функції як характеристики її місця в структурі міжфункціональних взаємозалежностей.

Ключові слова: критична інфраструктура, критична функція, операційна стійкість, системний ризик, аксіоматичний підхід, системна значущість.

ВСТУП

У сучасних концепціях операційної стійкості дедалі більшого поширення набуває поняття критичної функції, під яким розуміють здатність організації підтримувати виконання функцій, порушення яких спричиняє неприйнятні наслідки [1–4]. Розвиток ризику в складних системах описується послідовністю:

$$R = pH \rightarrow SR \rightarrow ICF_i,$$

де класична формула ризику [5] переходить у показник впливу сукупності взаємопов'язаних ризиків на критичну функцію $I_{CF_i} = F(R_1, R_2, \dots, R_n)$, що й мотивує розгляд критичної функції як самостійного математичного об'єкта. Це поняття є центральним у документах Basel Committee on Banking Supervision, а також у Regulation DORA, CER Directive та NIS2 Directive [1–4]. Водночас аналіз літератури свідчить, що критична функція залишається переважно нормативною категорією: відсутні її формальне математичне визначення, аксіоматика та формальна модель як самостійного об'єкта аналізу. Це створює розрив між сучасними концепціями операційної стійкості та математичним апаратом аналізу системного ризику.

Метою роботи є побудова аксіоматичної основи критичної функції як нового математичного об'єкта та розроблення її формальної моделі як базового об'єкта оцінювання стійкості критичної інфраструктури. Наукова новизна полягає в тому, що критична функція вперше розглядається не як управлінська чи нормативна категорія, а як самостійний математичний об'єкт.

1. БАЗОВІ ВИЗНАЧЕННЯ

Функцію системи подамо як відображення множини вхідних ресурсів у множину вихідних результатів:

$$F: I \rightarrow O, \tag{1}$$

де I – множина вхідних ресурсів; O – множина вихідних результатів.

Визначення 1. Критичною функцією називатимемо функцію, втрата або деградація якої призводить до неприйнятних наслідків для функціонування системи, сектору або суспільства [1–4].

Рівень виконання критичної функції CF_i позначимо $L(CF_i)$, причому:

$$0 \leq L(CF_i) \leq 1, \tag{2}$$

де $L(CF_i) = 1$ відповідає повному виконанню функції, а $L(CF_i) = 0$ – її повній втраті. Деградація функції визначається як $Deg(CF_i) = 1 - L(CF_i)$.

2. АКСІОМАТИЧНА ОСНОВА КРИТИЧНОЇ ФУНКЦІЇ

Для формалізації критичної функції введено систему з шести аксіом, які виконуються для будь-якої критичної функції незалежно від сектору критичної інфраструктури, типу оператора чи характеру послуг, що надаються.

Аксіома 1 (результату). Будь-яка критична функція має визначений результат виконання:
 $\exists O_i: CF_i \rightarrow O_i$.

Аксіома 2 (входів). Будь-яка критична функція має непорожню множину необхідних входів:
 $Inputs_i \neq \emptyset$.

Аксіома 3 (залежностей). Будь-яка критична функція має непорожню множину залежностей:
 $Dependencies_i \neq \emptyset$.

Аксіома 4 (допустимої області функціонування). Існує область Ω_i , така що $L(CF_i) \in \Omega_i$.
Аксіома 5 (стійкості). Будь-яка критична функція має непорожню множину характеристик стійкості:
 $Res_i \neq \emptyset$.

Аксіома 6 (взаємного впливу). Будь-яка критична функція потенційно впливає на інші критичні функції: $CF_i \rightarrow CF_j$.

Аксіоми 1 і 2 визначають функціональну складову критичної функції, аксіоми 3 і 5 – її системну складову, аксіома 6 – мережеву складову, чим зумовлена потрійна природа критичної функції [6–9].

3. ФОРМАЛЬНА МОДЕЛЬ КРИТИЧНОЇ ФУНКЦІЇ

Об'єднання функціонального, системного та мережевого представлень дає узагальнену модель критичної функції^

$$CF_i = \{Owner_i, Sector_i, Subsector_i, Inputs_i, Outputs_i, Dependencies_i, Res_i\}$$
 (3)

де $Owner_i$ – власник (оператор) функції; $Sector_i, Subsector_i$ – сектор і підсектор критичної інфраструктури; $Inputs_i, Outputs_i$ – множини входів і виходів; $Dependencies_i$ – множина залежностей; Res_i – характеристики стійкості.

Теорема (про мінімальну структуру критичної функції). Будь-яка критична функція повинна містити щонайменше компоненти $Inputs_i, Outputs_i, Dependencies_i, Res_i$, тобто

$$CF_i min = \{Inputs_i, Outputs_i, Dependencies_i, Res_i\}$$
 (4)

Доведення впливає безпосередньо з аксіом 1–3 і 5: вилучення будь-якого з цих компонентів порушує відповідну аксіому, тому жоден з них не може бути виключений з мінімального опису критичної функції. Компоненти Owner_i, Sector_i, Subsector_i не визначають математичну природу функції, а характеризують її організаційну й секторальну належність, тому модель (3) є розширенням мінімальної моделі (4).

4. СИСТЕМНА ЗНАЧУЩІСТЬ КРИТИЧНОЇ ФУНКЦІЇ

Відповідно до аксіоми взаємного впливу критичність функції визначається не лише її внутрішніми властивостями, а й положенням у структурі взаємозалежностей [10]. Нехай m_{ij} характеризує силу впливу функції CF_i на функцію CF_j . Тоді системна значущість функції визначається як:

$$SI(CF_i) = \sum j = 1..nm_{ij}$$
 (5)

За значенням $SI(CF_i)$ функції поділяються на локальні ($SI \approx 0$), важливі ($SI > 0$) та системно значущі ($SI \gg 0$), втрата яких здатна створювати масштабні каскадні наслідки. Відповідно, критичність функції доцільно розглядати як функцію двох компонентів – наслідків її втрати та системної значущості:
 $Crit(CF_i) = f(Impact(CF_i), SI(CF_i))$

Висновки. Побудовано аксіоматичну основу критичної функції, як самостійного математичного об'єкта. Сформульовано систему з шести аксіом (результату, входів, залежностей, допустимої області функціонування, стійкості та взаємного впливу), доведено теорему про мінімальну структуру критичної функції та побудовано її мінімальну й узагальнену формальні моделі. Запропоновано показник системної значущості критичної функції, який характеризує її місце у структурі міжфункціональних взаємозалежностей. Отримані результати створюють математичне підґрунтя для побудови простору критичних функцій і формальних моделей стійкості критичної інфраструктури.

Література

1. Basel Committee on Banking Supervision. Principles for Operational Resilience. Basel: Bank for International Settlements, 2021.
2. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA).

3. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).
4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive).
5. Мохор В.В., Бакалинський О.В., Богданов О.В., Цуркан В.В. Інтерпретування залежності рівня простого ризику від імовірності його реалізування в термінах аналітичної геометрії // Information Technology and Security. 2017. Т. 5, № 1. С. 61–73.
6. von Bertalanffy L. General System Theory: Foundations, Development, Applications. New York: George Braziller, 1968. 295 p.
7. Simon H.A. The Architecture of Complexity // Proceedings of the American Philosophical Society. 1962. Vol. 106, No. 6. P. 467–482.
8. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies // IEEE Control Systems Magazine. 2001. Vol. 21, No. 6. P. 11–25.
9. Ouyang M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems // Reliability Engineering & System Safety. 2014. Vol. 121. P. 43–60.
10. Sukhodolia O.M. The Resilience of Critical Infrastructure and Vital Functions and Services: Conceptual Foundations and Practical Implications // Baltic Journal of Economic Studies. 2024. Vol. 10, No. 2. P. 225–236.

УДК 351:004.9

Анісімова К. С.

ТЕХНОЛОГІЇ ЕЛЕКТРОННОГО ВРЯДУВАННЯ ЯК ІНСТРУМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ДЕРЖАВНОГО УПРАВЛІННЯ УКРАЇНИ

Київський столичний університет імені Бориса Грінченка, факультет економіки та управління, здобувачка другого (магістерського) рівня вищої освіти
anis.ka.anis.ka.anis@gmail.com

Анотація. У тезах розглянуто роль цифрових технологій у трансформації державного управління України. Визначено значення електронних реєстрів, системи міжвідомчої електронної взаємодії «Трембіта» та цифрової екосистеми «Дія» для забезпечення інтегрованої взаємодії держави з громадянами і бізнесом. Окрему увагу приділено інформаційній безпеці цифрової держави, якості реєстрових даних, захисту персональних даних та кіберстійкості. Обґрунтовано, що ефективність цифровізації залежить від поєднання інтероперабельності, надійного захисту інформації та людиноцентричної організації публічних послуг.
Ключові слова: електронне врядування, цифрова трансформація, державне управління, «Дія», «Трембіта», електронні реєстри, інформаційна безпека, кіберстійкість.

Цифрова трансформація державного управління України супроводжується переходом від окремих електронних послуг до інтегрованої цифрової екосистеми. Її функціонування ґрунтується на взаємодії державних електронних реєстрів, інструментів електронної ідентифікації, системи міжвідомчого обміну даними та цифрових сервісів для громадян і бізнесу. Така модель підвищує доступність публічних послуг, однак одночасно посилює залежність держави від достовірності даних, безпеки інформаційних систем та безперервності цифрової інфраструктури.

Ключовим принципом побудови сучасної цифрової держави є інтероперабельність. Система «Трембіта» забезпечує електронний обмін даними між інформаційними ресурсами суб'єктів електронної взаємодії, що дає змогу зменшувати потребу громадянина самостійно подавати відомості, які вже перебувають у розпорядженні держави. У цьому контексті принцип once-only набуває не лише сервісного, а й безпекового значення: централізовані та стандартизовані механізми обміну мають супроводжуватися чітким розмежуванням доступу, автентифікацією та контролем операцій з даними.

Користувачьким рівнем цієї архітектури виступає цифрова екосистема «Дія». Її функціонування демонструє перехід до моделі, за якої громадянин взаємодіє з державою через єдиний цифровий інтерфейс, тоді як необхідні відомості надходять із відповідних державних інформаційних ресурсів. Такий підхід скорочує адміністративні бар'єри та кількість повторних дій користувача. Водночас зростає значення захисту персональних даних, адже порушення безпеки одного з елементів цифрової інфраструктури потенційно може впливати на довіру до всієї системи.

Особливого значення в умовах воєнного стану набуває кіберстійкість. Розширення цифрових сервісів означає, що держава має забезпечувати не тільки конфіденційність та цілісність інформації, а й доступність критично важливих послуг. До ключових напрямів належать резервування інформаційних ресурсів, безперервність роботи цифрових сервісів, захист державних реєстрів, моніторинг кіберзагроз та регулярне тестування механізмів відновлення. Отже, інформаційна безпека повинна розглядатися як невід'ємна складова цифрового врядування, а не як окремий технічний напрям.

Подальший розвиток цифрової держави пов’язаний із використанням штучного інтелекту та аналітики даних. Запровадження Dіia.AI демонструє рух до персоналізованої взаємодії з користувачем. Проте застосування AI у публічних послугах потребує особливої уваги до якості вихідних даних, захисту персональної інформації, прозорості алгоритмів, людського контролю та відповідальності за результати автоматизованої обробки. У разі інтеграції таких інструментів із державними реєстрами вимоги до кібербезпеки та управління доступом мають бути посилені.

Таким чином, захист інформації в системі електронного врядування доцільно розглядати як комплексну систему організаційних, правових і технологічних заходів. Її основою є якісні державні дані, інтероперабельна інфраструктура, контрольований обмін інформацією, захищені цифрові сервіси та механізми забезпечення стійкості. Ефективність цифрової трансформації визначається не лише кількістю електронних послуг, а здатністю держави гарантувати їх надійність, доступність, безпеку та відповідність потребам громадян.

Висновки. Цифровізація державного управління створює значні переваги для доступності та якості публічних послуг, але водночас формує нові вимоги до захисту інформації. Для України пріоритетними є забезпечення якості й актуальності реєстрових даних, розвиток інтероперабельності, кіберстійкості критичної цифрової інфраструктури, захист персональних даних та відповідальне використання штучного інтелекту. Поєднання цих компонентів створює основу для безпечного переходу від фрагментарної цифровізації до системної цифрової трансформації державного управління.

Література

1. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX. URL: <https://zakon.rada.gov.ua/laws/show/1907-20> (дата звернення: 15.08.2026).

2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 15.08.2026).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 15.08.2026).

4. Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». URL: <https://trembita.gov.ua> (дата звернення: 15.08.2026).

5. Офіційний портал «Дія». URL: <https://diia.gov.ua> (дата звернення: 15.08.2026).

6. Міністерство цифрової трансформації України. Dіia.AI. URL: <https://diia.gov.ua/diia-ai> (дата звернення: 15.08.2026).

7. OECD. Governing with Artificial Intelligence: The State of the Play and Way Forward in Core Government Functions. Paris: OECD Publishing, 2025. DOI: <https://doi.org/10.1787/795de142-en>.

8. OECD. The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government. Paris: OECD Publishing, 2020. DOI: <https://doi.org/10.1787/f64fed2a-en>.

УДК 004.056.55

Басов В.Є., Басов С.В.

АНАЛІЗ КРИПТОГРАФІЧНИХ ВЛАСТИВОСТЕЙ ПОВНОЇ МНОЖИНИ БІЄКТИВНИХ ТРІЙКОВИХ S-БЛОКІВ РОЗМІРНОСТІ 2×2.

Державний університет інтелектуальних технологій і зв’язку.
v.y_basov@suitt.edu.ua, s.v_basov@suitt.edu.ua

Анотація. У роботі виконано повний перебір усіх 362 880 бієктивних трійкових S-блоків розмірності 2×2. Досліджено диференціальну рівномірність, лінійні властивості на основі перетворення Віленкіна—Хрестенсона, а також два варіанти суворого лавинного критерію (SACm та SACv). Встановлено, що жоден блок не задовольняє масковий SAC, тоді як SACv виконують 1552 блоки, але лише 288 із них одночасно мають найкращі диференціальні та лінійні характеристики. Показано, що критерій SACv не є достатньою умовою для забезпечення високої криптостійкості.

Ключові слова: S-блок, трійчна криптографія, диференціальний криптоаналіз, лінійний криптоаналіз, суворий лавинний критерій.

Вступ. Нелінійні підстановки (S-блоки) є ключовими компонентами сучасних симетричних криптографічних алгоритмів. Вони забезпечують нелінійність шифру, стійкість до диференційного та лінійного криптоаналізу, а також суттєво впливають на загальну криптографічну стійкість алгоритму.

Упродовж останніх років зростає інтерес до багатозначної криптографії, зокрема до використання S-блоків над алфавітами потужністю, відмінною від 2. Такі перетворення можуть знайти застосування в спеціалізованих криптографічних примітивах, перспективних багатозначних обчислювальних системах та під час побудови криптографічних алгоритмів для нетрадиційних обчислювальних платформ. Водночас криптографічні властивості багатозначних S-блоків вивчені недостатньо порівняно з двійковими аналогами.

Повний перебір усіх бієктивних трійкових S-блоків невеликої розмірності дає змогу отримати вичерпні статистичні дані про їхні криптографічні характеристики, дослідити взаємозв'язок між окремими критеріями та оцінити можливість одночасного виконання кількох вимог до криптографічно стійких підстановок.

У роботі проведено повний аналіз множини бієктивних трійкових S-блоків розмірності 2×2. Для кожного S-блоку визначено показники диференціальної рівномірності [1], виконано лінійний аналіз [2] із використанням перетворення Віленкіна—Хрестенсона, а також перевірено виконання суворого лавинного критерію, запропонованого Webster A. F., Tavares S. E. у роботі [3]. Для двійкових S-блоків цей критерій вимагає, щоб зміна одного вхідного біта змінювала кожен вихідний біт із імовірністю 0,5. Пізніше цей критерій узагальнили Yuan Li та T. W. Cusick у роботі [4] (масковий критерій) та Sokolov A. V., Zhdanov O. N. у роботі [5] (критерій за значенням).

Дослідження. Для аналізу обрано множину бієктивних трійкових S-блоків розмірності 2×2. Це зумовлено такими чинниками: множина є скінченною та допускає повний перебір; кількість можливих S-блоків дорівнює $9! = 362\,880$, що робить експеримент практично здійсненим; бієктивність забезпечує оборотність S-блоку — необхідну властивість для симетричних шифрів; повний перебір дає змогу отримати точні статистичні результати, а не оцінки, властиві випадковій вибірці. Відомостей про виконання такого перебору іншими дослідниками у відкритих джерелах не виявлено. Тому ця множина є зручною моделлю для експериментального дослідження криптографічних властивостей багатозначних S-блоків.

Критерій відбору блоків, стійких до диференційного криптоаналізу, полягає в такому. Для кожного S-блоку будували таблицю розподілу різниць (DDT):

$$DDT[\Delta x, \Delta y] = |\{x \in GF(q)^n : S(x + \Delta x) - S(x) = \Delta y\}|$$

де q – потужність алфавіту, n – кількість вхідних символів, $S(\cdot)$ – S-блок, x – вхідний вектор, $\square x$ – вхідна різниця, $\square y$ – вихідна різниця, всі операції виконуються за модулем q . Основною характеристикою для аналізу є диференційна рівномірність:

$$DU = \max_{\Delta x \neq 0, \Delta y} DDT[\Delta x, \Delta y]$$

Максимальна диференціальна ймовірність визначається як $MDP = DU/q^n$. Оскільки менші значення DU та MDP відповідають більшій стійкості до диференціального криптоаналізу, найкращими вважалися S-блоки з **мінімальною диференціальною рівномірністю**.

Відбір блоків стійких до лінійного криптоаналізу виконували так. Для кожного S-блоку будувалася таблиця лінійних апроксимацій (LAT)

$$LAT[a, b, k] = |\{x \in GF(q)^n : \langle a, x \rangle - \langle b, S(x) \rangle = k\}|$$

де $k \in GF(q)$, a – вхідна маска, b – вихідна маска, $\square, \cdot, \square$ – скалярний добуток над $GF(q)$, x – вхідний вектор, $S(x)$ – вихідний вектор S-блоку. Якщо для двійкового випадку використовують спектр Волша. Для трійкового випадку використовують спектр Віленкіна—Хрестенсона. Максимальний коефіцієнт спектру визначався як

$$V_{max} = \max_{a \neq 0, b \neq 0} |VH(a, b)|$$

Ймовірність відповідної лінійної апроксимації обчислювалася як $P = N_{max}/q^n$, де N_{max} – кількість входів, для яких виконується відповідне лінійне співвідношення.

Найкращими вважалися S-блоки, для яких максимальна ймовірність статистичного аналога була мінімально можливою, тобто максимальне відхилення від випадкової поведінки було найменшим. Для кожного блоку побудована повна множина ефективних лінійних статистичних аналогів

Відбір за суворим лавинним критерієм (SACm) (версію за Li назвемо - масковий критерій). Перевірявся узагальнений суворий лавинний критерій, сформульований через **усі ненульові вихідні маски**. Для кожної одиничної вхідної різниці a та кожної ненульової вихідної маски b визначалася ймовірність зміни значення скалярного добутку $P(a, b)$. Для алфавіту потужності q теоретично очікувана ймовірність дорівнює $P = (q - 1)/q$. S-блок вважався таким, що задовольняє SAC за масковим критерієм Li , **лише тоді, коли ця рівність виконувалася для всіх припустимих пар (a, b)** . Стверджується, що якщо S-box відповідає цьому критерію – то для нього не існують ефективні лінійні статистичні аналогів.

Критерій відбору SACv за значенням (версія Sokolov). Цей критерій досліджує **не маски, а розподіл самих вихідних приростів**. Для кожної одиничної вхідної різниці a обчислювався розподіл

$$\Delta y = S(x + a) - S(x)$$

Для виконання критерію кожне можливе значення вихідної різниці повинно зустрічатися однаково кількість разів.

$$N_i = \frac{q^n}{q}, i = 0, \dots, q - 1.$$

Тобто розподіл похідних має бути рівномірним. S-блок вважався таким, що задовольняє SAC за Соколовим, якщо для всіх одиничних вхідних різниць отримувався рівномірний розподіл вихідних пристовів.

Проаналізовано всі 362 880 можливих блоків. Отримано такі результати (табл. 1).

Таблиця 1. – Розподіл блоків за криптографічними властивостями			
Критерій	Найкраще знайдене значення	Кількість S-блоків	Частка
Differential Uniformity	3	94608	0.260714
Maximum Differential Probability	0.333333 = 1/3	94608	0.260714
Maximum Linear Probability	0.777778 = 7/9	39168	0.107936
Мінімальна нелінійність	0	432	0.000119
Масковий SAC - SACm	–	жодного	0
SAC за значенням – SACv	–	1552	0.000428
Best DDT + best LAT	MDP=1/3, MLP=7/9	18432	0.050794
Best DDT + best LAT + SACv	MDP=1/3, MLP=7/9	288	0.000794

Результати аналізу показують, що суворий лавинний критерій за значенням (SACv) виявився недостатньо суворим. По-перше, він не гарантує, що синтезований за ним блок буде абсолютно стійким до лінійного криптоаналізу: таких блоків серед досліджених не знайдено взагалі. По-друге, далеко не всі блоки, що задовольняють SACv, належать до множини найкращих, принаймні серед досліджених трійкових S-блоків розмірності 2×2.

$$\frac{288}{1552} \approx 0,1856 \approx 18.6\%.$$

Хоча критерій SACv виконують 1552 S-блоки (0,428 %), лише 288 із них (18,6 %) одночасно мають найкращі показники диференціальної та лінійної криптостійкості. Отже, виконання критерію SACv саме по собі не є достатньою умовою високої криптографічної якості S-блоку.

Висновки. Уперше виконано повний перебір усіх 362 880 бієктивних трійкових S-блоків розмірності 2×2. Результати показали, що: найстійкішими до диференційного криптоаналізу виявилися 94 608 блоків із максимальною диференціальною ймовірністю MDP = 1/3; найстійкішими до лінійного криптоаналізу виявилися 39 168 блоків із мінімальною максимальною лінійною ймовірністю MLP = 7/9, що вказує на високу ефективність таких лінійних статистичних аналогів і, відповідно, на низьку стійкість найкращих зі знайдених блоків до цієї атаки; кількість блоків, які одночасно демонструють найкращу стійкість до лінійного та диференціального аналізу, становить 18 432; жоден із блоків не задовольняє узагальнений масковий суворий лавинний критерій (SACm); 1552 блоки задовольняють критерій SACv, однак лише 288 із них одночасно мають найкращі показники диференціальної та лінійної криптостійкості. Це свідчить про те, що критерій SAC за значеннями є значно слабшим за масковий SAC і не забезпечує автоматично високої стійкості до лінійного криптоаналізу.

Література

1. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. New York : Springer, 1993. 250 p. ISBN 0-387-97930-1.

2. Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology – EUROCRYPT'93 : Proceedings of a Workshop, Lofthus, Norway, May 23–27, 1993 / ed. T. Helleseth. Berlin : Springer, 1994. Vol. 765 of Lecture Notes in Computer Science. P. 386–397. DOI: 10.1007/3-540-48285-7_33.

3. Webster A. F., Tavares S. E. On the Design of S-Boxes // Advances in Cryptology – CRYPTO'85 : Proceedings of a Conference, Santa Barbara, Calif., Aug. 18–22, 1985 / ed. H. C. Williams. Berlin : Springer, 1986. Vol. 218 of Lecture Notes in Computer Science. P. 523–534. DOI: 10.1007/3-540-39799-X_37.

4. Li Y., Cusick T. W. Strict Avalanche Criterion over Finite Fields // Journal of Mathematical Cryptology. 2007. Vol. 1, No. 1. P. 1–12. DOI: 10.1515/JMC.2007.001.

5. Sokolov A. V., Zhdanov O. N. Avalanche Characteristics of Cryptographic Functions of Ternary Logic // Radio Electronics, Computer Science, Control. 2019. No. 4. P. 82–95. DOI: 10.15588/1607-3274-2019-4-8.

МЕТОД АДАПТИВНОГО ФОРМУВАННЯ СЕМАНТИЧНОГО ВІДЕОПОВІДОМЛЕННЯ
З УРАХУВАННЯМ СТАНУ БЕЗДРОТОВОГО КАНАЛУ

Державний університет інтелектуальних технологій і зв'язку, м. Одеса
it.ddo.od@gmail.com

Анотація. Запропоновано метод адаптивного формування семантичного відеоповідомлення залежно від поточного стану бездротового каналу. Визначено архітектуру semantic video communication та розглянуто гібридне представлення semantic metadata + key frame / ROI / evidence fragment. Базовим імітаційним експериментом показано, що за однакового бюджету надлишковості нерівнозначний захист підвищує ймовірність відновлення метаданих з 87,43 % до 98,67 %, а доступність візуальної перевірки - з 79,48 % до 90,88 %. На цій основі запропоновано адаптивно змінювати не лише рівень FEC, а й склад повідомлення відповідно до доступної швидкості, пакетних втрат і максимально допустимої затримки. Числовий експеримент демонструє керовану семантичну деградацію $M+K+C \rightarrow M+K \rightarrow M$ при погіршенні стану каналу.

Ключові слова: семантична комунікація, semantic video communication, адаптивне передавання, стан каналу, семантичні метадані, ключовий кадр, ROI, пакетизація, FEC, бездротовий канал.

Вступ до проблеми та архітектура semantic video communication

Зростання роздільної здатності камер, кількості відеосенсорів та частки машинної обробки відео створює ситуацію, у якій передавання повного піксельного потоку не завжди є необхідним. Для систем відеоспостереження, транспортного моніторингу, мобільної робототехніки та інших task-oriented сценаріїв приймачеві часто потрібний не повний відеоряд, а інформація, достатня для виконання конкретної задачі: виявити подію, визначити клас об'єкта, оцінити його положення або траєкторію, підтвердити подію візуально чи прийняти керувальне рішення. Сучасні огляди semantic communication для візуальних даних саме цю зміну мети - від точного відновлення бітів до передавання значущого для задачі змісту - визначають як базову ознаку семантичної комунікації [1].

Узагальнена архітектура semantic video communication може бути подана трактом Video source → semantic encoder → semantic representation / packetization → physical or network channel → semantic decoder → machine/user task. Семантичний кодер виконує аналіз відеопослідовності та формує компактне представлення; блок packetization перетворює його на передавані одиниці, додає службові поля, пріоритети та завадостійкий захист; канал вносить затримку, стирання або спотворення; семантичний декодер відновлює необхідне представлення або відеосвідчення; кінцевий блок оцінює не обов'язково PSNR/SSIM, а успішність цільової задачі. Такий функціональний поділ узгоджується як із дослідницькими системами [2-6], так і з поточним напрямом стандартизації ITU-T для AI-based semantic communication у відеовикликах, де окремо виділяються semantic extraction, semantic data transmission, semantic reconstruction та semantic QoE evaluation [8].

Ключовою особливістю цієї архітектури є відсутність єдиного обов'язкового формату семантичного представлення. Залежно від задачі між semantic encoder і каналом можуть передаватися текстовий або структурований опис події; класи та параметри об'єктів; bounding boxes, координати й траєкторії; embeddings або latent features; scene graph чи object-attribute-relation граф; ключові кадри; ROI-фрагменти; короткі відеофрагменти або комбінація цих типів. Наприклад, VISTA передає семантичні ознаки разом із semantic location graphs, що описують об'єкти та їхні просторові відношення [2]; OAR-VSC використовує послідовності object-attribute-relation як інтерпретоване низькобітрейтне представлення та пов'язує його з розподілом ресурсів JSCC [5]. Інший напрям використовує латентні ознаки та генеративне відновлення відео [6, 9].

Основні форми семантичного представлення

Представлення	Приклад вмісту	Перевага для каналу	Типова роль
Структуровані метадані	event type, ID, time, coordinates	дуже малий обсяг	машинне рішення
Object-centric дані	class, bbox, trajectory, attributes	передається лише стан об'єктів	detection / tracking
Latent / embeddings	feature vectors, latent tensors	компактність та JSCC	reconstruction / inference
Scene graph / OAR	object-attribute-relation, spatial links	інтерпретовані зв'язки	reasoning / reconstruction
Key frame / ROI	ключовий кадр, область інтересу	візуальний доказ без повного потоку	human verification
Short evidence fragment	короткий фрагмент події	локалізація трафіку в часі	context / audit
Hybrid	metadata + key frame / ROI / fragment	гнучке співвідношення зміст/обсяг	machine + human task

Таблиця 1 - Основні форми семантичного представлення відео

Для даної роботи найбільш важливим є гібридне представлення semantic metadata + key frame / ROI / evidence fragment. Його принципова перевага полягає в розділенні двох функцій. Компактні метадані забезпечують машинно-читане повідомлення про факт і параметри події, тоді як візуальний компонент дозволяє оператору або подальшому алгоритму перевірити правильність семантичного висновку. Гібридний підхід уже має близькі аналоги: у роботі Samarathunga et al. семантичне міжкадрове кодування доповнюється VVC-кодуванням ключових кадрів і residual data [4], а в goal-oriented генеративній системі Li et al. виділяються ключові кадри та semantic information для їх подальшої реконструкції і генерації відео [6]. Проте для мережевого тракту лишається окреме питання: які саме компоненти такого гібридного повідомлення слід передавати, коли доступний каналний ресурс змінюється швидше, ніж зміст самої події.

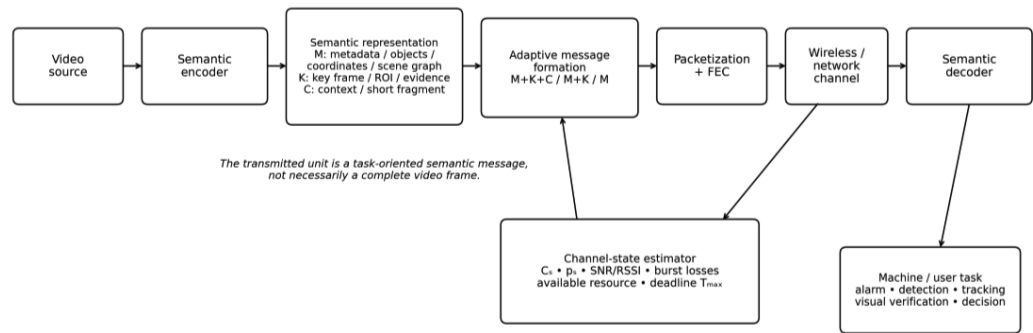


Рис. 1. Структура адаптивного формування семантичного відеоповідомлення

На рис. 1 запропоновану архітектуру доповнено контуром оцінювання стану каналу. Це принципово відрізняє досліджувану задачу від статичного семантичного кодування: channel-state estimator формує оцінки доступної швидкості, імовірності пакетних втрат, SNR/RSSI, серійності втрат і доступного deadline, після чого блок adaptive message formation визначає не лише параметри FEC, а й сам склад передаваного семантичного повідомлення.

Базове обґрунтування: функціональна нерівнозначність компонентів повідомлення

Перш ніж переходити до адаптації складу повідомлення залежно від стану каналу, необхідно перевірити, чи однаково впливає втрата різних компонентів гібридного семантичного повідомлення на виконання цільової задачі. Розглянуто три типи даних: М - семантичні метадані; К - ключовий кадр; С - додатковий візуальний контекст. Для модельного повідомлення прийнято k_M=4, k_K=30 та k_C=60 інформаційних пакетів. Для двох захищених режимів використано однаковий бюджет надлишковості R=24 пакети.

За рівномірного розподілу надлишковість становить (r_M,r_K,r_C)=(1,8,15), тоді як за нерівнозначного захисту вона перерозподіляється як (3,9,12). Отже, загальний каналний ресурс не збільшується: частина надлишковості переноситься від менш критичного контексту до метаданих і ключового кадру.

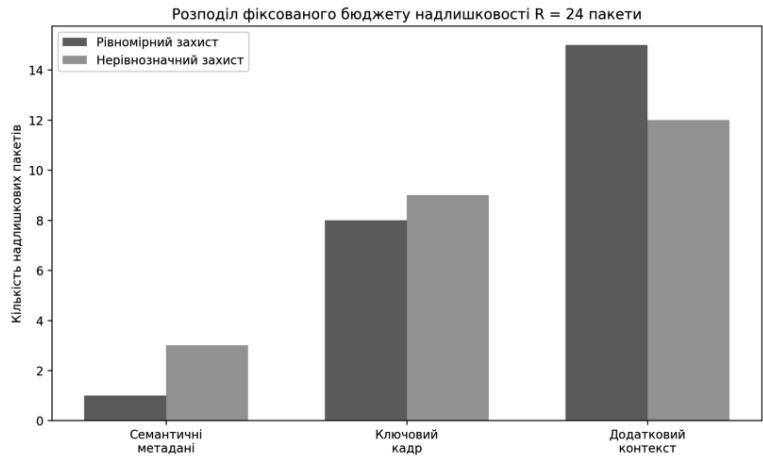


Рис. 2. Розподіл фіксованого бюджету надлишковості між компонентами семантичного повідомлення

Для перевірки ефекту такого перерозподілу виконано 250 000 реалізацій передавання для кожного режиму. Порівнювалися рівномірний захист, нерівнозначний захист та передавання без додаткового захисту. Критеріями були імовірність відновлення окремих компонентів і практична придатність повідомлення для машинної обробки та візуальної перевірки.

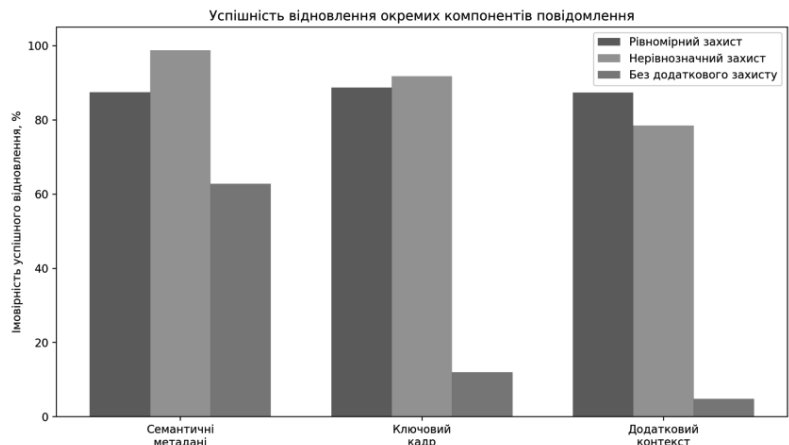


Рис. 3. Успішність відновлення окремих компонентів семантичного повідомлення

Нерівнозначний захист підвищує імовірність відновлення семантичних метаданих з 87,43 % до 98,67 %, а ключового кадру - з 88,64 % до 91,72 %. Це підтверджує, що однаковий рівень захисту не є оптимальним, коли різні компоненти мають різні функціональні наслідки втрати.

Для semantic communication принциповим є не лише факт відновлення пакетів, а можливість виконати кінцеву задачу. За однакового бюджету надлишковості частка повідомлень, придатних для машинної обробки, зростає до 98,67 %, а доступність візуальної перевірки - з 79,48 % до 90,88 %. Інтегральний критерій семантичних втрат J зменшується з 0,1222 до 0,0544. Таким чином, базовий експеримент підтверджує доцільність пріоритизації компонентів і створює підставу для основної задачі роботи: адаптивно змінювати склад повідомлення та його захист при зміні стану каналу.

Режим	r_M/r_K/r_C	Пакетів	M, %	K, %	M+K, %	Yci, %	J
Рівномірний	1/8/15	118	87,43	88,64	79,48	74,47	0,1222
Нерівнозначний	3/9/12	118	98,67	91,72	90,88	76,00	0,0544
Без дод. захисту	0/0/0	94	62,74	11,97	10,24	2,51	0,5828

Таблиця 2 - Результати базового експерименту з нерівнозначним захистом

Постановка задачі

У традиційній системі відеозв'язку погіршення стану каналу зазвичай компенсується зміною бітрейту, параметрів модуляції і кодування, повторними передаваннями або погіршенням якості відновленого відеозображення. Для semantic video communication існує додатковий ступінь свободи: змінювати не лише кількість бітів на одиницю часу, а й склад інформації, що передається. Adaptive Bitrate Video Semantic Communication уже демонструє доцільність зміни семантичного бітрейту відповідно до мережевих умов [3]. У цій роботі адаптація переноситься на рівень структури гібридного повідомлення.

Розглядається подієве повідомлення, що може містити: М - семантичні метадані; К - ключовий кадр або ROI/evidence fragment для візуальної перевірки; С - додатковий контекст. За сприятливого каналу доцільно передавати М+К+С. При зменшенні доступної пропускну здатності або зростанні пакетних втрат повний набір може не вкладатися у допустиму затримку; тоді система переходить до М+К. За критичного стану каналу пріоритетом стає коротке М-повідомлення.

При цьому семантична важливість факту події не змінюється від SNR або packet loss. Змінюється ефективна корисність передавання конкретного компонента: дані, які неможливо доставити до завершення deadline, перестають бути корисними для поточного рішення. Саме тому стан каналу повинен впливати на оптимальний склад повідомлення.

Метою дослідження є розроблення методу адаптивного вибору складу гібридного семантичного відеоповідомлення та параметрів його завадостійкого захисту залежно від поточного стану бездротового каналу за обмеження на максимально допустиму затримку.

Модель семантичного повідомлення

Семантичне повідомлення представимо множиною компонентів:

$$D = \{M, K, C\}$$

де М - семантичні метадані; К - ключовий кадр, ROI або інший візуальний доказ; С - додатковий візуальний контекст. Для демонстраційного експерименту кількість інформаційних пакетів компонентів прийнято рівною:

$$k_M = 4, k_K = 30, k_C = 60.$$

Для кожного компонента вводиться бінарна змінна передавання:

$$x_i \in \{0,1\}.$$

Функціональна залежність компонентів задається умовою:

$$x_C \leq x_K \leq x_M.$$

Компонент і може містити r_i надлишкових пакетів FEC. Загальна кількість переданих пакетів:

$$N = \sum_i x_i (k_i + r_i).$$

Обмеження, визначене станом каналу

Нехай C_s - оцінена корисна швидкість передавання в поточному стані каналу s , $T_{\max}$ - максимально допустимий час доставки повідомлення, L_p - довжина одного пакета в бітах. Максимальна кількість пакетів, яку можна передати до завершення допустимого інтервалу:

$$N_{\max}(s) = \lfloor \frac{C_s T_{\max}}{L_p} \rfloor.$$
$$N \leq N_{\max}(s).$$

Імовірність відновлення та критерій функціональної корисності

Для первинного аналізу використано модель пакетного стирання з поточною оцінкою імовірності втрати p_s . Якщо компонент містить k_i інформаційних і r_i надлишкових пакетів та MDS-код дозволяє відновлення за втрати не більше r_i пакетів, імовірність відновлення компонента визначається:

$$P_i = \sum_{l=0}^{r_i} C_{k_i+r_i}^l p_s^l (1 - p_s)^{k_i+r_i-l}.$$

Для демонстраційної моделі функціональні ваги прийнято рівними $w_M=0,45$, $w_K=0,35$, $w_C=0,20$. Корисність повідомлення визначається з урахуванням залежності візуальних компонентів від наявності метаданих:

$$U = w_M P_M + w_K P_M P_K + w_C P_M P_K P_C.$$

Оптимізаційна задача має вигляд:

$$\{x_i, r_i\} = \operatorname{argmax} U, \text{ за умов } N \leq N_{\max}(s), x_C \leq x_K \leq x_M.$$

Алгоритм адаптивного формування повідомлення

- Оцінюється поточний стан бездротового каналу.
- Визначаються C_s , p_s та доступний пакетний бюджет $N_{\max}(s)$.
- Формуються допустимі конфігурації $M+K+C$, $M+K$ і M .
- Для кожної конфігурації визначаються допустимі значення r_i .
- Обчислюються P_i та функція U .
- Обирається конфігурація з максимальним значенням U .
- Виконується пакетизація, FEC-кодування і передавання.

Числовий експеримент

Для перевірки принципу роботи методу використано пакет довжиною $L_p=1000$ байт та максимальну допустиму затримку $T_{\max}=250$ мс. Розглянуто три характерні стани каналу.

Стан каналу	C_s	p_s	$N_{\max}$
Сприятливий	4 Мбіт/с	0,03	125
Нестабільний	2 Мбіт/с	0,12	62
Критичний	0,5 Мбіт/с	0,30	15

Таблиця 3 - Параметри станів бездротового каналу

Оптимізацію виконано повним перебором допустимих конфігурацій та цілочисельних значень надлишковості. Для сприятливого стану оптимальним є $M+K+C$ з розподілом $(r_M, r_K, r_C)=(6,11,14)$ і загальним обсягом 125 пакетів; $U \approx 1,000$. Для нестабільного стану бюджет скорочується до 62 пакетів, і оптимальним стає $M+K$ з $(r_M, r_K)=(9,19)$; $P_M=0,9999999$, $P_K=0,9999997$, $U \approx 0,800$. За критичного стану оптимізатор переходить до M : чотири інформаційні пакети доповнюються 11 надлишковими, $P_M=0,99991$, $U \approx 0,450$.

Стан	Склад	Надлишковість	Пакетів	U
Сприятливий	$M+K+C$	6 / 11 / 14	125	$\approx 1,000$
Нестабільний	$M+K$	9 / 19	62	$\approx 0,800$
Критичний	M	11	15	$\approx 0,450$

Таблиця 4 - Результат адаптивного вибору режиму

Для порівняння, передавання початкового повідомлення без додаткового захисту потребує 94 пакетів. Час передавання становить 188 мс за 4 Мбіт/с, 376 мс за 2 Мбіт/с та 1,504 с за 0,5 Мбіт/с. Отже, вже у другому стані фіксоване повідомлення порушує $T_{\max}=250$ мс, тоді як адаптивний метод зберігає своєчасну доставку функціонально найважливіших компонентів.

Результат демонструє керовану семантичну деградацію:

$$M + K + C \rightarrow M + K \rightarrow M.$$

Наукова новизна та відмінність від відомих підходів

Адаптація semantic video communication до мережевих умов не є новою сама по собі. ABRVSC змінює бітрейт семантичної інформації відповідно до стану мережі [3]; OAR-VSC використовує семантичне представлення для пріоритетного розподілу комунікаційних ресурсів [5]; сучасні роботи з UEP розподіляють

різний рівень каналного захисту між семантично нерівнозначними бітами [7]. Тому наукова новизна даної постановки не формулюється як «урахування стану каналу» в загальному вигляді.

Запропонована відмінність полягає у спільному адаптивному виборі 1) складу різнотипного гібридного повідомлення metadata + visual evidence + context та 2) рівня FEC для компонентів за єдиного обмеження на каналний ресурс і deadline. Оптимізатор має право не лише зменшити бітрейт, а повністю виключити менш корисний у поточному стані каналу компонент, реалізуючи структурний перехід $M+K+C \rightarrow M+K \rightarrow M$. Критерієм є очікувана функціональна корисність своєчасно доставленої інформації, а не лише BER, PER або якість піксельного відновлення.

Обмеження

Наведений експеримент використовує спрощену модель пакетного стирання зі сталою p_s протягом одного повідомлення та ідеалізовану MDS-властивість FEC. У реальному бездротовому каналі втрати можуть бути корельованими і формувати серії, а оцінка стану каналу може містити похибку та затримку. Тому наступним етапом має бути перевірка на моделі Гілберта-Елліотта або багатостановій марковській моделі, а також на реальних трасах packet loss. Функціональні ваги w_M, w_K, w_C у цьому експерименті мають демонстраційний характер і для конкретної системи повинні визначатися відповідно до вартості втрати події, вимог до візуальної верифікації та допустимої затримки.

Висновки

- Визначено узагальнену архітектуру semantic video communication як тракт від відеоджерела через semantic encoder, формування семантичного представлення, packetization і фізичний/мережевий канал до semantic decoder та кінцевої machine/user task.
- Показано, що семантичне представлення може бути структурованим, latent/feature-based, graph-based, візуальним або гібридним; для задачі адаптивного передавання особливий інтерес має metadata + key frame / ROI / evidence fragment.
- Запропоновано метод, у якому стан каналу впливає не на семантичний зміст події, а на оптимальний склад і ступінь захисту повідомлення.
- Запропоновано критерій функціональної корисності, який враховує машинну придатність метаданих, доступність візуальної перевірки та додаткового контексту.
- Для модельного повідомлення з 94 інформаційних пакетів показано перехід $M+K+C \rightarrow M+K \rightarrow M$ при зменшенні доступної швидкості $4 \rightarrow 2 \rightarrow 0,5$ Мбіт/с.
- За $T_{\max}=250$ мс адаптивний метод зберігає своєчасну доставку критичної інформації в умовах, коли фіксоване повідомлення потребувало б 376 мс та 1,504 с.
- Базовий експеримент з нерівнозначним захистом підтвердив, що різні компоненти гібридного семантичного повідомлення мають різну функціональну цінність; це обґрунтовує подальший адаптивний вибір режиму $M+K+C$, $M+K$ або M залежно від стану каналу.

Література

- Cheng R., Sun Y., Taha A., Liu X., Flynn D., Imran M. A. A Survey on Semantic Communication for Vision: Categories, Frameworks, Enabling Techniques, and Applications. IEEE Transactions on Network Science and Engineering. 2026. Vol. 13. P. 8080-8103. DOI: 10.1109/TNSE.2026.3671446.
- Liang C., Deng X., Sun Y., Cheng R., Xia L., Niyato D., Imran M. A. VISTA: Video Transmission Over a Semantic Communication Approach. ICC Workshops 2023. DOI: 10.1109/ICCWorkshops57953.2023.10283754.
- Gong W., Tong H., Wang S., Yang Z., He X., Yin C. Adaptive Bitrate Video Semantic Communication over Wireless Networks. 2023 International Conference on Wireless Communications and Signal Processing (WCSP). 2023. P. 122-127. DOI: 10.1109/WCSP58612.2023.10405124.
- Samarathunga P., Ganearachchi Y., Fernando T., Jayasingam A., Alahapperuma I., Fernando A. A Semantic Communication and VVC Based Hybrid Video Coding System. IEEE Access. 2024. Vol. 12. P. 79202-79224. DOI: 10.1109/ACCESS.2024.3399174.
- Du Q., Duan Y., Yang Q., Tao X., Debbah M. Object-Attribute-Relation Representation-Based Video Semantic Communication. IEEE Journal on Selected Areas in Communications. 2025. Vol. 43, No. 7. P. 2446-2461. DOI: 10.1109/JSAC.2025.3559115.
- Li N., Deng Y., Niyato D. Goal-Oriented Semantic Communication for Wireless Video Transmission via Generative AI. IEEE Transactions on Wireless Communications. 2026. Vol. 25. P. 10841-10854. DOI: 10.1109/TWC.2026.3654401.
- Kim S., Oh Y., Kim Y., Lee N., Jeon Y.-S. Channel Coding for Unequal Error Protection in Digital Semantic Communication. arXiv:2508.03381. 2025.
- ITU-T SG21 Q5/21. F.AI-SCVC: Requirements and framework of AI-based semantic communication for video calls. Work item, 2025-2028, status: Under study.
- Lokumarambage M., Sivalingam T., Dong F., Rajatheva N., Fernando A. Latent Prediction-Based Generative Semantic Communication for Video Transmission in Wireless Networks. IEEE Open Journal of the Communications Society. 2026. Vol. 7. P. 3974-3986. DOI: 10.1109/OJCOMS.2026.3684230.

МЕТОДИ ТА МОДЕЛІ ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ
ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ
З УРАХУВАННЯМ СТУПЕНЯ ПЕРЕКРИТТЯ ЗАГРОЗ

Державний університет інформаційно-комунікаційних технологій
dentruhan11@gmail.com

Анотація. Запропоновано метод оцінювання захищеності системи захисту інформації корпоративної мережі, який враховує не лише наявність засобів, а й ступінь перекриття кожної актуальної загрози. Модель використовує матрицю «загроза - захід», ваги критичності, підтверджену ефективність і достовірність доказів. Сукупне перекриття визначається через залишкову експозицію з корекцією залежних заходів. Метод дає локальні оцінки за загрозами, інтегральний індекс захищеності та пріоритетний перелік прогалін для вдосконалення корпоративного захисту.

Ключові слова: оцінка захищеності, корпоративна мережа, загроза, перекриття загроз, система захисту інформації, залишковий ризик.

Оцінювання систем захисту інформації корпоративних мереж часто зводиться до перевірки наявності окремих засобів або до усереднення часткових показників. Такий підхід не показує, які саме загрози залишаються недостатньо контрольованими. Кілька налаштованих засобів можуть перекривати одну й ту саму техніку атаки, тоді як інший сценарій не матиме дієвого запобігання, виявлення чи відновлення. Каталоги контролів описують функціональні та гарантійні властивості заходів [2], а процедури оцінювання вимагають підтверджувати їх виконання доказами [3]. Проте для прийняття рішення потрібна модель, що пов'язує ці докази з конкретними загрозами та залишковим ризиком.

Мета роботи. Розробити метод і модель оцінки захищеності корпоративної мережі з урахуванням ступеня перекриття загроз чинними організаційними та технічними заходами. Вхідними даними є перелік активів і сценаріїв загроз, ваги їх критичності, склад засобів захисту, результати перевірок та залежності між заходами. Виходом є вектор локальних оцінок перекриття, інтегральний індекс, залишковий ризик і ранжований перелік прогалін. Такий результат можна використати для порівняння поточного й цільового профілів захисту та формування плану вдосконалення [4].

Модель даних. Нехай множина актуальних загроз утворює рядки матриці, а впроваджені заходи захисту - її стовпці. Елемент матриці набуває значення від 0 до 1 і характеризує частку сценарію загрози, яку здатний перекрити відповідний захід. Нуль означає відсутність релевантного впливу, одиниця - повне перекриття за визначених умов. Загрози формуються для конкретних активів, меж мережі та способів порушення конфіденційності, цілісності або доступності. Для деталізації сценаріїв доцільно використовувати техніки атак і пов'язані з ними класи протидій [5].

Склад часткової оцінки. Ступінь прямого перекриття доповнюється коефіцієнтом фактичної ефективності засобу та коефіцієнтом довіри до доказу. Ефективність визначається за конфігурацією, результатами тестів, телеметрією і статистикою інцидентів. Довіра є вищою для відтворюваного технічного тесту або незалежного аудиту й нижчою для неперевіреної декларації. Окремо оцінюються чотири фази: запобігання, виявлення, реагування та відновлення. Їх ваги залежать від властивості активу: для персональних даних домінує запобігання витоку, а для критичного сервісу - стійкість і відновлення.

Агрегування перекриття. Для кожної загрози часткові внески об'єднуються через доповнення до залишкової експозиції: кожний незалежний захід зменшує ту частину сценарію, що залишилася після попередніх заходів. Щоб не завищувати результат, засоби зі спільною точкою відмови або однаковим джерелом телеметрії об'єднуються в одну залежну групу; всередині неї враховується найсильніший підтверджений внесок, а не проста сума. Додатковий штраф застосовується за невідомий стан, застарілий тест, неповне розгортання чи неможливість перевірити реакцію на відмову.

Таблиця 1 - Ілюстративна матриця прямого перекриття загроз

Загроза	M1	M2	M3	M4
T1 Компрометація облікових даних	0,85	0,15	0,35	0,45
T2 Шкідливе ПЗ та шифрування	0,20	0,80	0,45	0,70
T3 Експлуатація вразливостей	0,15	0,65	0,55	0,45
T4 Несанкціонований витік даних	0,55	0,30	0,65	0,55
T5 Порушення мережевої доступності	0,10	0,25	0,75	0,60

Примітка. Значення наведено для демонстрації розрахунку; вони не є результатами аудиту реальної мережі.

Інтерпретація прикладу. Матриця в табл. 1 є ілюстративною: M1 позначає керування ідентичностями та багатофакторну автентифікацію, M2 - захист кінцевих точок, M3 - сегментацію й фільтрацію, M4 - резервування та моніторинг. Для розрахунку враховано коефіцієнти ефективності та довіри до доказів. Отримані значення на рис. 1 не є результатами випробування реальної мережі, а демонструють роботу моделі. За цільового рівня 0,80 недостатньо перекритими виявляються T3 та T5; тому високий інтегральний показник не повинен приховувати локальні прогалини.

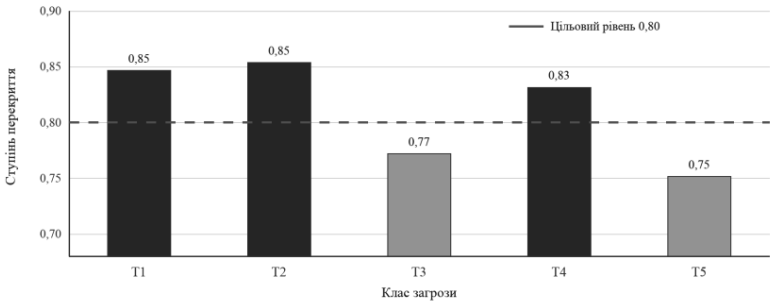


Рисунок 1 - Ілюстративні ступені перекриття загроз після врахування ефективності й довіри

Інтегральна оцінка. Загальний індекс визначається як зважене середнє локальних ступенів перекриття. Вага загрози поєднує ймовірність реалізації, вплив на актив і його критичність. Для наведеного прикладу за ваг 0,25; 0,25; 0,20; 0,20 та 0,10 індекс дорівнює 0,821. Проте рішення про достатню захищеність приймається лише за одночасного виконання двох умов: загальний індекс не нижчий від цільового, а перекриття кожної критичної загрози перевищує локальний мінімум. Залишковий ризик розраховується за неперекритою частиною кожної загрози, тому його можна зіставити з толерантністю власника системи [1, 6].

Метод оцінювання. Процедура містить сім етапів: визначення меж корпоративної мережі; інвентаризацію активів; побудову актуальних сценаріїв загроз; формування матриці перекриття; збирання доказів ефективності; агрегування з урахуванням залежностей; аналіз чутливості та формування рекомендацій. Для кожної низької оцінки фіксуються причина, власник ризику, потрібний доказ, варіант додаткового заходу, вартість і строк. Поточна матриця порівнюється з цільовою, після чого план робіт упорядковується за зменшенням залишкового ризику на одиницю витрат.

Динамічне оновлення. Оцінка має строк актуальності. Після зміни топології, появи нової техніки атаки, оновлення засобу або інциденту відповідні рядки й стовпці перераховуються. Довіра до доказу поступово зменшується, якщо контроль давно не тестували. Телеметрія SIEM, EDR, сканерів вразливостей, сервісів ідентифікації та резервного копіювання використовується для автоматичного підтвердження частини показників, але експерт переглядає причинний зв'язок між заходом і загрозою. Це запобігає ситуації, коли велика кількість подій помилково трактується як висока ефективність захисту.

Перевірка адекватності. Модель валідується трьома способами. Узгодженість експертних оцінок перевіряється повторним оцінюванням і аналізом розбіжностей. Фактичну ефективність перевіряють контрольованим відтворенням технік атаки та процедурами оцінювання контролів [3]. Стійкість результату досліджують аналізом чутливості: змінюють ваги, довіру до доказів і припущення про залежність засобів. Якщо невелика зміна одного параметра різко змінює висновок, оцінка позначається нестійкою і потребує додаткового доказу.

Обмеження. Числова оцінка не усуває невизначеність і залежить від повноти переліку загроз. Модель не повинна підміняти аналіз ланцюгів атак, людських помилок і ризиків постачання. Значення перекриття не можна переносити між організаціями без повторної перевірки конфігурації, активів і компетентності персоналу. Проте явна матриця робить припущення видимими, дозволяє відокремити наявність контролю від доведеної ефективності та виявляє дублювання засобів при відсутності захисту від окремих критичних сценаріїв.

Висновки. Запропонований метод оцінює захищеність корпоративної мережі через ступінь перекриття кожної актуальної загрози засобами захисту, підтверджену ефективність і достовірність доказів. Корекція залежних заходів знижує ризик подвійного врахування, а поєднання локальних порогів з інтегральним індексом не дозволяє компенсувати критичну прогалину високими оцінками інших напрямів. Метод формує вимірюваний поточний профіль, залишковий ризик і пріоритетний план удосконалення. Подальше дослідження передбачає апробацію на стенді корпоративної мережі та оцінювання чутливості моделі до якості телеметрії й експертних даних.

Література

1. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments. NIST SP 800-30 Rev. 1. Gaithersburg: NIST, 2012. DOI: 10.6028/NIST.SP.800-30r1.
2. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. Gaithersburg: NIST, 2020. DOI: 10.6028/NIST.SP.800-53r5.
3. Joint Task Force. Assessing Security and Privacy Controls in Information Systems and Organizations. NIST SP 800-53A Rev. 5. Gaithersburg: NIST, 2022. DOI: 10.6028/NIST.SP.800-53Ar5.

4. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0: Quick-Start Guide for Creating and Using Organizational Profiles. NIST SP 1301. 2024. DOI: 10.6028/NIST.SP.1301.
5. MITRE ATT&CK. Enterprise Mitigations. URL: <https://attack.mitre.org/mitigations/enterprise/> (accessed: 15.08.2026).
6. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva: ISO, 2022.

УДК 004.056(7):619.8:351.007

Кононович В.Г., Стайкуца С.В.

СТРУКТУРНА ЦІЛІСНІСТЬ, НЕПОДІЛЬНІСТЬ ТА ЕМЕРДЖЕНТНІСТЬ – ФУНДАМЕНТАЛЬНІ ВЛАСТИВОСТІ СУЧАСНИХ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ. НАСЛІДКИ

Державний університет інтелектуальних технологій і зв’язку
vl_kononovich@ukr.net; s.staikuca@gmail.com

Анотація. Виконано аналіз причин регулярного розширення функцій і задач систем безпеки інформації (СБІ) та прискорення їх розвитку. Отримано розуміння фундаментальності властивостей структурної цілісності та неподільності емерджентних СБІ, а раніше комплексних систем захисту інформації (КСЗІ). Це дало можливість обґрунтувати перехід на ризико-орієнтовані системи безпеки інформації, запропонувати додати доведення неподільності профілів безпеки та структурної цілісності СБІ. Доцільним є конвергенція СБІ та систем контролю й управління, бо СБІ компенсує нестачу контрольної й управлінської інформації, притаманну цифровим технологіям. Для досягнення неподільності сучасні СБІ слід доповнити, окрім заходів безпеки кіберфізичних систем, заходами соціокіберфізичних систем. Треба розвивати захист від соціальної інженерії та заходи когнітивної безпеки.

Ключові слова: безпека інформації, структурна цілісність, неподільність, емерджентність, системи управління.

Сучасний етап розвитку людства характеризується глибокою інтеграцією цифрових технологій (до штучного інтелекту включно) в усі сфери діяльності установ, підприємств, промислового виробництва – від систем освіти, електронного документообігу, автоматизації та роботизації виробництва, до збереження конфіденційних персональних даних і результатів наукових досліджень. З ростом об’ємів інформації, швидкості інформаційного обміну, значущості інформації для нашого буття, гнучкість і свобода руху інформації перетворилась у хаос і багато у чому в інформаційне сміття. Інформаційне сміття потрібно регулярно прибирати подібно прибиранню сміття на дорогах, вулицях, домівках. Очевидно, що треба розумно обмежити свободу в інформаційному світі, як це організовано фізичному світі за консолідованою згодою людей. Звідси випливає необхідність розгорнути систему кіберзахисту інформації в інформаційно-комунікаційних системах та електронних комунікаціях. Треба розробити «правила інформаційного руху» на «інформаційних дорогах» подібно тому, як у Лондоні вводились правила руху карет, а потім руху перших автомобільних екіпажів. В інформаційному світі слід мати справу з організованими і керованими потоками інформації, подібно тому, як у фізичному світі організовані потоки енергії і матерії.

Система безпеки інформації (СБІ) стає критично важливим фундаментом як процесів функціонування та життєдіяльності, так і конвергуючись до систем керування й державного управління. СБІ є фундаментом у двох ролях. Перша, внутрішня роль полягає у забезпеченні умов для виконання своєї задачі – створювати безпеку. Друга, зовнішня, роль полягає у постачанні даних щодо стану об’єкта контролю та управління й певних засобів управління.

У першій ролі СБІ можуть мати наступні недоліки. СБІ часто розбудовується фрагментарно через намагання закрити локальні вразливості окремими технічними засобами. Головна методологічна помилка такого підходу полягає в ігноруванні принципу структурної неподільності: СБІ є емерджентною системою, де захисна функція виникає виключно як результат синергії та взаємозв’язку всіх її елементів. Вилучення, послаблення або збій навіть одного компонента (наприклад, контуру розмежування прав доступу чи мережевого екрана) не просто створює локальну вразливість, а повністю руйнує цілісність усього периметра безпеки, нівелюючи ефективність інших засобів захисту.

Мета дослідження. Теоретично обґрунтувати необхідність дотримання принципу цілісності (неподільності) при проектуванні та експлуатації СБІ в умовах специфічного гетерогенного середовища.

Результати дослідження.

Справедливим є твердження: «Всякий новий вимисел, по-перше, стає кінець-кінцем зброєю, а по друге, руйнує неподільність безпеки». Як свідчить штучний інтелект, першу частину цього твердження висловив у 1721 році французький мислитель Шарль Луї Монтенсьє у своєму епістолярному романі «Персидські листи»

(Лист CV / 105). Персонаж на ім’я Реді висловлює побоювання щодо розвитку наук і ремесел, зазначаючи, що нові відкриття та хімічні винаходи у підсумку слугують лише потребам війни та стають знаряддям для винищення людства.

Неподільність систем (або цілісність) у теорії систем означає, що властивості системи не зводяться до простої суми властивостей її окремих елементів. При вилученні або заміні хоча б однієї частини руйнується вся структура, і утворюється зовсім інша система з новими характеристиками. [1, с. 33]. У нашому випадку, при появі нових елементів, блоків, вузлів мережі, підсистем, тим більше – технік та технологій, неподільність системи безпеки порушується внаслідок нових вразливостей і для відновлення неподільності необхідно добудовувати нові характеристики, функції, заходи і засоби. СБІ має сенс лише якщо вона цілісна. Інформація як об’єкт захисту схожа на рідину або газ. Якщо у судині, де вона зберігається, виникає будь-яка тріщина чи отвір – вона витікає.

Прослідкуємо історично розвиток систем безпеки з точки зору їх властивості неподільності і введемо необхідні системні поняття.

Першим знаряддям безпеки інформації стала криптографія. Після виникнення письменності і можливості транспортувати написане, виявилась необхідність у безпеці інформації. Наприклад, можна приховати повідомлення таким способом. На побритій голові розвідника написати повідомлення. Потримати його в камері пару тижнів, щоб відросло волосся і послати цього розвідника до адресата. Розвідник, подолавши всі фронти, ріки, ліси і гори, доставляє повідомлення полководцю. Голову розвідника, іноді окремо від тіла (треба ж і фізична безпека), брили і читали повідомлення. Одним із найперших задокументованих інструментів для шифрування стала спартанська «скітала» (V століття до нашої ери) [2]. Відправник і одержувач мали по деревному циліндру однакового діаметру. На циліндр намотували вузьку смужку пергаменту або шкіри, писали повідомлення вздовж осі циліндра і отримували зашифроване повідомлення у вигляді хаотичного набору літер. У Стародавній та Середньовічній часи застосовувались шифри заміщення. Прикладом є шифр Цезаря, у якому зміщувались літери алфавіту на декілька позицій. Криптографічний захист інформації (КЗІ) активно розвивався протягом століть. Сьогодні актуальна квантова криптографія.

Наступними геніальними винаходами стали електричний телеграф ний зв’язок і азбука (Семюел Морзе у 1837 році); електричний телефонний зв’язок (Александр Грем Белл у 1876 році та троє інших винахідників); радіозв’язок (теоретичне обґрунтування – Джеймс Максвел і Генріх Герц; пристрої створили Нікола Тесла, Гульємо Марконі, патент 1897 року, та Олександр Попов у 1895 році без патенту). Перше застосування радіо для порятунку людей відбулось 6 лютого 1900 року. О. Попов передав з берегової станції на острові Куутсало радіограму з наказом криголаму «Ермак» вийти на допомогу 27 рибалкам, яких віднесло на крижині у Фінській затоці біля острова Лавенсаарі.

Винайдення телефону примусило винайти технічний захист інформації (ТЗІ). З 1870 року стали масово виявляти перетік сигналів або перехресні завади з телеграфних ліній до телефонних і навпаки, внаслідок електромагнітної індукції та паралельного прокладання проводів. Телеграфні лінії були одно провідними, другим проводом служила земля і вони були прекрасними антенами. Явище витоку інформації детально дослідив фізик Олівер Гевісайд у 1881 році.

Прискорили розвиток ТЗІ та привели до сполучення та інтеграції КЗІ з ТЗІ події російсько-японської війни в 1904 - 1905 роках. Це повчальна історія. Японія застосовувала радіорозвідку у бойових діях. Радіотелеграфний зв’язок між обложеним Порт-Артур і Владивостоком активно перехоплювався та розшифровувався японською армією і флотом. Підводні морські кабелі були перерізані японцями. В Порт-Артурі були встановлені 18 бездротових телеграфних станцій системи Попова-Дюкрете Паризької та кронштадтської майстерні. Повідомлення передавалися за допомогою азбуки Морзе на довгих хвилях, можливо зі слабким шифруванням. Повідомлення від штабів до берегової бездротової радіотелеграфної станції передавалися за допомогою (Увага!) польового провідного телефонного та телеграфного зв’язку, а також кур’єрами. Порт-Артур оточений сопками, з яких велось візуальне спостереження за містом і гаванню та перехоплення радіосигналів, джерелом яких були телефонні лінії та одно провідні телеграфні лінії. Японське командування заздалегідь дізнавалося про плани російської Тихоокеанської ескадри, рухи суден, переміщення військ та наявність запасів у фортеці. Радіозв’язок з Владивостоком якимось шифрувався, але сигнали з наземних ліній перехоплювався безпосередньо.

Для вирішення проблеми потрібні сполучення, уніфікація та інтеграція КЗІ та ТЗІ. КЗІ має забезпечити безпеку інформації у радіоэфірі. ТЗІ забезпечує безпеку нешифрованої інформації в наземних каналах до входу у шифратор, безпеку процесів, засобів та апаратури шифрування. Потрібні ще заходи фізичної безпеки.

Сполучення (об’єднання) – це злиття кількох однорідних або різнорідних об’єктів в одну спільну структуру чи масив під спільне управління; створення інтерфейсу або каналу зв’язку між двома окремими системами для їх безпечної взаємодії без втрати їхньої автономності; фізичне та логічне підключення компонентів для забезпечення правильного руху трафіку та сигналів тривоги каналами зв’язку.

Уніфікація – це приведення різнорідних засобів захисту, протоколів та політик безпеки до єдиного стандарту чи форми; встановлення єдиних правил, норм для усунення зайвої різноманітності, спрощення роботи та забезпечення сумісності, введення єдиних форматів документів. Без уніфікації правил, політик безпеки та форматів даних система потоне в хаосі несумісних налаштувань.

Інтеграція – це процес та результат об’єднання окремих частин, різних стандартизованих елементів чи систем у нову скоординовану єдину цілісну систему для спільної роботи, створення синергетичного ефекту та побудови міцної взаємозалежної структури заради спільної ефективності.

Кардинальний винахід ХХ століття – мікропроцесор – відкрив нову еру комп’ютерних технологій і декілька разів порушував неподільність систем безпеки по декільком напрямках. Першою реакцією на ці виклики стали комплексні системи захисту інформації (КСЗІ).

Комплекс (лат. *complexus* – зв’язок, сполучення) – це сукупність взаємопов’язаних елементів, що утворюють єдине ціле для виконання певної задачі. Комплексність – це повнота та всебічність охоплення всіх сторін, факторів або умов процесу чи проблеми, що вимагає не вибіркового, а системного вирішення завдань. Комплексування – це процес об’єднання, інтеграції та синхронізації окремих засобів безпеки в єдину систему захисту, де всі елементи взаємодіють без конфліктів, як один злагоджений алгоритм.

Першим нормативним документом із цього напрямку є «Оранжева книга», опублікована у 1983 році під назвою – *Критерії оцінки захисту комп’ютерної системи. Вона стала основою* для всіх наступних міжнародних і національних стандартів інформаційної безпеки. В 1992 році вийшли *«Канадські критерії безпеки комп’ютерних систем»*. В Україні відповідний пакет НД ТЗІ введений у дію в 1999 році. Для відновлення неподільності КСЗІ об’єднували собою три компоненти: ТЗІ в апаратній частині, КЗІ та захист від несанкціонованого доступу в частині програмного забезпечення. Розширено об’єкт захисту. На першому етапі захисту підлягають інформаційні ресурси: інформація, засоби обробки інформації та персонал. На другому етапі забезпечується безпека інформаційних технологій. Далі ми побачимо безпеку інформаційного простору. Міняється методологія опису безпеки. Опис безпеки конструюється через три головних поняття: об’єкт оцінки – елемент або система, безпека якої перевіряється; профіль захисту – незалежний від реалізації документ, який описує вимоги безпеки для певного класу продуктів; завдання безпеки – специфікація вимог для конкретного комерційного продукту. В Україні діють ДСТУ ISO/IEC 15408-1:2023, -2, -3.

Паралельно з інформаційною безпекою розвивається кібербезпека. Під комплектацією (або комплексним пакетом рішень) у кібербезпеці розуміють набір взаємопов’язаних технічних інструментів, програмних модулів та організаційних політик, які об’єднуються в єдину багаторівневу систему захисту для запобігання, виявлення та нейтралізації кіберзагроз. Основні компоненти комплексу захисту:

– **Захист мережі:** міжмережеві екрани, систем виявлення вторгнень, захищений віддалений доступ.

– **Безпека кінцевих точок:** антивірусне ПЗ та агенти для контролю робочих станцій та серверів.

Захист даних: інструменти шифрування та системи запобігання витоку даних.

– **Моніторинг та реагування:** центри моніторингу подій інформаційної безпеки (SOC) та регулярний аудит (тестування на проникнення).

У контексті кіберзахисту (кібербезпеки) емерджентність також є фундаментальним принципом.

Тим часом, КСЗІ втратили свою неподільність (структурну повноту) внаслідок нових масштабних задач та кардинальної зміни умов середовища функціонування. КСЗІ будуються в межах певного периметра. Граничні брандмауери поділяють мережі на зовнішні та внутрішню. Створюється своєрідна «контрольована зона». Сьогодні є потреба забезпечення безпеки інформації в транс граничному глобальному інформаційному середовищі чи кіберсередовищі. Крім того, держави рішуче перейшли від захисту інформації з обмеженим доступом (доля якої не перевищує 5 – 7%) до захисту фактично безмежних масивів відкритої інформації. В першу чергу захищають критичну для забезпечення життєдіяльності інформацію. Захисту підлягають державні інформаційні ресурси та персональна (її, можливо помилково, називають конфіденційною). Ці нові задачі є не самотніми і є похідними від всепланетарної історичної задачі. Після чергової світової війни побудувати раціональний світ – забезпечити захищений доступ до ресурсів Землі і Космосу при збереженні ієрархічної багаторівневої структури: людина, сім’я, нація, народ... В частині безпеки, наша задача побудувати масштабовану, емерджентну, цілісну, керовану СБІ за ефективною методологією і методам побудови.

Масштабування – це здатність системи безпеки збільшувати (або зменшувати) свою продуктивність та обсяг захисту у відповідь на зростання мережі чи кількості користувачів без зміни архітектури, із збереженням її базових властивостей та структури; здатність системи безпеки збільшувати свою пропускну здатність (обробляти більше трафіку, логів, користувачів) без втрати рівня захищеності..

Комплектація – це підбір та забезпечення системи повним набором необхідних елементів (програм, ліцензій, обладнання) для її повноцінного функціонування; збирання окремих елементів для конкретної мети (антивірус, шифратор та DLP для захисту ноутбука бухгалтера – вони діють окремо, але разом складають повний комплект захисту).

Емерджентність (англ. *Emergence* – виникнення, поява нового) у теорії систем – наявність у будь-якої системи особливих властивостей, не властивих її підсистемам і блокам, а також сумі елементів, не пов’язаних системо утворюючими зв’язками, – це поява у системи нових властивостей, яких немає в її окремих складових. Властивість важко чи неможливо передбачити, знаючи лише окремі компоненти. Позитивний приклад. Окремо антивірус та міжмережевий екран (файрвол) мають обмежену ефективність. Об’єднані в систему XDR (Extended Detection and Response), вони обмінюються даними та зупиняють складні атаки, які не помітив би жоден із них самотійно. Нова парадигма кіберзахисту визнає – зламати можна все. Тому емерджентною властивістю системи стає здатність функціонувати під час атаки та миттєво відновлюватися (через автоматичні бекапи, дублювання каналів та ізоляцію сегментів). Можливі негативні наслідки. Окремо дві програми можуть бути абсолютно безпечними та сертифікованими. Проте під час їхньої інтеграції виникає конфлікт або «діра» в

логіці, яку використовують хакери. Помилка в налаштуванні одного компонента безпеки (наприклад, системи аутентифікації) через взаємозв’язки може повністю заблокувати роботу всієї установи. В криптографії стійкість окремих алгоритмів не гарантує стійкість системи.

Сучасний інформаційний та кіберпростір настільки складний і динамічний, що захистити його статичними інструментами неможливо. Безпека виникає не тоді, коли ви купуєте найкращі програми, а тоді, коли ці програми, люди та процеси починають правильно взаємодіяти. СБІ мають бути емерджентні, структурно цілісні, масштабуємі. СБІ об’єднують у собі системи інформаційної безпеки, ТЗІ, КЗІ (разом це КСЗІ), фізичної безпеки, відео спостереження та сигналізації, зокрема пожежної. КСЗІ комплектувались із 24 функцій захисту інформації. До СБІ пред’являються 96 вимог до заходів оцінки реалізації базового профілю безпеки у випадку обробки службової інформації. А загальна кількість заходів оцінки складає 437.

Нова структура сучасних «Загальних критеріїв» складається не з трьох а з 5 частин: 1) Загальна модель – задає базові поняття та архітектуру оцінювання; 2) Компоненти функціональних вимог безпеки – каталог функцій захисту, таких як автентифікація, криптографія, аудит тощо; 3) Компоненти гарантій безпеки – критерії оцінки правильності розробки та тестування; 4) Рамкова структура для специфікації методів та дій з оцінювання – детально описує методики, за якими повинні проводитись аудит; 5) Пакеті вимог безпеки – містить готові набори вимог для спрощення розробки Профілів захисту під типові технології. В Україні продовжують напрацьовуватись базові, галузеві та цільові профілі безпеки для службової та відкритої інформації, для технологічного сектору та критичної інфраструктури.

Удосконалено методологію побудови СБІ. Замість Технічного завдання, Проекту системи захисту для СБІ рекомендовано План захисту. Замість сертифікації системи захисту рекомендовано Оцінка реалізації СБІ та її авторизація. Ось як виглядає порядок побудови СБІ: Нова версія пристосована до динамічних середовищ. Жорсткі правила порівняння безпекових профілів ліквідує двозначність при сертифікації. Наявність типових профілів пришвидшує роботу і знижує вартість сертифікації для розробників.

Етапи розгортання ризико-орієнтованих СБІ наступні: 1) Етап аналізу ризиків за детально розробленою методикою розрахунків ризику; 2) Етап категоріювання безпеки з врахуванням всіх активів інформаційної системи на основі її опису. 3) Етап вибору заходів захисту – це вибір базового або галузевого профілю безпеки за результатами оцінки ризиків та категоріювання безпеки. 4) Етап реалізації заходів захисту відповідно до розробленої Концепції безпеки інформації та приватності із методології проектування систем захисту інформації; 5) Етап оцінювання безпеки – встановлення коректності реалізації заходів захисту інформації та персональних даних в інформаційній системі відповідно до обраного профілю захисту; 6) Етап авторизації безпеки інформаційної системи шляхом внесення запису до реєстру авторизованих систем; 7) Етап постійного моніторингу безпеки, для чого розробляється відповідна стратегія.

Згідно сучасної концепції кіберзахисту і оскільки всі зв’язки в складній глобальній системі неможливо, то до кіберзахисту слід додати наступні важливі заходи:

– Концепція нульової довіри. Архітектура будується на принципі «нікому не довіряй, завжди перевіряй». Взаємодія багатьох елементів може породити вразливі та відповідну загрозу. Будь-який запит всередині мережі повинен перевірятися так само жорстко, як і ззовні.

– Постійний хаос-інжиніринг. Для перевірки захищеності наймають етичних хакерів, які імітують реальні атаки, щоб виявити непередбачувані емерджентні помилки на стиках технологій та людської поведінки.

– Автоматизація та штучний інтелект. Обсяг емерджентних подій у сучасній мережі перевищує можливості людського мозку. Тому стало необхідним застосовувати штучний інтелект для аналізу аномалій в поведінці всієї системи в реальному часі.

І все ж, незважаючи на всі викладені заходи, СБІ недостає властивості неподільності і по суті є неефективними. Причина полягає у слабості захисту від людського фактору, соціальної інженерії, відсутності когнітивної безпеки. Це є напрямками подальших досліджень.

Висновки.

Наша задача побудувати масштабовану, емерджентну, цілісну, керовану СБІ за ефективною методологією і методам комплектування профілів захисту, категоріювання об’єктів, побудови, оцінювання реалізації та авторизації систем безпеки інформації та приватності.

Забезпечення системної цілісності контуру безпеки вимагає переходу від дискретного застосування захисних інструментів до планування монолітної, методологічно обґрунтованої архітектури, здатної протидіяти каскадним загрозам у гетерогенному середовищі.

Не є раціональним суперечки навколо виділення окремої спеціальності K4 – Управління інформаційною безпекою. З огляду на принцип (властивість) структурної неподільності спеціальність F5 – Кібербезпека та захист інформації включає в себе управління інформаційною безпекою. Це констатовано в документі [4], де в колонці «Спеціальності 2023» сказано, що «Спеціальності 2026 F5 – Кібербезпека та захист інформації» відповідають «Спеціальності 2023 125 – Кібербезпека та захист інформації і 256 – Національна безпека (за окремими сферами забезпечення і видами діяльності). І навпаки, спеціальності K4 – Управління інформаційною безпекою відповідає спеціальність F5 – Кібербезпека та захист інформації, звісно з урахування специфіки галузі наук Безпеки держави, національної безпеки тощо. Логічні зв’язки спеціальності K4 витікають з ланцюга K3 – Національна безпека → K4 – Управління інформаційною безпекою → K5 – Військове управління.

Література

1. Теорія систем і системний аналіз: навчальний посібник / О.А. Балтовський, К.Ю. Ісмаїлов, О.І. Сіфоров, Г.В. Форос, О.М. Заєць; за заг. ред. Балтовського О.А. Одеса: РВВ ОДУВС, 156 с. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/d1afe0b7-8bc0-40c9-a1b9-bcd93ff8a7content>.
2. Калакутський Антон. Як еволюціонувала криптографія. 2026. [Електронний ресурс] URL: <https://dou.ua/forums/topic/61026/>.
3. Актуальний Перелік галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти. (Назва з екрану). URL: https://m8.org.ua/uk/specialities-new/?srsltid=AfmBOooPQh_o2b56pWtuuwWelM-RXmkYoPPr6FF_5nrX_8SIDMrvpMAT.

УДК 004.056:681.5

¹Тарасенко Я.В., ²Матусяк П.О.

ПРОБЛЕМИ РОЗМЕЖУВАННЯ ШТАТНИХ ТА АНОМАЛЬНИХ ЗМІН ІНФОРМАЦІЙНОГО СТАНУ КІБЕРФІЗИЧНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ ВИМІРЮВАННЯ

¹Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки
yaroslav.tarasenko93@gmail.com

²Державний університет інформаційно-комунікаційних технологій
Pavelmatusyak@gmail.com

Анотація. Розглянуто проблеми розмежування штатних та аномальних змін інформаційного стану кіберфізичних систем за результатами вимірювання. Визначено необхідність урахування режиму функціонування, узгодженості взаємопов'язаних вимірювальних каналів, часових характеристик відхилень та невизначеності результатів вимірювання. Обґрунтовано послідовне розмежування етапів встановлення аномальної зміни інформаційного стану та подальшої інтерпретації її походження як можливого прояву вторгнення. Сформульовано вимоги до представлення вимірювальної інформації для забезпечення достовірного розмежування станів.

Ключові слова: кіберфізична система, інформаційний стан, вимірювання, аномалія, самодіагностика, виявлення вторгнень.

У корпоративних кіберфізичних системах одним зі шляхів контролю поточного стану є вимірювання параметрів фізичних, обчислювальних і комунікаційних процесів. Для задач виявлення вторгнень встановлення самого факту зміни вимірюваного параметра повинно супроводжуватися визначенням того, чи відповідає ця зміна допустимому режиму функціонування та чи містить вона ознаки аномального перебігу процесів. У роботі [1] показано, що при взаємодії корпоративної та сенсорної IoT-мереж кіберзагрози сенсорного сегмента впливають на області кіберзахисту корпоративної мережі, що визначає взаємозалежність фізичної та інформаційної складових безпеки кіберфізичної системи. Потребує врахування як помилкове віднесення штатної зміни до аномальної, так і прийняття аномальної зміни за штатну.

Розмежування штатних та аномальних станів не може зводитися до перевірки окремого значення відносно незмінного порога. У роботі [2] зашумлені вхідні й вихідні дані зіставляються з множиною поведінок номінальної моделі за наявності параметричної невизначеності. Така постановка показує, що штатний стан доцільно характеризувати допустимою областю поведінки системи. Відповідно, постає ряд проблем, які потребують окремого рішення в ході вимірювання стану кіберфізичної системи.

Перша проблема пов'язана з формуванням меж штатної зміни. Один і той самий числовий приріст параметра може бути допустимим для перехідного режиму і неприйнятним для усталеного. Статична межа, сформована без урахування режиму функціонування, змішує аномалію з природною варіативністю процесу. Водночас надмірне розширення допустимої області приховує слабкі відхилення, що можуть накопичуватися поступово. Еталонний стан для задачі розмежування має задаватися залежною від режиму функціонування областю допустимих результатів вимірювання.

Окремо необхідно розрізняти фактичну зміну стану та невизначеність результатів вимірювання, за якими цей стан оцінюється. Розширення діапазону спостережуваних значень унаслідок шуму або неповноти даних саме по собі не означає аномалії, але повинно впливати на межі, у яких результат може вважатися сумісним зі штатною поведінкою. Звідси впливає необхідність врахування невизначеності саме як характеристики достовірності розмежування.

Друга проблема полягає в недостатній інформативності одиничного параметра. Аномальна поведінка може проявлятися порушенням характерного співвідношення між декількома показниками та водночас

окремий показник може не досягати критичного значення. У роботі [3] сформовано поведінкові сигнатури з даних моніторингу та порівняно їх з еталонними профілями поведінки за кількісними показниками відповідності. У наведених авторами експериментах розмежовуються нормальна поведінка, тривалі та перехідні відхилення з додатковим поділом останніх за характером їх впливу [3], що підтверджує практичну значущість одночасного врахування складу параметрів і характеру їх зміни. При цьому, штатність зміни оцінюється за узгодженістю результатів взаємопов'язаних вимірювальних каналів. Значення окремих параметрів можуть залишатися допустимими, але їх спільна конфігурація вже не відповідатиме типовому режиму. Протилежна ситуація також можлива: вихід одного параметра за звичний діапазон може бути закономірною реакцією системи.

Крім того, агрегування результатів вимірювання має зберігати інформацію про джерело та структуру відхилення. Інтегральна оцінка може підтвердити невідповідність поточного стану еталонному, але без збереження структури первинних даних втрачається можливість визначити, чи сформовано її одиничним каналом, групою взаємопов'язаних параметрів або зміною їх часової узгодженості.

Третя проблема стосується природи виявленого відхилення. Аномальна зміна інформаційного стану не є автоматичним доказом вторгнення, оскільки подібний вимірювальний прояв може бути зумовлений несправністю сенсора, збуренням фізичного процесу тощо. У роботі [4] окремо вирішується задача розмежування атаки повторного відтворення та зміщення показів сенсора як різних причин порушення спостережуваного стану. Така задача підтверджує необхідність відокремлювати встановлення факту аномальної зміни від подальшої інтерпретації її походження. На вимірювальному рівні доцільно встановити невідповідність спостережуваної поведінки допустимому стану та визначити параметри, які сформували таку невідповідність, тоді як висновок про вторгнення потребує додаткового аналізу характеру відхилення.

Принциповою межею є інформаційна розрізняюваність спостережуваних траєкторій. Якщо послідовність вимірювань одночасно сумісна зі штатною та аномальною поведінкою, підвищення чутливості порога не усуває неоднозначності. У роботі [2] формалізовано процеси виявлення через уникнення перетину множин поведінки номінальної та несправної моделей на скінченному часовому горизонті. З цього випливає, що для частини змін необхідним є накопичення достатньої послідовності вимірювань або залучення додаткових інформативних параметрів.

Четверта проблема пов'язана з часовою локалізацією аномальної зміни. Короткочасне відхилення може бути допустимим перехідним процесом, тоді як невелике, але стійке або закономірно повторюване відхилення здатне мати більшу діагностичну значущість. У роботі [5] для виявлення прихованих атак цілісності застосовують підхід зі зворотною в часі обробкою інформації про зміну стану. Такий результат демонструє інформативність часової структури зміни стану при виявленні прихованих впливів.

Для розмежування штатних та аномальних змін за результатами вимірювання доцільно одночасно враховувати три типи контексту: режимний, міжпараметричний та часовий. Режимний контекст визначає допустимість зміни для поточного стану функціонування; міжпараметричний – узгодженість зміни з поведінкою взаємопов'язаних каналів; часовий – стійкість, тривалість і повторюваність відхилення. Невизначеність вимірювання при цьому повинна характеризувати достовірність такого розмежування.

Перспективним напрямом вирішення визначених проблем є формування представлення результатів вимірювання, у якому відхилення характеризується відносно допустимої області поточного режиму, взаємозв'язків між параметрами та його часової поведінки. Такий напрям створює можливість переходу від реакції на одиничне порогове перевищення до оцінювання відповідності спостережуваної зміни закономірностям штатного функціонування.

Для задач виявлення вторгнень доцільно розмежувати два послідовні рівні оброблення вимірювальної інформації: встановлення аномальності зміни інформаційного стану та подальшу інтерпретацію її походження як можливого прояву вторгнення. Такий поділ не отождоює будь-яку аномалію з атакою та дає змогу зберегти вимірювальну обґрунтованість результатів перед переходом до безпекової інтерпретації.

Перевірку коректності розмежування доцільно проводити на сценаріях, де штатна зміна режиму та аномальний вплив формують близькі за величиною відхилення параметрів. Для таких випадків необхідно окремо оцінювати хибне віднесення штатних переходів до аномалій і пропуск слабких аномальних змін, що дозволить визначити фактичний внесок режимного, міжпараметричного та часового контексту в розрізняюваність станів.

Висновки. За результатами аналізу визначено, що достовірне розмежування штатних та аномальних змін інформаційного стану потребує врахування режиму функціонування, узгодженості взаємопов'язаних вимірювальних каналів і часових характеристик відхилення. Невизначеність результатів вимірювання при цьому визначає ступінь обґрунтованості такого розмежування. Обґрунтовано послідовність, за якої встановлення аномальності зміни передуватиме інтерпретації її походження як можливого прояву вторгнення. Визначені положення задають вимоги до представлення вимірювальної інформації та до сценаріїв перевірки розмежування штатних і аномальних станів.

Література

1. Тарасенко Я., Туровський О., Іванкін В., Матусяк П., Томашевський М. Забезпечення кіберзахисту корпоративної мережі передачі даних в ході організації взаємодії між пристроями IoT дослідницьких

- лабораторій // *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. № 82(2). С. 334-343.
2. Harirchi F., Ozay N. Guaranteed model-based fault detection in cyber-physical systems: A model invalidation approach // *Automatica*. 2018. Vol. 93. P. 476-488.
 3. Odyurt U., Pimentel A.D., Gonzalez Alonso I. Improving the robustness of industrial Cyber-Physical Systems through machine learning-based performance anomaly identification // *Journal of Systems Architecture*. 2022. Vol. 131. Art. 102716.
 4. Zhang K., Keliris C., Polycarpou M.M., Parisini T. Discrimination between replay attacks and sensor faults for cyber-physical systems via event-triggered communication // *European Journal of Control*. 2021. Vol. 62. P. 47-56.
 5. Zhang K., Keliris C., Polycarpou M.M., Parisini T. Detecting stealthy integrity attacks in a class of nonlinear cyber-physical systems: A backward-in-time approach // *Automatica*. 2022. Vol. 141. Art. 110262.

УДК 004.056

¹Орлов Р.Р., ²Тарасенко Я.В.

ВИМІРЯНА КРИТИЧНІСТЬ ЯК ІНФОРМАЦІЙНА ОСНОВА ПРОГНОЗНОГО ОЦІНЮВАННЯ РИЗИКУ КІБЕРІНЦИДЕНТІВ

¹Державний університет інформаційно-комунікаційних технологій
romanorlov0110@gmail.com

²Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки
yaroslav.tarasenko93@gmail.com

Анотація. Розглянуто виміряну критичність кіберінциденту як інформаційну основу прогнозного оцінювання ризику. Обґрунтовано вимоги до її представлення у вхідному просторі прогновної моделі з урахуванням СІА-компонентів, часової прив'язки, невизначеності та контексту. Визначено необхідність розмежування невизначеності вимірювання критичності й невизначеності прогнозу, а також відокремлення контексту активу та загрози від самої критичності. Запропоновано методологічну часову межу між даними поточного стану та прогнозованими наслідками і підхід до перевірки інформаційного внеску критичності у прогноз ризику.

Ключові слова: кіберінцидент, критичність, ризик, прогнозне оцінювання, СІА-профіль, невизначеність.

У сучасних інформаційно-комунікаційних системах прогнозне оцінювання ризику кіберінцидентів набуває важливого практичного значення. Таке оцінювання спирається на дані, що відображають фактичний стан інциденту та зміну його впливу. Виміряна критичність може виконувати функцію узагальнення спостережуваних наслідків порушення конфіденційності, цілісності та доступності. Кількісне оцінювання кіберризiku при цьому розглядається як задача поєднання сукупності вимірюваних факторів. У байєсівському розширенні FAIR, описаному в роботі [1], показано доцільність інтеграції таких факторів у ймовірнісну модель для підтримки рішень. Критичність у такому випадку трактується як один із ключових інформаційних входів прогновної оцінки.

Потреба формування такого набору вхідних параметрів визначається різницею між констатацією поточного стану і прогнозуванням подальшого розвитку інциденту. Результат вимірювання критичності характеризує вже наявний або виявлений вплив на інформаційні властивості та пов'язані активи, тоді як прогноз ризику має відображати потенційні наслідки на визначеному часовому горизонті. У роботі [2] пов'язано недостатню проактивність реагування саме з дефіцитом прогнозних моделей, що використовують дані та фактичні свідчення для визначення чинників майбутнього розвитку кіберподій. Доцільність формалізованого інформаційного забезпечення прийняття рішень з урахуванням структурованих і неструктурованих даних за ризикових умов також у дослідженні ситуаційного управління ризиками [3]. У сукупності це обґрунтовує необхідність формування вхідного простору прогновної моделі з даних, що кількісно характеризують поточний стан кіберінциденту.

Для використання вимірної критичності як такого входу недостатньо передавати в прогнозну модель лише дискретний клас (низька, середня або висока критичність) або лише інтегральну оцінку. Інформаційна повнота передбачає збереження структурованого профілю критичності, у якому окремо представлені складові впливу на конфіденційність, цілісність і доступність, підсумкова оцінка та характеристика невизначеності її отримання. Завдяки цьому забезпечується можливість відрізнити інциденти з однаковим інтегральним рівнем, але різною природою впливу, і не втрачати ознаки, потенційно значущі для прогнозування.

Важливою властивістю зазначеного типу представлення є порівнюваність. Якщо критичність різних інцидентів формується за різними шкалами або з різною семантикою компонентів, прогнозна модель отримусь неоднорідні ознаки, а зміна їх числових значень не обов'язково відповідає реальній зміні стану. До включення критичності у вхідний простір необхідно забезпечити єдині правила інтерпретації компонентів, узгоджений діапазон значень та незмінність змісту шкали в часі. При цьому нормалізація повинна зберігати співвідношення між СІА-компонентами, інакше вхідне представлення може спотворювати характер впливу.

Часова прив'язка є принциповою вимогою до використання вимірної критичності. Значення, отримане на початковому етапі розслідування, може змінюватися в міру надходження нових цифрових спостережень, виявлення додаткових уражених активів або уточнення фактичних наслідків. Вхід прогновної моделі повинен містити значення критичності і момент або інтервал його формування, попередні оцінки та ознаки їх зміни. Динамічний характер такого підходу узгоджується з результатами дослідження [4], у якому для проактивного оцінювання кіберризiku інтегрують внутрішню інформацію організації та відкриті джерела, переводять різнорідні дані у кількісне подання і використовують їх у байєсівській мережі для динамічного визначення ймовірності успішної кібератаки.

Для прогнозування значущим є характер зміни поточного рівня критичності. Стабільне значення, поступове зростання та різкий стрибок можуть відповідати різним сценаріям розвитку інциденту навіть за однакового значення в останній момент спостереження. Доцільно зберігати послідовність попередніх вимірювань або похідні від неї часові ознаки, що дозволяють відрізнити стан інциденту від його динаміки.

Водночас виміряна критичність не повинна підміняти контекст прогнозування. Два інциденти з близьким поточним рівнем впливу можуть мати різний подальший ризик, якщо для них відрізняються актуальні відомості про експлуатацію вразливостей і поточну активність загроз. У роботі [5] показано, що надходження актуальної інформації про кіберзагрози змінює апостеріорні ймовірності, а вразливості з новими свідченнями активної експлуатації отримують вищі динамічні оцінки ризику, ніж вразливості з подібними CVSS-оцінками без підтвердженої активності. Із зазначеного слідує, що виміряна критичність має доповнюватися контекстом, який характеризує актуальність і розвиток загрози.

Контекст активу доцільно відокремлювати від самої критичності. Критичність характеризує вплив конкретного інциденту на конфіденційність, цілісність і доступність, тоді як контекст відображає властивості середовища, у якому цей вплив реалізується: функціональне призначення, залежності, зовнішню доступність та стан захисних засобів. Таке розділення запобігає подвійному врахуванню одних і тих самих факторів та дає змогу окремо оцінити внесок вимірної критичності і контекстних ознак у прогнозну оцінку.

Оцінка невизначеності вимірної критичності повинна бути відокремлена від невизначеності самого прогнозу ризику. Оцінка невизначеності вимірної критичності характеризує повноту і надійність цифрових спостережень, на основі яких визначено поточний стан. У свою чергу, невизначеність самого прогнозу ризику є невизначеністю щодо майбутнього розвитку інциденту на заданому горизонті. Їх змішування ускладнює інтерпретацію результату: високий прогнозний ризик може бути наслідком як справді несприятливого сценарію, так і недостатньо визначеного початкового стану. Характеристика довіри до критичності має передаватися у модель окремою ознакою, а не приховуватися всередині інтегрального значення.

Окремо необхідно враховувати неповноту СІА-профілю. Відсутність підтверджених відомостей щодо однієї з компонент не повинна інтерпретуватися як нульовий вплив, оскільки на ранніх етапах розслідування це може бути наслідком недостатності спостережень. Пропуск компоненти та її фактичне нульове значення мають бути розрізнені у вхідних даних, оскільки неповнота спостережень перетворюється на систематичне заниження поточного стану і спотворює інформацію, на основі якої формується прогноз ризику.

Не менш важливою є узгодженість критичності з горизонтом прогнозування. Одна й та сама оцінка поточного впливу має різну прогностичну цінність для різних часових горизонтів, оскільки з часом зростає роль зовнішніх чинників і реакції захисних механізмів. Момент вимірювання критичності та горизонт прогнозу повинні задаватися явно, щоб зіставляти оцінки, сформовані за однакових часових умов.

Методологічну межу між вимірюванням критичності та прогнозуванням ризику доцільно задавати моментом формування оцінки. До критичності повинні включатися лише цифрові спостереження, доступні на цей момент. Ознаки наслідків, що виникають після цього моменту або використовуються як ціль прогнозування, мають належати прогнозному контуру. Таке розмежування запобігає змішуванню поточного вимірної стану з майбутнім результатом і дає змогу окремо оцінювати внесок критичності у якість прогнозу.

Доказовість інформаційної ролі вимірної критичності слід оцінювати окремо від загальної якості прогновної моделі: за незмінної архітектури порівнювати вхід без критичності та з її структурованим представленням. Послідовне вилучення СІА-компонентів, невизначеності й часових ознак дозволить встановити, які складові дають самостійний внесок у прогноз, а які лише дублюють контекст.

Висновки. Сформульовано вимоги до представлення вимірної критичності у вхідному просторі прогновної моделі ризику кіберінцидентів у вигляді структурованого і визначеного на часовому інтервалі опису поточного стану. Невизначеність вимірювання критичності має бути відокремлена від невизначеності прогнозу, а відсутність підтвердженого значення СІА-компоненти не можна прирівнювати до нульового впливу. Контекст активу і загрози слід подавати окремо, щоб уникнути подвійного врахування факторів. Обґрунтовано, що часова межа між доступними спостереженнями та прогнозованими наслідками визначає коректний склад вхідних даних та створює умови для подальшої перевірки внеску критичності у прогноз ризику.

1. Wang J., Neil M., Fenton N.E. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model // *Computers & Security*. 2020. Vol. 89. Art. 101659.

2. Ferreira D.J., Mateus-Coelho N., Mamede H.S. Methodology for predictive cyber security risk assessment (PCSRA) // *Procedia Computer Science*. 2023. Vol. 219. P. 1555-1563.

3. Prokopenko T., Lanskykh Y., Prokopenko V., Pidkuiko O., Tarasenko Y. Development of the comprehensive method of situation management of project risks based on big data technology // *Eastern-European Journal of Enterprise Technologies*. 2023. Vol. 1, No. 3(121). P. 38-45.

4. Cheimonidis P., Rantos K. A novel proactive and dynamic cyber risk assessment methodology // *Computers & Security*. 2025. Vol. 154. Art. 104439.

5. Thevaratnam S., Rezaeifar Z. Quantifying cyber threat using Bayesian statistical analysis // *International Journal of Information Security*. 2026. Vol. 25. Art. 43.

УДК 004.056:616-073.7

Рябко І. Б., Ключишников І. М.

ОЦІНЮВАННЯ КРИТИЧНОСТІ ВІДМОВ БЕЗПЕКИ МЕДИЧНОЇ ЗОБРАЖУВАЛЬНОЇ КІБЕРФІЗИЧНОЇ СИСТЕМИ МЕТОДОМ ІМЕСА

Національний аерокосмічний університет «Харківський авіаційний інститут»
i.b.ryabko@student.csn.khai.edu, i.kliushnikov@csn.khai.edu

Анотація. Розглянуто задачу кількісного оцінювання критичності відмов, спричинених порушеннями безпеки, у медичній зображувальній кіберфізичній системі на базі PACS. Показано, що двовимірні матриці ризику непридатні для цього класу систем, оскільки згортають виявність у наслідок і не розрізняють гучну відмову та тиху компрометацію з однаковими наслідками. Застосовано метод ІМЕСА з тривимірною шкалою «тяжкість — імовірність — виявність» до 21 сценарію атаки. Показано, що запропонована архітектура контрзаходів знижує сумарний RPN на 72,1 %, причому основний внесок дає зростання виявності, а не запобігання.

Ключові слова: кібербезпека медичних систем; PACS; DICOM; ІМЕСА; критичність відмов; RPN; виявність; NIST SP 800-53.

Актуальність. Медичні зображувальні платформи на базі DICOM обробляють персональні дані пацієнтів і водночас формують вхід для клінічно значущих рішень — від оптимізації протоколів опромінення до рекомендацій систем підтримки прийняття рішень. Порушення безпеки в таких системах є не лише інцидентом конфіденційності: спотворений об’єкт RDSR або підмінена вага моделі перетворюються на хибну клінічну дію. Це вимагає інструменту, який ранжує сценарії атак за інженерним критерієм.

Чому ІМЕСА, а не матриця ризику. Двовимірні матриці «ймовірність × наслідок» домінують у практиці, але вони згортають виявність у наслідок. Для клінічної платформи ця відмінність вирішальна: відмова в обслуговуванні на порту DIMSE проявляє себе за секунди, тоді як цілеспрямована модифікація дозових величин із автентифікованого джерела може залишатися непоміченою місяцями, поступово зміщуючи базові рівні дози. Метод ІМЕСА (Intrusion Modes and Effects Criticality Analysis) вводить третю вісь — виявність — і тим самим робить «тихі» сценарії видимими для процедури ранжування.

Шкали та показник критичності. Кожен сценарій оцінюється за трьома порядковими шкалами 1–5: тяжкість S, імовірність реалізації O та виявність D до впровадження контролів, де більше значення D означає гіршу виявність. Показник критичності обчислюється як $RPN = S \times O \times D$ і належить проміжку [1, 125]. Клас High присвоюється при $RPN \geq 40$ і означає, що контрзаходи є обов’язковими до клінічного впровадження. Оскільки RPN є добутком порядкових шкал, він використовується виключно для ранжування, а не як абсолютна міра ризику; додатково діє правило, за яким сценарій із $S = 5$ потребує контрзаходу незалежно від добутку.

Результати. Модель охоплює 21 сценарій атаки T1–T21, віднесених до компонентів платформи та до категорій STRIDE. Агрегований ефект архітектури контрзаходів наведено у таблиці 1, а перерозподіл сценаріїв за класами критичності — на рис. 1.

Таблиця 1 – Агрегований вплив архітектури контрзаходів на модель ІМЕСА.

Показник	До	Після	Зміна
Сумарний RPN за T1–T21	971	271	–72,1 %
Середній RPN на сценарій	46,2	12,9	–72,1 %
Середня ймовірність O	2,52	1,48	–41,3 %
Середня виявність D	4,14	1,95	–52,9 %

Сценаріїв класу High

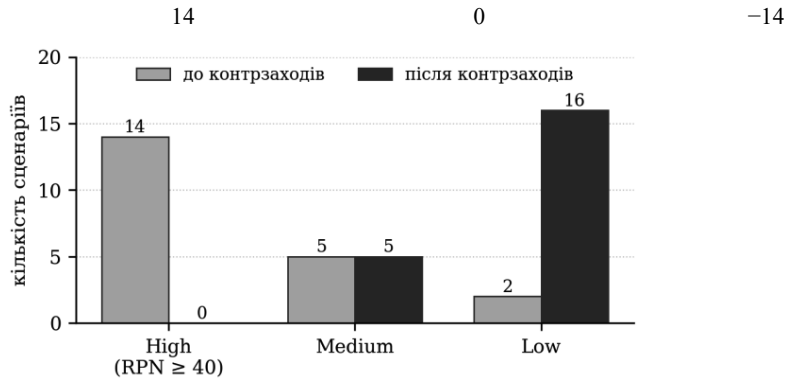


Рисунок 1 – Розподіл 21 сценарію за класами критичності до і після впровадження контрзаходів.

Основний результат оцінювання полягає не у величині зниження, а в його природі, що видно з рис. 2. Середня тяжкість S залишається незмінною за побудовою: контрзаходи не змінюють клінічних наслідків реалізованої атаки. Зниження на 72,1 % забезпечується переважно зростанням виявності (–52,9 % за шкалою D) і меншою мірою — зниженням імовірності (–41,3 % за шкалою O). Іншими словами, домінуючий внесок архітектури полягає не в тому, що атаки стають складнішими, а в тому, що вони перестають бути невидимими. Саме цю властивість двовимірної матриці «ймовірність × наслідок» виразити не здатна.

Як показано на рис. 1, після впровадження контрзаходів жодного сценарію класу High не залишається, проте п’ять сценаріїв класу Medium зберігаються свідомо: кожен з них виконується через легітимний авторизований канал, і їхній залишковий ризик обмежується якістю поведінкових свідчень, а не засобами контролю доступу. Твердження про їх усунення не було б достовірним. Контролі відображено на родині заходів NIST SP 800-53 та згруповано за функціями NIST CSF 2.0.

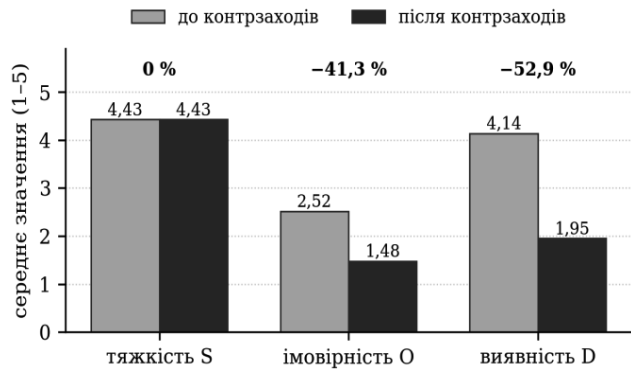


Рисунок 2 – Середні значення шкал тяжкості, імовірності та виявності. Тяжкість не змінюється за побудовою; основне зниження дає виявність.

Відображення на стандарти. Кожному сценарію поставлено у відповідність заходи NIST SP 800-53, згруповані за функціями NIST CSF 2.0: GV — ролі та політики; ID — інвентаризація компонентів і потоків даних; PR — родини IA, SC та AC; DE — AU та SI; RS — IR; RC — CP. Це робить перелік контрзаходів перевірюваним зовнішнім аудитом.

Співвідношення з іншими інструментами. ІМЕСА не замінює CVSS і класичний FMEA, а займає проміжну нішу. CVSS [7] оцінює окрему вразливість поза контекстом системи і не враховує ані клінічних наслідків, ані спроможності організації помітити експлуатацію. FMEA [8] розроблявся для випадкових відмов апаратури і погано описує цілеспрямовану поведінку порушника. ІМЕСА зберігає тривимірну шкалу FMEA, але переозначає режим відмови як режим вторгнення.

Обмеження оцінювання. По-перше, RPN є добутком порядкових шкал, тому різниця між значеннями 75 і 60 не має метричного змісту і використовується лише для впорядкування. По-друге, оцінки O і D є експертними: вони спираються на архітектуру системи та відомі класи атак, а не на статистику інцидентів. По-третє, оцінювання виконано для проєктної конфігурації і підлягає перегляду за даними телеметрії після розгортання.

Висновки. Для медичних зображувальних кіберфізичних систем оцінювання критичності потребує явного врахування виявності, оскільки тиха компрометація даних дози або моделі має ті самі клінічні наслідки, що й гучна відмова, але виявляється на порядки пізніше.

Застосування ІМЕСА до 21 сценарію дало відтворюване ранжування і показало зниження сумарного RPN на 72,1 % із переведенням усіх 14 сценаріїв класу High у класи Medium і Low.

Структура залишкового ризику вказує напрям подальшої роботи: він зосереджений на сценаріях, де порушник є авторизованим суб'єктом, що робить площину аналізу поведінкових свідчень самостійним чинником надійності, а не допоміжним засобом моніторингу.

Література

1. Babeshko E., Kharchenko V., Gorbenko A. Applying F(I)MEA-technique for SCADA-based industrial control systems dependability assessment. *Proc. DepCoS-RELCOMEX*. 2008. P. 309–315.

2. DICOM Standards Committee. DICOM PS3.15: Security and System Management Profiles.

3. IHE International. Audit Trail and Node Authentication (ATNA) Profile.

4. NIST. Cybersecurity Framework (CSF) 2.0. 2024.

5. NIST. SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. 2020.

6. NIST. SP 800-190: Application Container Security Guide. 2017.

7. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. 2019.

8. IEC 60812:2018. Failure modes and effects analysis (FMEA and FMECA). IEC, 2018.

УДК 004.056.5:004.75

Кулієв Р.Д.

МЕТОДИКА ПОБУДОВИ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ
КІБЕРЗАХИСТУ ДАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ
РОЗПОДІЛЕНОГО РЕЄСТРУ

Державний університет інформаційно-комунікаційних технологій
rakhman.kuliiev@gmail.com

Анотація. Запропоновано методику побудови децентралізованої системи кіберзахисту даних на основі дозвільного розподіленого реєстру. Методика поєднує моделювання загроз, обґрунтування доцільності реєстру, розмежування даних між реєстром і зовнішнім зашифрованим сховищем, керування доступом за атрибутами та перевірку стійкості. Визначено послідовність формування архітектури, політик підтвердження транзакцій, життєвого циклу ключів і сценаріїв реагування. Результатом застосування методики є конфігурація системи, у якій цілісність та аудит забезпечуються реєстром, а конфіденційність - криптографічним захистом позареєстрових даних.

Ключові слова: децентралізована система, кіберзахист даних, розподілений реєстр, блокчейн, керування доступом, смартконтракт, нульова довіра.

Централізовані системи зберігання та обміну даними спрощують адміністрування, однак утворюють єдину точку відмови й концентрують привілеї в одного оператора. Компрометація адміністративного облікового запису, сховища журналів або сервера авторизації може одночасно порушити конфіденційність, цілісність і доступність інформації. Розподілений реєстр дає можливість узгоджувати стан між незалежними учасниками та формувати стійкий до непомітної модифікації журнал подій [1]. Водночас незмінність записів сама по собі не забезпечує секретність, правильність вхідних даних чи безпечне керування ключами. Тому використання реєстру має бути частиною цілісної методики кіберзахисту, а не окремим універсальним засобом.

Мета роботи. Сформувати відтворювану послідовність рішень для побудови децентралізованої системи кіберзахисту даних, у якій довіра розподіляється між кількома адміністративними доменами. Вхідними даними методики є перелік інформаційних активів, вимоги до їх конфіденційності, цілісності, доступності та простежуваності, модель порушника, допустимі показники затримки й відновлення, а також організаційні ролі учасників. Виходом є профіль захисту: топологія вузлів, модель консенсусу, правила розміщення даних, політики доступу і підтвердження транзакцій, схема керування ключами, набір контрольних подій та критерії приймання системи.

Методичний принцип. Побудову пропонується вести у трьох взаємопов'язаних контурах. Контур даних визначає, які об'єкти шифруються та зберігаються поза реєстром, а які метадані допускаються до спільного журналу. Контур довіри визначає ідентичності учасників, кворум, правила консенсусу та межі компрометації. Контур управління задає порядок зміни політик, оновлення смартконтрактів, підключення і виключення організацій, реагування на інциденти та аудиту. Рішення вважається узгодженим лише тоді, коли одна й та сама загроза має запобіжний, виявляльний і відновлювальний захід щонайменше в одному з цих контурів.

Етап 1 - інвентаризація та класифікація. Для кожного набору даних фіксуються власник, джерело, споживачі, правова або договірна підстава обробки, строк зберігання, допустимість копіювання між вузлами й наслідки порушення властивостей безпеки. Окремо виділяються змістові дані, службові метадані, політики доступу, криптографічні матеріали та журнали подій. Такий поділ запобігає перенесенню до незмінного реєстру

персональної або іншої чутливої інформації, яку надалі може знадобитися виправити чи видалити. Для кожного класу задається мінімальний набір атрибутів, достатній для перевірки походження, версії та цілісності об'єкта.

Етап 2 - модель загроз і довіри. Аналіз охоплює зовнішнього порушника, скомпрометованого користувача, адміністратора з надлишковими повноваженнями, шкідливий або недоступний вузол, змову частини валідаторів, підміну зовнішнього сховища, викрадення ключа, повтор транзакції, відмову мережевої взаємодії та помилку смартконтракту. Для кожного сценарію визначаються ймовірність, вплив, наявні заходи та залишковий ризик. Межа припустимого ризику задається до вибору платформи. Це дає змогу відмовитися від декларативної децентралізації, коли всі валідатори фактично залежать від одного центру адміністрування, хмарного облікового запису чи спільного сховища ключів.

Етап 3 - перевірка доцільності розподіленого реєстру. Його застосування обґрунтоване, якщо стан мають спільно підтверджувати щонайменше дві організаційно незалежні сторони, між ними немає повністю довіреного оператора, потрібна єдина історія змін, а затримка узгодження сумісна з бізнес-процесом. Якщо даними керує один власник, достатній підписаний централізований журнал або необхідне масове оперативне редагування записів, реєстр не повинен застосовуватися. Для корпоративних та відомчих сценаріїв доцільним є дозвільний реєстр з автентифікованими вузлами, оскільки він дає змогу реалізувати кероване членство, предметні політики підтвердження й контрольоване розкриття даних [2].

Етап 4 - синтез архітектури. У системі виділяються власник даних, користувач, вузол організації, сервіс ідентифікації, сервіс політик, валідатори, зовнішнє сховище, служба керування ключами та незалежний аудитор. Вузли розміщуються у різних адміністративних і, за можливості, інфраструктурних доменах. Жоден учасник одноосібно не повинен змінювати правила доступу, затверджувати власну критичну транзакцію та керувати всіма ключами. Політика підтвердження визначається для кожного типу операцій: реєстрації даних може вимагати підпису власника, зміна прав - власника й служби безпеки, а оновлення смартконтракту - кваліфікованої більшості організацій. Розподіл функцій між контурами системи узагальнено в табл. 1.

Таблиця 1 - Розподіл функцій кіберзахисту між контурами системи

Контур	Артефакт	Захисна функція
Дані	Шифротекст, хеш, версія	Конфіденційність і контроль цілісності
Довіра	Ідентичності вузлів, кворум	Усунення одноосібного підтвердження
Доступ	Версія політики, подія рішення	Найменші привілеї та простежуваність
Ключі	Версія, стан відкликання	Ротація, відновлення, криптознищення
Моніторинг	Події реєстру та телеметрія	Виявлення відхилень і реагування

Етап 5 - розмежування реєстрового та позареєстрового зберігання. Змістовий об'єкт перед передаванням шифрується й розміщується у зовнішньому реплікованому сховищі. До реєстру записуються ідентифікатор об'єкта, криптографічний хеш шифротексту, версія, ідентифікатор власника, посилання на політику доступу, версія ключа, час і стан життєвого циклу. Отримувач спочатку перевіряє підписи й політику, після завантаження повторно обчислює хеш, і лише тоді розшифровує дані. Практика приватних колекцій у дозвільних реєстрах підтверджує можливість передавати зміст лише уповноваженим вузлам, тоді як у загальному каналі залишається хеш для контролю цілісності [4].

Криптографічний контур. Для кожного об'єкта або логічної групи формується окремий ключ шифрування даних, який захищається ключем одержувача або домену. Закриті ключі користувачів і вузлів не зберігаються у реєстрі; для критичних ролей передбачаються апаратне захищене зберігання, багатофакторна автентифікація, ротація, резервне відновлення та журналювання використання. Відкликання доступу супроводжується зміною політики, припиненням видачі ключів і, для високого рівня ризику, повторним шифруванням актуальної версії. Видалення ключа після завершення строку обробки забезпечує криптографічне знищення позареєстрового вмісту, але не скасовує обов'язку мінімізувати метадані в реєстрі.

Етап 6 - керування доступом за принципами нульової довіри. Розташування користувача або вузла не є підставою для неявної довіри. Кожний запит повинен мати перевірену ідентичність суб'єкта і пристрою, мету операції, атрибути об'єкта, строк дії повноважень та контекст ризику [3]. Базові ролі поєднуються з атрибутними умовами, а рішення за замовчуванням є заборonoю. Смартконтракт зберігає версії політик і реєструє результат авторизації, але не отримує відкритих даних чи секретних ключів. Критичні зміни політик набувають чинності лише після багатостороннього підтвердження; аварійне блокування доступу виконується окремою обмеженою функцією з обов'язковим подальшим аудитом.

Послідовність захищеної транзакції. Власник автентифікується, формує об'єкт, шифрує його, передає шифротекст до сховища та підписує метадані. Вузли перевіряють сертифікат, актуальність політики, унікальність номера операції та відповідність хешу; після досягнення кворуму запис фіксується у реєстрі. Під час читання сервіс політик оцінює атрибути запиту, а служба ключів видає матеріал розшифрування лише для дозволеної версії. Завантаження, успішна або відхилена авторизація, зміна прав і відкликання ключа створюють

пов'язані події аудиту. Завдяки цьому можна відновити не тільки факт зміни даних, а й ланцюг рішень, що передував доступу.

Етап 7 - забезпечення стійкості. Тип відмов визначає склад групи узгодження: для збоїв без довільної поведінки потрібна більшість працездатних вузлів, а для візантійських відмов - алгоритм і кворум, розраховані на очікувану кількість скомпрометованих учасників. Вузли не повинні мати спільної точки живлення, адміністрування, резервного копіювання або служби сертифікації. Передбачаються контроль стану реплік, резервні копії конфігурації та позареєстрових даних, перевірка відновлення з контрольної точки і захищений початковий комплект довіри. Розподілений реєстр підвищує стійкість журналу, але не замінює резервування змістових даних і план безперервності. Розрахункову зміну доступності показано на рис. 1

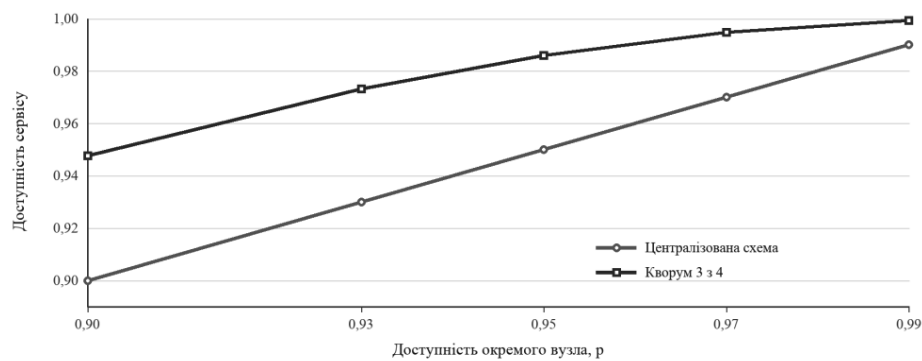


Рисунок 1 - Розрахункова доступність за незалежних відмов вузлів

Безпека смартконтрактів і змін. Логіка контракту описується як скінченний автомат із дозволеними станами об'єкта та переходами між ними. Перевіряються повнота валідації вхідних даних, розмежування функцій, детермінованість, захист від повтору, коректність часових обмежень і неможливість обходу політики через застарілу версію. Код проходить статичний аналіз, модульні й інтеграційні тести, а критичні зміни - незалежне рецензування. Версія контракту, хеш пакета та рішення органів управління фіксуються до розгортання. Механізм оновлення має включати сумісність стану, можливість призупинення операцій та план повернення до перевіреної версії.

Моніторинг і реагування. Події реєстру корелюються з телеметрією кінцевих пристроїв, мережі, сховища та служби ключів у системі керування подіями безпеки. Контролюються аномальна частота відмов авторизації, зміна складу кворуму, відставання реплік, невідповідність хешів, використання відкликаних сертифікатів і спроби звернення до неактуальних версій. Для компрометації ключа визначаються операції відкликання, перевидачі, повторного шифрування та позначення недовірених транзакцій. Відновлення управління виконується позареєстровою процедурою з кількома уповноваженими особами, щоб порушення самого механізму голосування не блокувало систему безстроково.

Інваріанти безпеки. Для формальної перевірки архітектури задається набір властивостей, які мають виконуватися для кожного допустимого стану. Активна версія об'єкта повинна мати єдиний підтверджений запис метаданих; хеш отриманого шифротексту має збігатися з реєстровим; рішення про доступ повинно посилалися на чинну версію політики; відкликаний сертифікат або ключ не може підтверджувати нову операцію; критичний перехід стану не може бути схвалений одним адміністративним доменом; кожна зміна політики повинна мати автора, час, підставу та набір підтверджень. Порушення інваріанта переводить об'єкт у стан карантину, забороняє видачу ключа та створює пріоритетну подію для розслідування.

Профіль експерименту. Прототип доцільно досліджувати у щонайменше трьох конфігураціях: штатна робота всіх вузлів, відмова одного адміністративного домену та наявність одного вузла з довільною поведінкою. Для кожної конфігурації повторюються операції реєстрації, читання, зміни прав, ротації ключа й відновлення. Окремо перевіряються малі службові записи та великі зашифровані об'єкти, адже час їх передавання не повинен помилково приписуватися механізму консенсусу. Результати фіксуються разом із версією контракту, складом вузлів, політикою підтвердження та параметрами мережі. Це забезпечує повторюваність вимірювань і дозволяє відокремити вплив реєстру від впливу зовнішнього сховища та криптографічних операцій.

Межі застосування. Запропонована схема не усуває ризик введення неправдивих даних уповноваженим джерелом, компрометації кінцевого пристрою після розшифрування, витоку через аналіз трафіку або помилки організаційного управління. Достовірність зовнішніх відомостей потребує окремого механізму атестації джерел, а секретність відкритого вмісту - захисту робочого середовища користувача. Крім того, незмінний журнал може зберігати непрямі ідентифікатори й часові кореляції, тому оцінювання приватності охоплює не лише текст запису, а й структуру зв'язків між подіями. Виявлені залишкові ризики документуються та приймаються власником системи до введення в експлуатацію.

Перевірка результативності. Апробація методики передбачає функціональні, безпекові, відмовостійкі та навантажувальні випробування. Моделюються підміна об'єкта у сховищі, несанкціонована зміна політики, компрометація одного вузла, втрата ключа, розділення мережі та відновлення після зупинки. Вимірюються

частка виявлених порушень цілісності, затримка підтвердження для 95-го перцентиля, пропускна здатність, доступність, час відкликання доступу, час відновлення, накладні витрати сховища та повнота аудиторського сліду. Показники порівнюються з централізованою базовою архітектурою за однакових обсягів даних і сценаріїв відмов; критерії приймання задаються до проведення експерименту.

Практичний результат. Методика завершується матрицею відповідності, у якій кожній загрозі зіставлено актив, контроль, відповідального учасника, подію моніторингу, тест і критерій приймання. Це робить архітектурне рішення перевірюваним та дозволяє повторно оцінювати його після зміни складу організації, платформи або криптографічних алгоритмів. Гібридне зберігання узгоджується з підходами, де реєстр використовується для незмінного аудиту й керування доступом, а великі або чутливі об'єкти залишаються у захищеному зовнішньому сховищі [5, 6]. Водночас конкретна реалізація не прив'язується до однієї блокчейн-платформи: обов'язковими є властивості, інтерфейси та докази виконання політик.

Висновки. Запропонована методика поєднує аналіз доцільності розподіленого реєстру, моделювання загроз, синтез дозвільної багатодоменної архітектури, гібридне зберігання, керування ключами, нульову довіру та перевірку стійкості. На відміну від підходу, за якого блокчейн розглядається як самодостатній засіб захисту, методика розмежує функції: реєстр забезпечує узгодженість, простежуваність і контроль версій, а конфіденційність та доступність підтримуються окремими криптографічними й інфраструктурними механізмами. Подальше дослідження передбачає створення експериментального прототипу та кількісне порівняння з централізованою архітектурою за визначеними сценаріями атак і відмов.

Література

1. Yaga D., Mell P., Roby N., Scarfone K. *Blockchain Technology Overview*. NISTIR 8202. Gaithersburg: National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.IR.8202.
2. Hu V. C. *Blockchain for Access Control Systems*. NISTIR 8403. Gaithersburg: National Institute of Standards and Technology, 2022. DOI: 10.6028/NIST.IR.8403.
3. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-207.
4. Hyperledger Fabric Docs. *Using Private Data in Fabric*. URL: https://hyperledger-fabric.readthedocs.io/en/latest/private_data_tutorial.html (accessed: 15.08.2026).
5. European Union Agency for Network and Information Security. *Distributed Ledger Technology & Cybersecurity: Improving Information Security in the Financial Sector*. Heraklion: ENISA, 2017.
6. Banerjee J., Dhoundiyal S., Ghosh M., Raj R., Wary A. et al. *Dashdikpala: A Blockchain-Enabled Lattice Based Access Control Scheme for Digital Evidence Data Protection* // Peer-to-Peer Networking and Applications. 2026. Vol. 19. Art. 46. DOI: 10.1007/s12083-025-02179-2.

УДК 004.75:004.052.3

¹Царьов Р.Ю., ¹Квачук В.О., ²Онотяк Ю.В., ¹Царьова Г. А.

АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ СЕРВІСНИХ ПЛАТФОРМ НАДАННЯ ВЕБСЕРВІСІВ ЗА СКЛАДОВИМИ ПОКАЗНИКА НЕДОСТУПНОСТІ

¹Державний університет інтелектуальних технологій і зв’язку

²Національний університет "Львівська політехніка"

r-y.tsarov@suitt.edu.ua

Анотація. Розглянуто задачу вибору кратності резервування сервісної платформи надання вебсервісів. Показник недоступності розкладено на три складові: дефіцит ємності за незалежних відмов екземплярів, відмови зі спільною причиною та запізнення виявлення відмови з перемиканням. Кожній складовій зіставлено методи, які на нього діють. Сформульовано критерій вибору кратності, що поєднує ємнісне обмеження з умовою співмірності незалежної та спільної складових, проведено верифікацію ефективності використання сформульованих критеріїв для забезпечення надійності функціонування сервісних платформ.

Ключові слова: сервісна платформа, вебсервіс, готовність, недоступність, кратність резервування, спільна відмова, β-фактор, контроль стану.

Кратність резервування сервісної платформи обґрунтовують коефіцієнтом готовності, розрахованим за схемою «k з n» з припущенням незалежності відмов екземплярів. Результат такого розрахунку зручний: кожна додана репліка зменшує ймовірність відмови на порядок і більше, а межі нарощування модель не має. Експлуатаційна практика цьому не відповідає. Платформи з десятками і більше репліками не показують готовності, яку обіцяє модель, тому додані репліки оплачують ємністю, не одержуючи розрахованого виграшу.

Поза розрахунком лишається питання, за якої кратності приріст готовності припиняється і що саме після цього залишається джерелом простою.

Надійність програмних систем нормовано в ISO/IEC 25010 [1] як характеристику якості, процедури розрахунку показників стандарт не задає. Терміни та показники доступності визначено Рекомендацією ITU-T E.800 [2], структурні моделі надійності – стандартом IEC 61078 [3]. Обидва документи оперують блоками, відмови яких вважають незалежними. Метод β-фактора, що описує частку відмов зі спільною причиною, стандартизовано в IEC 61508-6 [4] для систем функційної безпеки і у проєктуванні вебплатформ він застосовують рідко. Настанови з експлуатації [5] розглядають балансування навантаження з активним контролем стану екземплярів, та шаблони стійкості до перевантаження, передусім автоматичний відключення (circuit breaker) і тайм-аути викликів [6]. Узагальнення повідомлень про відмови хмарних сервісів [7] показує, що помітну частку становлять події, які стосуються кількох екземплярів одночасно, тобто саме ті, що лежать поза моделлю незалежних відмов.

Мета роботи полягає в тому, щоб розкласти показник недоступності платформи на складові за механізмом їх виникнення, зіставити з кожною складовою методи, які на неї діють, і за цим розкладом визначити верхню межу корисної кратності резервування. Числові значення нижче одержано розрахунком за явно заданими припущеннями; вимірювань на діючій платформі не проводилося.

Зіставлення методів зі складовими недоступності наведено в таблиці 1. Метод віднесено до складової тоді, коли він змінює параметр, від якого відповідна складова залежить безпосередньо. Три перші рядки табл.1 підтверджують наше припущення: методи не є взаємозамінними, і відсутність одного з них не компенсується нарощуванням іншого.

Таблиця 1 – Методи забезпечення надійності та складові недоступності, на які вони діють			
Метод	Складова, на яку діє	Керований параметр	Складові, що не змінюються
Реплікація в межах одного домену відмов	Q ₁ , дефіцит ємності за незалежних відмов	n	Q ₂ , Q ₃
Рознесення реплік за доменами відмов	Q ₂ , відмови зі спільною причиною	β	Q ₃ , витрати ємності
Активний контроль стану екземплярів	Q ₃ , час виявлення	I, m	Q ₁ , Q ₂
Виведення екземпляра з ротації, повтори запитів	Q ₃ , час перемикання	Tп	Q ₁ , Q ₂
Автоматичне відключення, обмеження швидкості (інтенсивності запитів)	Глибина деградації за дефіциту ємності	Пороги, тайм-аути	Частота відмов екземплярів
Запас ємності за коефіцієнтом використання	Тривалість дефіциту після перерозподілу	ρ*	Q ₂ , Q ₃

Недоступність окремого екземпляра визначимо через інтенсивність відмов та середній час відновлення:

$$U = \lambda \cdot Tв / 8760, \tag{1}$$

де λ – кількість відмов екземпляра за рік; Tв – середній час відновлення, год. Прийmemo λ = 4 рік⁻¹ і Tв = 1 год, звідки U = 4,57·10⁻⁴. Мінімальну кількість справних реплік задає навантаження, а не надійність:

$$k = \lceil L / (\rho^* \cdot c) \rceil, \tag{2}$$

де L – сумарна інтенсивність запитів; c – продуктивність одного екземпляра; ρ* – гранично допустимий коефіцієнт використання, за якого затримка ще вкладається в норму. Значення ρ* обмежене зверху не пропускною здатністю, а хвостом розподілу затримки, який за використання понад 0,8 зростає швидше за середнє [8]. За L/c = 4,8 і ρ* = 0,8 маємо k = 6.

Дефіцит ємності настає, коли справних реплік менше за k. Ймовірність цього стану за незалежних відмов:

$$Q_1(n) = \sum C(n, j) \cdot u^j \cdot (1 - u)^{n-j}, \quad j = n - k + 1, \dots, n, \tag{3}$$

де u = (1 - β) · U. Відмови, спричинені однією подією для всіх реплік одразу, дає помилкове розгортання, вичерпання спільного ресурсу або втрата живлення стійки. Їхній внесок виразимо через β-фактор [4]:

$$Q_2 = \beta \cdot U. \tag{4}$$

Величина Q₂ від кількості реплік не залежить узагалі – подія з визначення стосується всіх екземплярів домену. Результати розрахунку за виразами (3) і (4) для β = 0,05 наведено в таблиці 2.

Таблиця 2 – Складові недоступності платформи за різної кратності резервування, k = 6					
n	Резерв ємності, %	ρ за нормального режиму	Q ₁ , хв/рік	Q ₂ , хв/рік	Разом із Q ₃ , хв/рік
6	0	0,800	1366,5	12,0	1379,7
7	14,3	0,686	2,07	12,0	15,24
8	25,0	0,600	2,4·10 ⁻³	12,0	13,17
9	33,3	0,533	2,3·10 ⁻⁶	12,0	13,17
10	40,0	0,480	2,0·10 ⁻⁹	12,0	13,17
12	50,0	0,400	1,2·10 ⁻¹⁵	12,0	13,17

Перехід від n = 7 до n = 8 зменшує незалежну складову з 2,07 до 2,4·10⁻³ хв/рік, тобто майже на три порядки, а сумарну недоступність – з 15,24 до 13,17 хв/рік, тобто на 13,6 %. Далі зміни немає. Кратність понад вісім не змінює сумарного значення в межах першої значущої цифри, тоді як резерв ємності зростає з 25 до 50 %. Уже за n = 7 спільна складова перевищує незалежну в 5,8 раза, і саме вона визначає результат.

Стрибок між n = 7 і n = 8 має структурну природу. За семи реплік платформа витримує одну відмову, за восьми – дві, і показник змінюється разом з цією величиною, а не плавно з кратністю. Вибір кратності тому зводиться до вибору допустимої кількості одночасних відмов, а не до підбору n за неперервною кривою.

Третій складник пов’язаний із запізненням реакції. Поки відмову екземпляра не виявлено, балансувальник надсилає на нього частку 1/n запитів, а кількість таких подій за рік дорівнює n·λ, тому добуток від кратності не залежить:

$$Q_3 = \lambda \cdot (Tд + Tп) / 3,15 \cdot 10^7, \quad Tд = I \cdot (m - 0,5), \tag{5}$$

де I – інтервал активного контролю стану, с; m – поріг послідовних невдалих проб; Tд – середній час виявлення; Tп – час перемикання з дренажем з’єднань, прийнятий 5 с. Розрахунок для типових значень I та m подано в таблиці 3; частоту хибного вилучення справної репліки обчислено за ймовірності втрати окремої проби 0,01.

Скорочення порогу з трьох проб до двох за I = 5 с зменшує Q₃ на 0,34 хв/рік, а частоту хибних вилучень збільшує з 6,3 до 631 випадку на рік. Кожне хибне вилучення на час до повернення репліки підвищує навантаження решти, і за n, близького до k, воно наближає платформу до того самого дефіциту ємності, від якого захищає резервування. Виграш у 0,34 хв/рік такої ціни не виправдовує. Заміна ж інтервалу з 30 на 5 с дає 4,16 хв/рік і не має побічного ефекту, доки поріг лишається рівним трьом.

Таблиця 3 – Вплив параметрів контролю стану на складову Q ₃				
Інтервал I, с	Поріг m	Tд + Tп, с	Q ₃ , хв/рік	Хибних вилучень за рік
2	2	8,0	0,53	1577
2	3	10,0	0,67	15,8
5	2	12,5	0,83	631
5	3	17,5	1,17	6,3
10	3	30,0	2,00	3,2
30	3	80,0	5,33	1,1

Сумарну недоступність залежно від кратності для трьох значень β подано на рисунку 1. Криві мають однаковий вигляд: різкий спад до n = 8 і горизонтальна ділянка далі. Рівень цієї ділянки задає тільки β і становить 25,2; 13,2 та 3,6 хв/рік. Рознесення реплік за незалежними доменами відмов зміщує криву вниз, збільшення їх кількості в межах одного домену – ні.

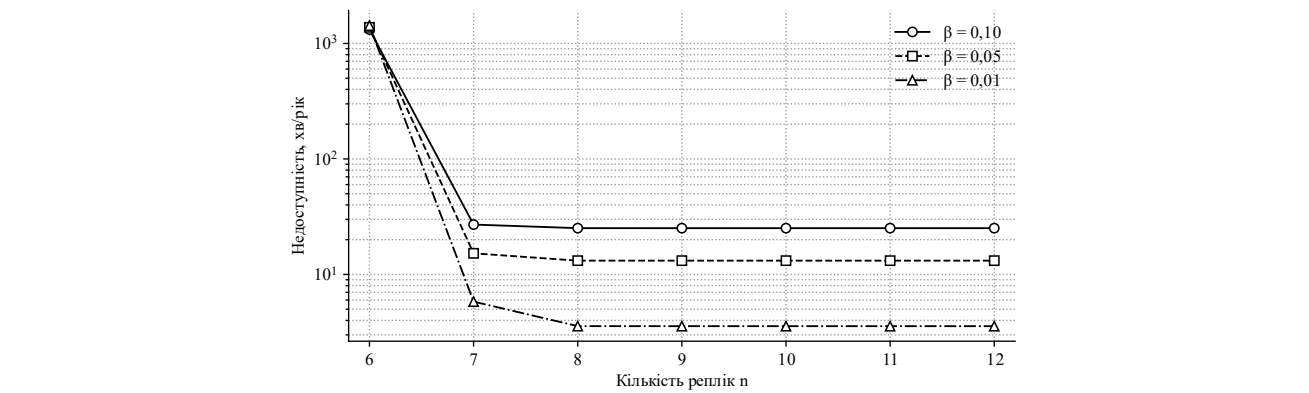


Рисунок 1 – Розрахункова недоступність платформи залежно від кількості реплік для трьох значень частки відмов зі спільною причиною

Розклад дає критерій вибору кратності. Достатніми є дві умови: платформа витримує t одночасних відмов без виходу за ρ*, а незалежна складова не перевищує спільної, тобто n - t ≥ k і Q₁(n) ≤ Q₂. Для прийнятих

даних обидві виконуються за $n = 7$ і $t = 1$, бо $2,07 < 12,0$ хв/рік. Модель без урахування спільних відмов на тому самому вихідному матеріалі вимагає $n = 8$, оскільки цільове значення 1 хв/рік за $n = 7$ не досягається. Різниця в одну репліку коштує 10,7 % пункту резерву ємності, а виграш становить лише 2,07 хв/рік при загальному рівні 13,2 хв/рік.

Методи з двох нижніх рядків таблиці 1 не діють на жодну із трьох складових: вони змінюють наслідки дефіциту ємності, а не його ймовірність. За $n = 7$ і відмови однієї репліки коефіцієнт використання решти зростає з 0,686 до 0,800, тобто рівно до межі ρ^* . За $n = 6$ резерву немає, використання перевищило б одиницю, і черга зростала б до вичерпання клієнтського тайм-ауту. Обмеження швидкості з відкиданням надлишку переводить цей стан у відмову частини запитів замість відмови всіх, а автоматичне відключення [6] знімає навантаження із залежних сервісів. У підсумковий показник такі методи входять через частку запитів, утрачених у події, а не через частоту самої події.

Для практичного застосування критерію потрібні чотири величини: λ і T_v з журналу експлуатації, k з навантажувального випробування одного екземпляра та β з класифікації інцидентів за причинами. Перші три звичайно доступні. Саме брак четвертої змушує проєктувальника лишатися в межах моделі незалежних відмов і компенсувати невизначеність кратністю, хоча за наведеним розкладом кратність цієї невизначеності не знімає.

Наукова новизна одержаних результатів полягає в тому, що показник недоступності сервісної платформи розкладено на складові за механізмом виникнення і кожній складовій зіставлено метод, який на неї діє, після чого верхню межу корисної кратності резервування визначено з умови співмірності незалежної та спільної складових. Відомі підходи виводять кратність з моделі незалежних відмов [3, 9] і такої межі не мають, тому дають завищену оцінку потрібної кількості реплік.

Одержані результати обмежені такими умовами – розрахунок стосується платформи з однорідними екземплярами за одним балансувальником. Конфігурації з розділенням трафіку за сегментами потребують окремого розгляду. Значення β взято зі стандартного діапазону 0,01–0,10 [4], а не виміряно (для вимірювання потрібен облік інцидентів з розділенням за причинами, чого звичайні журнали не дають). Відмови балансувальника і спільного сховища утворюють окрему послідовну ланку і в модель не входять. Тривалість завершення з’єднань узято сталою, хоча для довгих сесій вона зростає.

Висновки. Недоступність сервісної платформи складається зі складових, на які діють різні методи, і нарощування кратності резервування впливає лише на одну з них. За прийнятих вихідних даних незалежна складова падає з 1366,5 до $2,4 \cdot 10^{-3}$ хв/рік при зміні кратності з шести до восьми реплік, після чого сумарне значення 13,2 хв/рік визначається спільною складовою 12,0 хв/рік і складовою виявлення 1,17 хв/рік, які від кратності не залежать. Кожна репліка понад восьму додає резерв ємності і не змінює розрахункового простору. Спільну складову зменшує лише рознесення реплік за незалежними доменами відмов: перехід від $\beta = 0,05$ до $\beta = 0,01$ знижує сумарну недоступність з 13,2 до 3,6 хв/рік, чого нарощуванням реплік не досягти за жодної кратності. Складова виявлення керується параметрами контролю стану, причому зменшення порогу з трьох проб до двох дає 0,34 хв/рік виграшу ціною стократного зростання частоти хибних вилучень справних реплік, тому прийнятним способом її скорочення лишається зменшення інтервалу опитування. Критерій, що поєднує ємнісне обмеження $n - t \geq k$ з умовою $Q_1(n) \leq Q_2$, дає для розглянутого прикладу сім реплік проти восьми за моделлю незалежних відмов, тобто 14,3 % резерву ємності замість 25,0 %.

Література

- ISO/IEC 25010:2023. Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). Product quality model. Geneva : ISO, 2023.
- ITU-T Recommendation E.800. Definitions of terms related to quality of service. Geneva : ITU-T, 2008.
- IEC 61078:2016. Reliability block diagrams. Geneva : IEC, 2016.
- IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. Geneva : IEC, 2010.
- Beyer B., Jones C., Petoff J., Murphy N. R. Site Reliability Engineering: How Google Runs Production Systems. Sebastopol : O’Reilly Media, 2016.
- Nygard M. T. Release It! Design and Deploy Production-Ready Software. 2nd ed. Raleigh : Pragmatic Bookshelf, 2018.
- Gunawi H. S., Hao M., Suminto R. O. et al. Why does the cloud stop computing? Lessons from hundreds of service outages. Proceedings of the 7th ACM Symposium on Cloud Computing (SoCC ’16). Santa Clara, 2016. P. 1–16.
- Dean J., Barroso L. A. The tail at scale. Communications of the ACM. 2013. Vol. 56, no. 2. P. 74–80.
- Trivedi K. S., Bobbio A. Reliability and Availability Engineering: Modeling, Analysis, and Applications. Cambridge : Cambridge University Press, 2017.

УДК 004.732:004.94

Царьов Р.Ю.
Коваленко І.О.
Андрухів Т.В.

КРИТЕРІЙ ДОЦІЛЬНОСТІ РЕКОНСТРУКЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ

Державний університет інтелектуальних технологій і зв’язку
r-y.tsarov@suitt.edu.ua

Анотація. Розглянуто задачу обґрунтування переходу корпоративної мережі на віртуалізовану інфраструктуру з накладеною мережею. Прийняте в проєктній практиці визначення розмірності за агрегованою смугою не враховує накладних витрат інкапсуляції, величина яких залежить від довжини пакета: за $L = 64$ Б втрата корисної пропускної здатності для VXLAN над IPv4 становить 32,9 %, за $L = 1450$ Б лише 3,3 %. Побудовано критерій вибору коефіцієнта консолідації, що пов’язує розподіл довжин пакетів з ємністю висхідного каналу вузла. Для двох профілів трафіку з однаковою агрегованою смугою гранична кількість сервісів на вузлі відрізняється на 27 %. Розділено складові приросту доступності: приріст дає механізм Perezanysky в кластері, тоді як консолідація змінює лише ймовірність дефіциту ємності.

Ключові слова: корпоративна мережа, віртуалізація, NFV, VXLAN, накладна мережа, коефіцієнт консолідації, доступність, довжина пакета.

Проєктні рішення щодо реконструкції корпоративної мережі обґрунтовують двома величинами: кількістю фізичних серверів, які вдається згорнути на один вузол, та агрегованою смугою каналів. Обидві описують ємність. Жодна не показує, у що обходиться сам перехід до накладної мережі, хоча інкапсуляція додає до кожного кадру сталу кількість байтів незалежно від його довжини. Звідси й питання, яке лишається поза розрахунком: за яких характеристик трафіку канал, розрахований за смугою до реконструкції, не витримає того самого навантаження після неї.

Архітектурну рамку віртуалізації мережевих функцій задано в ETSI GS NFV 002 [1], модель програмно керованої мережі описано Рекомендацією ITU-T Y.3300 [2]. Обидва документи визначають структуру та інтерфейси, показників навантаження не нормують. Огляд задач розміщення віртуальних мережевих функцій [3] зводить відомі постановки до мінімізації вартості або затримки, причому трафік у них подано інтенсивністю потоку. Розподіл довжин пакетів у цільові функції не входить. Для накладних мереж таке спрощення втрачає силу, оскільки витрати інкапсуляції за RFC 7348 [4] стали в байтах на кадр, а не в частці смуги.

Мета роботи полягає в тому, щоб виразити накладні витрати накладної мережі як функцію довжини пакета і за цією функцією визначити верхню межу коефіцієнта консолідації вузла. Довжини заголовків беруться зі специфікацій, а не добираються з інженерних міркувань; параметри трафіку та відмов задано явно як вихідні припущення.

Склад накладних витрат для чотирьох поширених схем зведено в таблиці 1. Рішення EVPN/VXLAN [5] змінює сигнальну площину, довжину заголовка воно не змінює, тому окремим рядком не подане. Geneve [6] у базовому варіанті збігається з VXLAN, проте допускає до 252 байтів опцій, і за їх використання витрати зростають. Складова ESP у тунельному режимі містить заголовок 8 Б, вектор ініціалізації 8 Б, поле контролю цілісності 16 Б, трейлер 2 Б і зовнішній заголовок IP 20 Б [7].

Таблиця 1 – Накладні витрати інкапсуляції на один кадр, байт

Схема інкапсуляції	Зовн. Ethernet	Зовн. IP	UDP	Заголовок VXLAN / Geneve	ESP	Разом h
VXLAN над IPv4	14	20	8	8	–	50
VXLAN над IPv6	14	40	8	8	–	70
Geneve над IPv4, без опцій	14	20	8	8	–	50
VXLAN над IPv4 всередині ESP	14	20	8	8	54	104

Відносну корисну пропускну здатність визначимо як частку часу зайняття середовища, витрачену на початковий кадр, за незмінної швидкості інтерфейсу:

$$v(L) = (L + 38) / (L + 38 + h), \quad (1)$$

де L – довжина пакета IP, байт; h – витрати інкапсуляції з таблиці 1; 38 байтів охоплюють заголовок Ethernet (14), контрольну послідовність (4), преамбулу з обмежувачем (8) та міжкадровий інтервал (12) [8]. За наявності тегу 802.1Q константа зростає до 42, що на висновки не впливає. Результати обчислення за виразом (1) наведено в таблиці 2.

Таблиця 2 – Відносна корисна пропускна здатність накладної мережі				
Довжина пакета L, Б	v за h = 50, %	v за h = 70, %	v за h = 104, %	Потрібний приріст смуги за h = 50, %
64	67,1	59,3	49,5	49,0
128	76,9	70,3	61,5	30,1
256	85,5	80,8	73,9	17,0
512	91,7	88,7	84,1	9,1
1024	95,5	93,8	91,1	4,7
1450	96,7	95,5	93,5	3,4

Розкид значень у крайніх рядках таблиці 2 сягає п'ятнадцяти разів за однієї й тієї самої схеми інкапсуляції. Канал, що до реконструкції передавав потік із пакетів по 64 байти, після ввімкнення VXLAN потребує на 49 % більшої смуги, тоді як для потоку з пакетів по 1450 байтів приріст становить 3,4 %. Швидкість інтерфейсу в цю оцінку не входить, тому перехід з 10 на 25 Гбіт/с співвідношення не змінює. Загальний вигляд залежності подано на рисунку 1: усі три криві мають ділянку різкого спаду ліворуч від 256 байтів і виположуються після 700 байтів.

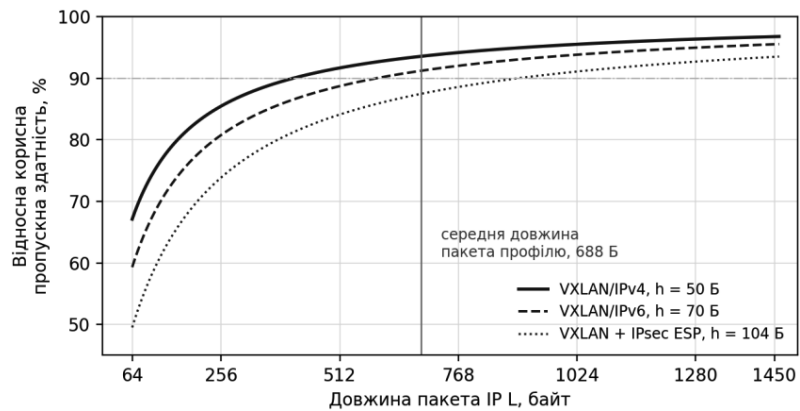


Рисунок 1 – Відносна корисна пропускна здатність залежно від довжини пакета для трьох схем інкапсуляції

Практичний наслідок стосується вибору коефіцієнта консолідації k, тобто кількості сервісів на одному вузлі. Навантаження висхідного каналу вузла з урахуванням інкапсуляції обмежене зверху:

$$k \leq \rho \cdot C / (r \cdot (1 + h / (\bar{L} + 38))), \tag{2}$$

де C – ємність висхідного каналу; ρ – допустимий коефіцієнт використання; r – середня швидкість одного сервісу; $\bar{L}$ – середня довжина пакета. Візьмемо C = 10 Гбіт/с, ρ = 0,6, r = 0,4 Гбіт/с і два профілі з однаковою агрегованою смугою. Змішаний профіль: половина пакетів по 100 Б, десята частина по 576 Б, решта по 1450 Б, звідки $\bar{L}$ = 688 Б. Сигнально-голосовий профіль: $\bar{L}$ = 100 Б. За виразом (2) перший профіль дає $k \leq 14,0$, другий лише $k \leq 11,0$. Різниця в 27 % виникає між конфігураціями, які за агрегованою смугою нерозрізненні.

Другий бік того самого обмеження стосується кількості пакетів за секунду. Змішаний профіль за повного завантаження каналу 10 Гбіт/с дає 1,61 млн пакетів/с і бюджет 621 нс на пакет, сигнально-голосовий – 6,65 млн пакетів/с і 150 нс, що на частоті 2,5 ГГц відповідає 376 тактам ядра на пакет. Такий бюджет мережевий стек загального призначення не витримує, потрібні закріплення ядер, великі сторінки пам'яті та прямий доступ до черг адаптера [9]. Вимірювання програмних комутаторів [10] і механізмів обходу стека ядра [11] показують, що вартість оброблення визначається числом пакетів, а не числом байтів у них.

Другу складову критерію дає доступність. Простій сервісу в кластері з перезапуском віртуальних машин на справному вузлі становить

$$D = (U \cdot 8760 / MTTR) \cdot T_p, \tag{3}$$

де U – коефіцієнт неготовності вузла; MTTR – середній час відновлення, год; T_p – тривалість перезапуску. За U = 10^{-3} , MTTR = 4 год і T_p = 5 хв частота відмов вузла становить 2,19 на рік, а простій сервісу 11,0 хв/рік проти 525,6 хв/рік для окремого фізичного сервера без резервування. Величина не залежить від k. Залежність від k виявляється в іншому: за схеми резервування N + 1 одночасна відмова двох вузлів залишає кластер без ємності, і ймовірність P₂ такої події зростає з кількістю вузлів M. Розрахунок для 24 сервісів наведено в таблиці 3.

Таблиця 3 – Простій сервісу та резерв ємності за різних коефіцієнтів консолідації						
Варіант розміщення	k	Вузлів M	Резерв ємності, %	P ₂	Простій від перезапуску, хв/рік	Простій від дефіциту ємності, хв/рік
Фізичні сервери, без НА	1	24	–	–	525,6	–
Віртуалізація, НА	1	25	4,0	$3,0 \cdot 10^{-4}$	11,0	155,3
Віртуалізація, НА	4	7	14,3	$2,1 \cdot 10^{-5}$	11,0	11,0
Віртуалізація, НА	8	4	25,0	$6,0 \cdot 10^{-6}$	11,0	3,1
Віртуалізація, НА	12	3	33,3	$3,0 \cdot 10^{-6}$	11,0	1,6

Таблиця 3 дає результат, зворотний до звичного уявлення про блоковий радіус ураження. Зростання k зменшує сумарний простій зі 166,3 до 12,5 хв/рік, оскільки кластер із трьох вузлів рідше опиняється у стані подвійної відмови, ніж кластер із двадцяти п'яти. Плата за це – частка резерву, яка за k = 12 сягає третини всієї ємності. Разом з обмеженням (2) виникає суперечність: доступність тягне k вгору, канал тримає його вниз. Для змішаного профілю область сумісних значень існує, k = 12 вкладається в межу 14,0. Для сигнально-голосового профілю межа дорівнює 11,0, і значення k = 12 недосяжне без агрегування каналів або переходу на 25 Гбіт/с.

Наукова новизна одержаних результатів полягає в тому, що критерій доцільності реконструкції корпоративної мережі доповнено обмеженням, яке враховує розподіл довжин пакетів через нормовану величину $h / (\bar{L} + 38)$, тоді як відомі підходи оперують агрегованою смугою і до цієї величини нечутливі. Це дає верхню межу коефіцієнта консолідації, обчислювану до початку робіт. Додатково розділено внески перезапуску в кластері та власне консолідації у приріст доступності: перший дає скорочення простою в 47 разів, другий впливає лише на ймовірність дефіциту ємності й на частку резерву.

Межі застосовності окреслимо прямо. Розрахунок стосується сталої частини накладних витрат і не враховує затримки програмного комутатора, яка залежить від реалізації та конфігурації вузла. Профілі трафіку взято як вихідні припущення, а не як результат вимірювань на діючій мережі підприємства. Модель доступності припускає незалежність відмов вузлів, що не виконується за спільного введення живлення або спільної системи зберігання. Перехід на MTU 9000 у транспортній мережі знімає більшу частину втрат за виразом (1), проте потребує узгодженого значення на всьому шляху, включно з каналами до філій.

Висновки. Витрати накладної мережі визначаються довжиною пакета, а не швидкістю інтерфейсу: за VXLAN над IPv4 втрата корисної пропускної здатності змінюється від 32,9 % за 64 Б до 3,3 % за 1450 Б, і перехід на швидший інтерфейс цього співвідношення не змінює. Два профілі трафіку з однаковою агрегованою смугою допускають різну кількість сервісів на вузлі, 14 проти 11 за прийнятих вихідних даних, тому визначення розмірності лише за смугою дає завищену оцінку для потоків з короткими пакетами. Приріст доступності після реконструкції створює механізм перезапуску в кластері, який скорочує простій з 525,6 до 11,0 хв/рік; коефіцієнт консолідації на цю величину не впливає і визначає лише ймовірність дефіциту ємності та частку резерву. Область сумісних значень k, обмежена зверху виразом (2) і знизу вимогою до доступності, для сигнально-голосового профілю порожня за ємності висхідного каналу 10 Гбіт/с, що й задає вихідну умову для проектування транспортної частини мережі.

Література

- ETSI GS NFV 002 V1.2.1. Network Functions Virtualisation (NFV); Architectural Framework. Sophia Antipolis : ETSI, 2014. 21 p.
- Framework of software-defined networking : Recommendation ITU-T Y.3300. Geneva : ITU, 2014. 18 p.
- Mijumbi R., Serrat J., Gorricho J.-L., Bouten N., De Turck F., Boutaba R. Network Function Virtualization: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials. 2016. Vol. 18, No. 1. P. 236–262. DOI: 10.1109/COMST.2015.2477041.
- Mahalingam M., Dutt D., Duda K., Agarwal P., Kreeger L., Sridhar T., Bursell M., Wright C. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks : RFC 7348. IETF, 2014. DOI: 10.17487/RFC7348.
- Sajassi A., Drake J., Bitar N., Shekhar R., Uttaro J., Henderickx W. A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN) : RFC 8365. IETF, 2018. DOI: 10.17487/RFC8365.
- Gross J., Ganga I., Sridhar T. Geneve: Generic Network Virtualization Encapsulation : RFC 8926. IETF, 2020. DOI: 10.17487/RFC8926.
- Kent S. IP Encapsulating Security Payload (ESP) : RFC 4303. IETF, 2005. DOI: 10.17487/RFC4303.
- IEEE Std 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks. New York : IEEE, 2022.
- ETSI GS NFV-PER 001 V1.1.2. Network Functions Virtualisation (NFV); NFV Performance & Portability Best Practises. Sophia Antipolis : ETSI, 2014. 66 p.
- Pfaff B., Pettit J., Koponen T. et al. The Design and Implementation of Open vSwitch. 12th USENIX Symposium on Networked Systems Design and Implementation (NSDI '15) : proceedings. Oakland, 2015. P. 117–130.
- Rizzo L. netmap: A Novel Framework for Fast Packet I/O. USENIX Annual Technical Conference : proceedings. Boston, 2012. P. 101–112.

АНАЛІЗ CTF-ЗАВДАНЬ

Державний університет інтелектуальних технологій і зв’язку
alexanderlie2q@gmail.com

Анотація. Виконано систематизацію підходів до аналізу завдань Capture the Flag (CTF) та технічних write-up’ів як джерела відтворюваних практичних знань з кібербезпеки. Розглянуто основні категорії завдань: web, pwn/binary exploitation, reverse engineering, cryptography, forensics, steganography та misc. Запропоновано єдину схему аналізу «артефакт - первинне спостереження - гіпотеза - контрольований експеримент - exploit/solver - flag - root cause - рекомендації», а також критерії порівняння складності й якості write-up’ів. Узагальнено типовий інструментарій і вимоги до відтворюваності рішень.

Ключові слова: CTF, Capture the Flag, write-up, кібербезпека, web security, binary exploitation, reverse engineering, cryptography, digital forensics, відтворюваність.

Змагання Capture the Flag є практичною формою перевірки навичок аналізу вразливостей, реверс-інжинірингу, криптоаналізу та цифрової криміналістики. На відміну від теоретичного опису окремої технології, CTF-завдання задає конкретний артефакт або сервіс, обмежену умову успіху та потребує побудови перевірюваного ланцюжка дій до отримання flag. Після завершення змагання write-up фіксує цей ланцюжок і може використовуватися не лише як інструкція, а і як матеріал для порівняльного аналізу методів розв’язання.

Таблиця 1 – Класифікація основних категорій CTF-завдань

№	Категорія	Типові задачі та вразливості	Основні інструменти та підхід
1	Web	Порушення контролю доступу (IDOR/BOLA), SQL/NoSQL injection, XSS, SSTI, SSRF, помилки JWT/OAuth, небезпечне завантаження файлів, вразливості бізнес-логіки.	Burp Suite Repeater/Intruder, curl, методичні підходи OWASP Web Security Testing Guide [1; 2].
2	Pwn / Binary Exploitation	Stack/heap corruption, format string, information leak, ret2libc, ROP/SROP, обхід захисних механізмів.	Pwntools для роботи з ELF, ROP, cyclic-послідовностями та процесами; GDB для аналізу регістрів, стеку, пам’яті й control flow [3; 4].
3	Reverse Engineering	Відновлення алгоритму програми без вихідного коду, аналіз рядків, імпортів, графа керування, декомпіляції та динамічної поведінки.	Ghidra та GDB. Результати декомпіляції використовуються як робоча гіпотеза та перевіряються під час виконання програми [4; 5].
4	Cryptography	XOR, повторне використання nonce/keystream, помилки параметрів RSA, слабкі генератори випадкових чисел, модульна арифметика, алгебраїчні залежності.	Python, SageMath, PyCryptodome. У write-up важливо наводити не лише solver, а й математичне пояснення використаної властивості [6].
5	Forensics	Аналіз PCAP, дампів пам’яті, файлових образів, журналів і метаданих.	TShark/Wireshark для аналізу та відновлення мережевих потоків; Volatility 3 для дослідження процесів, командних рядків, мережевих з’єднань і файлових об’єктів [7; 8].
6	Steganography	Пошук прихованих даних у метаданих, структурі файлів, доданих архівах, бітових площинах і каналах зображення.	file, ExifTool, Binwalk, zsteg; перевірка LSB/MSB, каналів і порядку їх обробки [9].
7	Misc	Багатошарові кодування, нестандартні формати, протокольні головоломки, автоматизація перетворень, AI/LLM-орієнтовані сценарії.	Поетапна перевірка кожного перетворення та чітке розмежування кодування, обфускації та криптографічного захисту.

Незалежно від категорії, аналіз доцільно виконувати за однаковою дослідницькою схемою. Спочатку фіксуються вхідні артефакти, їхні хеші та середовище виконання. Далі проводиться пасивний первинний аналіз, формулюється конкретна гіпотеза і виконується мінімальний експеримент, який має її підтвердити або спростувати. Після отримання експлуатаційного примітиву рішення автоматизується у вигляді exploit.py, solve.py або відтворюваного набору запитів. Завершальними етапами є отримання flag, пояснення першопричини (root cause) та формулювання захисних заходів. Такий підхід відділяє фактичні спостереження від інтерпретації і робить write-up придатним для повторної перевірки.

Для порівняння складності CTF-завдань недостатньо лише суб’єктивної позначки easy/medium/hard. Доцільно враховувати кількість незалежних примітивів, необхідність інформаційного витoku, обходу mitigations, відновлення параметрів, обсяг автоматизації, чутливість до версій бібліотек і кількість припущень про середовище. Якщо організатор публікує статистику, додатковими емпіричними показниками можуть бути частка команд, що розв’язали задачу, та час до першого/медіанного solve. Такі метрики слід трактувати в контексті конкретного змагання, оскільки вони залежать від складу учасників і доступного часу.

Окреме значення має якість write-up. Слабкий опис часто зводиться до переліку команд або готового payload без пояснення, чому він працює. Відтворюваний write-up повинен містити: умову й категорію задачі; опис артефактів; інструменти та суттєві версії; baseline-стан; ключове спостереження; доказ наявності уразливості або математичного механізму; мінімальний PoC; фактичний output із flag; пояснення root cause; рекомендації щодо усунення; а для binary/forensics - значення offset, адрес, PID, stream ID або інших констант і спосіб їх отримання. Класичні роботи зі stack smashing та return-oriented programming показують, що освітня цінність технічного матеріалу виникає саме з пояснення механізму, а не з демонстрації кінцевого результату [10].

Висновки. Аналіз CTF-завдань дає можливість систематизувати практичні методи кібербезпеки за повторюваними примітивами, інструментами та етапами перевірки. Найбільш корисним є не накопичення окремих payload’ів, а фіксація причинно-наслідкового ланцюжка від первинного артефакту до підтвердженого результату. Для підвищення якості такого аналізу доцільно використовувати єдину структуру write-up для різних категорій задач, чітко відокремлювати спостереження, гіпотезу, експеримент і висновок, щоб уникати неперевіраних припущень, а також документувати версії інструментів, хеші артефактів і всі константи, від яких залежить PoC. Складність завдань доцільно оцінювати за кількістю та взаємозалежністю використаних примітивів, а не лише за суб’єктивним рівнем складності. Завершення технічного опису поясненням першопричини вразливості та відповідними захисними заходами дає змогу перетворити CTF-рішення на відтворюваний і практично корисний навчальний матеріал.

Література

1. OWASP Foundation. Web Security Testing Guide (WSTG). URL: <https://owasp.org/www-project-web-security-testing-guide/> (дата звернення: 15.08.2026).

2. PortSwigger. Burp Suite Documentation: Repeater and Intruder; Web Security Academy. URL: <https://portswigger.net/burp/documentation> ; <https://portswigger.net/web-security> (дата звернення: 15.08.2026).

3. Pwntools Documentation 4.15.0. CTF framework and exploit development library. URL: <https://docs.pwntools.com/en/stable/> (дата звернення: 15.08.2026).

4. GNU Project. Debugging with GDB. URL: <https://sourceware.org/gdb/current/onlinedocs/gdb> (дата звернення: 15.08.2026).

5. National Security Agency. Ghidra API Documentation. URL: https://ghidra.re/ghidra_docs/api/index.html (дата звернення: 15.08.2026).

6. PyCryptodome Documentation. RSA; AES. URL: https://pycryptodome.readthedocs.io/en/latest/src/public_key/rsa.html ; <https://pycryptodome.readthedocs.io/en/latest/src/cipher/aes.html> (дата звернення: 15.08.2026).

7. Wireshark Foundation. TShark Manual Page. URL: <https://www.wireshark.org/docs/man-pages/tshark.html> (дата звернення: 15.08.2026).

8. Volatility Foundation. Volatility 3 Windows Plugins Documentation. URL: <https://volatility3.readthedocs.io/en/stable/volatility3.plugins.windows.html> (дата звернення: 15.08.2026).

9. Harvey P. ExifTool; ReFirm Labs. Binwalk; zed-0xff. zsteg. URL: <https://exiftool.org/ExifTool.html> ; <https://github.com/ReFirmLabs/binwalk> ; <https://github.com/zed-0xff/zsteg> (дата звернення: 15.08.2026).

10. Aleph One. Smashing The Stack For Fun And Profit // Phrack Magazine. 1996. Vol. 7, Issue 49. URL: https://phrack.org/issues/49/14_md

11. Shacham H. The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) // Proceedings of the 14th ACM Conference on Computer and Communications Security. 2007. P. 552-561. DOI: 10.1145/1315245.1315313.

УДК 004.8:316.77

Бубенцова Л.В., Царьов Р.Ю.

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ З ВИСОКИМ РІВНЕМ РИЗИКУ

Державний університет інтелектуальних технологій і зв’язку
ceis@suitt.edu.ua

Анотація. У роботі досліджено особливості систем штучного інтелекту з високим рівнем ризику. Проаналізовано основні сфери застосування таких систем, потенційні ризики їх використання та ключові механізми їх мінімізації. Особливу увагу приділено ризик-орієнтованому підходу до регулювання штучного інтелекту, закріпленому в Регламенті Європейського Союзу 2024/1689 (Artificial Intelligence Act). Визначено основні проблеми, пов’язані з алгоритмічною дискримінацією, якістю даних, непрозорістю алгоритмів, захистом персональних даних, кібербезпекою та недостатнім людським контролем. Обґрунтовано необхідність комплексного управління ризиками протягом усього життєвого циклу високоризикової системи штучного інтелекту.

Ключові слова: штучний інтелект, високоризикові системи, оцінювання ризиків, AI Act, алгоритмічна дискримінація, людський нагляд, кібербезпека, захист даних.

Стрімкий розвиток технологій штучного інтелекту (ШІ) є однією з визначальних тенденцій сучасної цифрової трансформації. Системи ШІ активно впроваджуються в економіці, промисловості, освіті, медицині, державному управлінні, транспорті, фінансовій сфері та інших галузях. Використання алгоритмів машинного навчання та інших технологій ШІ дає змогу автоматизувати значну кількість процесів, здійснювати аналіз великих обсягів інформації та підтримувати прийняття управлінських рішень.

Водночас розширення сфери застосування ШІ зумовлює появу нових технологічних, правових та соціальних ризиків. Особливої уваги потребують системи, результати роботи яких можуть істотно впливати на життя, здоров’я, безпеку або фундаментальні права людини. У таких випадках технічна помилка алгоритму, некоректні дані або неправильно сформована модель можуть мати значно серйозніші наслідки, ніж при використанні ШІ для виконання звичайних інформаційних завдань.

У зв’язку з цим у сучасному регулюванні ШІ формується ризик-орієнтований підхід, відповідно до якого вимоги до систем визначаються залежно від потенційного рівня шкоди. Одним із найбільш системних прикладів такого підходу є Регламент Європейського Союзу 2024/1689 — Artificial Intelligence Act (AI Act) [1].

Метою роботи є аналіз особливостей систем штучного інтелекту з високим рівнем ризику; визначення основних сфер їх застосування, потенційних загроз та механізмів їх мінімізації, вимог до забезпечення безпечного та відповідального використання таких систем та напрямів їх подальшого розвитку.

Класифікація високоризикових систем штучного інтелекту

Відповідно до статті 6 Регламенту (ЄС) 2024/1689 (Artificial Intelligence Act, AI Act), високоризикові системи штучного інтелекту поділяються на дві основні категорії [1,2].

До першої належать системи, які є компонентами безпеки продукції або самі є продукцією, що підпадає під визначене законодавство Європейського Союзу щодо гармонізації, за умови обов’язкового проведення оцінювання відповідності із залученням третьої сторони. Наприклад, системи, пов’язані з обладнанням для потенційно вибухонебезпечних середовищ, радіоблабнанням, медичними виробами, автомобільним та авіаційним транспортом. Високий рівень ризику таких систем обумовлений тим, що помилка або неналежне функціонування системи може безпосередньо вплинути на безпеку людини.

До другої категорії належать системи, які використовуються у визначених суспільно значущих сферах. До них належать (табл.1):

Таблиця 1 - Системи, які використовуються у визначених суспільно значущих сферах		
Сфера	Приклади застосування ШІ	
Біометрія	дистанційна біометрична ідентифікація, біометрична категоризація	
Критична інфраструктура	управління та експлуатація критичної інфраструктури	
Освіта	оцінювання, вступ, визначення рівня знань	
Зайнятість	підбір працівників, прийняття кадрових рішень, оцінювання працівників	
Основні приватні та державні послуги	оцінювання права на отримання послуг, кредитна оцінка	
Правоохоронна діяльність	оцінювання ризиків, аналіз доказів	
Міграція та контроль кордонів	аналіз заяв, перевірка документів, біометрична ідентифікація	
Правосуддя та демократичні процеси	допомога судовим органам, окремі системи, пов'язані з виборчими процесами	

Основні ризики використання високоризикових систем та механізми їх мінімізації

Одним із найбільш суттєвих ризиків є **ризик дискримінації та упередженості**. Системи ШІ значною мірою залежать від якості даних, на яких вони навчаються та функціонують. Якщо вихідні дані містять історичні або соціальні упередження, алгоритм може не тільки відтворювати їх, а й масштабувати на велику кількість користувачів. Особливо небезпечною така проблема стає у сфері працевлаштування, освіти, кредитування або надання соціальних послуг. Наприклад, автоматизоване ранжування кандидатів чи оцінювання їхніх характеристик під час відбору на роботу може призвести до необґрунтованого обмеження можливостей певних груп осіб через статистичні особливості історичних даних, навіть якщо така дискримінація безпосередньо не закладена розробником.

Другим важливим ризиком є непрозорість алгоритмічних рішень. Складні моделі машинного навчання можуть формувати результати, причини яких важко пояснити навіть розробникам системи. Проблема «чорної скриньки» набуває особливого значення тоді, коли рішення ШІ безпосередньо впливає на права та інтереси людини. Якщо користувач не має можливості зрозуміти логіку використання системи та оцінити отриманий результат, виникає проблема відповідальності за прийняте рішення.

Важливим фактором ризику є якість даних. Дані повинні бути релевантними, достатньо репрезентативними та належним чином організованими.

Окрему групу становлять ризики, пов’язані із захистом даних і кібербезпекою. Високоризикові системи можуть бути об’єктами цілеспрямованих атак, спрямованих на зміну їхньої поведінки або результатів роботи. Вони можуть обробляти значні обсяги персональної інформації. Несанкціонований доступ, підміна даних, маніпулювання вхідною інформацією або втручання в алгоритм можуть призвести до неправомірних чи небезпечних результатів.

Слід виділити проблему надмірної довіри до автоматизованих рішень. Користувач може сприймати результат роботи системи як об’єктивний лише тому, що його сформував алгоритм. Проте алгоритм не гарантує абсолютної правильності рішення. Тому людський контроль є необхідною складовою безпечного використання високоризикових систем.

Ще одним важливим аспектом є технічна надійність системи. Високоризикова система повинна забезпечувати належний рівень точності, стійкості та кібербезпеки протягом усього життєвого циклу. Система має бути здатною коректно функціонувати в умовах помилок, несправностей або непередбачених ситуацій. / Результати аналізу основних потенційних ризиків високоризикових систем [1] подані у табл.2.

Таблиця 2 - Системи, які використовуються у визначених суспільно значущих сферах та основні потенційні ризики		
Сфера	Приклади застосування ШІ	Основні потенційні ризики
Біометрія	дистанційна біометрична ідентифікація, біометрична категоризація	помилкова ідентифікація, дискримінація, порушення приватності
Критична інфраструктура	управління та експлуатація критичної інфраструктури	загроза безпеці людей та безперервності життєво важливих послуг
Освіта	оцінювання, вступ, визначення рівня знань	необ'єктивність оцінювання, дискримінація, обмеження доступу до освіти
Зайнятість	підбір працівників, прийняття кадрових рішень, оцінювання працівників	дискримінація, непрозорість кадрових рішень
Основні приватні та державні послуги	оцінювання права на отримання послуг, кредитна оцінка	необґрунтована відмова у послугах, фінансові та соціальні ризики
Правоохоронна діяльність	оцінювання ризиків, аналіз доказів	помилкові висновки, порушення прав людини
Міграція та контроль кордонів	аналіз заяв, перевірка документів, біометрична ідентифікація	дискримінація, помилки у прийнятті рішень
Правосуддя та демократичні процеси	допомога судовим органам, окремі системи, пов'язані з виборчими процесами	вплив на фундаментальні права та демократичні процеси

Згідно з ризик-орієнтованою класифікацією, запропонованою AI Act [1], високоризиковою вважається не технологія ШІ сама по собі, а система, яка використовується у визначеному контексті та потенційно може завдати істотної шкоди здоров'ю, безпеці або фундаментальним правам людини. Ризик-орієнтоване регулювання дозволяє встановлювати різні вимоги залежно від потенційної небезпеки системи і високоризикові системи можуть застосовуватись за умови виконання визначених вимог безпеки, прозорості та відповідальності. Важливим інструментом мінімізації ризиків є система управління ризиками. Відповідно до статті 9 AI Act, вона повинна бути встановлена, впроваджена, документована та підтримуватися протягом усього життєвого циклу високоризикової системи. Управління ризиками має мати безперервний ітеративний характер і включати ідентифікацію відомих та передбачуваних ризиків, їх оцінювання, визначення відповідних заходів зменшення ризику та регулярний перегляд ефективності таких заходів.

Для зменшення ризиків дискримінації та упередженості в такій системі навчальні, валідаційні та тестові набори даних повинні відповідати призначенню, бути належно сформованими та перевірятися на наявність упередженості. Процеси збирання, підготовки, маркування та оброблення даних мають бути належним чином організовані та задокументовані. Для мінімізації ризику неправильного **або** непрозорого прийняття рішень AI Act встановлює вимоги щодо прозорості, технічної документації та ведення записів [3]. Документація повинна містити інформацію, необхідну для оцінювання відповідності системи встановленим вимогам, а експлуатаційні журнали мають забезпечувати можливість відстеження функціонування системи. Це створює основу для аудиту та контролю її роботи. Людський контроль є одним із ключових механізмів зменшення ризику надмірної довіри до автоматизованих рішень [4]. Для забезпечення технічної надійності системи можуть застосовуватися резервні механізми, дублювання компонентів та процедури безпечного припинення роботи. Забезпечення вимог кібербезпеки повинно враховувати специфічні властивості технологій штучного інтелекту.

Особливістю регулювання високоризикових систем ШІ відповідно до AI Act є перехід від реактивного підходу до превентивного управління ризиками [5]. Безпека, неупередженість, прозорість, людський контроль, якість даних, стійкість і кібербезпека повинні враховуватися не як окремі елементи після створення системи, а як складові єдиного процесу її життєвого циклу. Такий підхід дозволяє підвищити надійність систем ШІ та одночасно забезпечити належний рівень захисту фундаментальних прав людини.

Ризик-орієнтований підхід як основа безпечного використання штучного інтелекту

Ризик-орієнтоване регулювання дозволяє встановлювати різні вимоги залежно від потенційної небезпеки технології. Такий підхід має принципову відмінність від загальної заборони використання ШІ: високоризикові системи можуть застосовуватися за умови виконання визначених вимог безпеки, прозорості та контролю. При цьому необхідно відмежовувати високоризикові системи від практик використання ШІ, які вважаються неприйнятними та підлягають забороні. AI Act встановлює окремий перелік заборонених практик, пов'язаних, зокрема, з маніпулятивними технологіями, експлуатацією вразливостей людини та іншими видами використання ШІ, що створюють неприйнятний рівень ризику [1,6].

Для України досвід Європейського Союзу має особливе значення. Розвиток національної системи регулювання ШІ потребує врахування європейських принципів безпеки, прозорості, відповідальності та захисту фундаментальних прав. Це важливо не лише з погляду правового наближення до ЄС, а й для створення умов довіри до цифрових технологій. Провідні українські IT-компанії (зокрема Grammarly, MacPaw, LetsData та інші) вже підписали добровільну Декларацію про саморегулювання та етичне використання ШІ [7].

У березні 2026 року Україна отримала від Європейської Комісії умови вступу за всіма переговорними кластерами. Однією із таких умов є гармонізація законодавства у сфері штучного інтелекту. Крім цього, у квітні цього року було затверджено Національну програму адаптації законодавства України до права Європейського Союзу, якою визначено завдання з розробки Закону України про штучний інтелект [8]. Саме тому в межах подальшої євроінтеграції Україна має формувати власну нормативно-правову базу у цій сфері.

Водночас завдання нашої держави полягає у створенні умов для розвитку інновацій в Україні, залученні інвестицій, підтримці українських розробників та впровадженні сучасних технологій в публічному управлінні та бізнесі.

Одним із перспективних напрямів є запровадження процедур оцінювання впливу ШІ на права людини, алгоритмічного аудиту та постійного моніторингу систем після їх упровадження. Особливу увагу необхідно приділяти системам, що використовуються у державному секторі та можуть впливати на доступ громадян до суспільно важливих послуг.

Висновки. Проведений аналіз свідчить, що високоризикові системи штучного інтелекту мають специфічні особливості, пов'язані насамперед із потенційно значним впливом результатів їх роботи на людину та суспільство.

Основними ризиками є алгоритмічна дискримінація, недостатня якість даних, непрозорість прийняття рішень, порушення конфіденційності, кіберзагрози, технічні помилки та надмірна залежність користувача від автоматизованих рекомендацій.

Забезпечення безпечного використання таких систем потребує комплексного підходу, який включає управління ризиками протягом усього життєвого циклу системи, належне управління даними, технічне документування, тестування, моніторинг, забезпечення точності та кібербезпеки, а також ефективний людський нагляд.

Досвід Європейського Союзу, закріплений у AI Act, демонструє перехід від загальних етичних рекомендацій до конкретних нормативних вимог щодо розроблення та використання високоризикового ШІ. Для України врахування цього досвіду є важливим напрямом формування сучасної системи регулювання штучного інтелекту.

Отже, подальший розвиток високоризикових систем ШІ має здійснюватися за принципом «інновації за умови безпеки, прозорості та відповідальності». Ефективність технології не може бути єдиним критерієм її впровадження. Не менш важливими є захист прав людини, можливість реального людського контролю та чітке визначення відповідальності за наслідки використання автоматизованих систем.

Література

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 05.07.2026).
2. European Commission. AI Act Service Desk. Article 6: Classification rules for high-risk AI systems. URL: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-6> (дата звернення: 05.07.2026).
3. European Commission. AI Act Service Desk. Article 10: Data and data governance. URL: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-10> (дата звернення: 11.07.2026).
4. European Commission. AI Act Service Desk. Article 14: Human oversight. URL: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-14> (дата звернення: 08.08.2026).
5. Sousa e Silva N. The Artificial Intelligence Act: critical overview. 2024. URL: <https://arxiv.org/abs/2409.00264> (дата звернення: 08.08.2026).
6. Kelly J., Zafar S., Heidemann L. et al. Navigating the EU AI Act: A Methodological Approach for Safety-critical Products. 2024. URL: <https://arxiv.org/abs/2403.16808> (дата звернення: 08.08.2026).
7. Українські IT-компанії розроблять правила використання ШІ в технологічних продуктах URL: <https://thedigital.gov.ua/news/business/ukrainski-it-kompanii-rozroblyat-pravila-vikoristannya-shi-v-tekhnologichnikh-produktakh> (дата звернення: 09.08.2026).
8. Чіткі правила регулювання штучного інтелекту: у Комітеті з питань цифрової трансформації відбулося засідання робочої групи. URL: https://www.rada.gov.ua/news/news_kom/273621.html (дата звернення: 10.08.2026)

УДК 004.056:004.8:62-5

Хлапонін Ю.І.

ГУМАНОЇДНІ РОБОТИ В ЦИФРОВІЙ ЕКОСИСТЕМІ SMART CITY: МОЖЛИВОСТІ, ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКОВІ РИЗИКИ
Державний торговельно-економічний університет
y.khlaponin@knute.edu.ua

Анотація. Розглянуто перспективи інтеграції гуманоїдних роботів у цифрову екосистему Smart City як нового класу інтелектуальних кіберфізичних систем. Проаналізовано основні технології їх функціонування, зокрема штучний інтелект, сенсорне сприйняття, автономну навігацію та мережеву взаємодію. Визначено ключові проблемні питання безпеки: фізичну безпеку людино-роботичної взаємодії, кібербезпеку програмно-апаратної інфраструктури, захист даних і приватність, а також безпеку систем штучного інтелекту. Обґрунтовано необхідність комплексного підходу до забезпечення кіберстійкості гуманоїдних роботів у міському цифровому середовищі.

Ключові слова: гуманоїдний робот, Smart City, кіберфізична система, штучний інтелект, кібербезпека, кіберстійкість, робототехніка, цифрова міська інфраструктура.

Стрімкий розвиток робототехніки та штучного інтелекту зумовлює перехід гуманоїдних роботів від переважно експериментальних систем до технологій, орієнтованих на практичне застосування. Сучасні підходи до розвитку інтелектуальних роботів ґрунтуються на поєднанні фізичного втілення, сенсорного сприйняття, штучного інтелекту та здатності автономно взаємодіяти з навколишнім середовищем. Концепція embodied intelligence розглядає інтелект робота як результат взаємодії алгоритмів, фізичної конструкції та середовища функціонування [1].

Одним із перспективних напрямів застосування гуманоїдних роботів є цифрове міське середовище. Концепція Smart City передбачає інтеграцію інформаційно-комунікаційних технологій, IoT, цифрових

платформ та інтелектуальних систем для підвищення ефективності міських процесів і якості життя населення. У такій екосистемі робот може виконувати функції мобільного інтелектуального агента, взаємодіючи з людьми, об'єктами міської інфраструктури та цифровими сервісами. Сучасні дослідження застосування роботизованих систем у Smart City охоплюють транспорт, логістику, моніторинг, технічне обслуговування та інші міські процеси [2].

Особливістю гуманоїдного робота є поєднання фізичної автономності та цифрового інтелекту. Камери, мікрофони, LiDAR та інші сенсори забезпечують отримання інформації про навколишнє середовище, а алгоритми комп'ютерного зору, машинного навчання та мультимодального штучного інтелекту забезпечують її інтерпретацію. Мережеві технології створюють можливість обміну даними з хмарними та периферійними обчислювальними ресурсами, міськими інформаційними системами та іншими цифровими платформами.

Таким чином, гуманоїдний робот доцільно розглядати не лише як механічний пристрій, а як кіберфізичну систему, у якій інформаційні процеси безпосередньо пов'язані з фізичними діями. Така особливість суттєво змінює підхід до оцінювання безпеки. Сучасні дослідження безпеки гуманоїдних роботів виділяють фізичну безпеку людино-роботичної взаємодії, кібербезпеку та надійність програмного забезпечення, стандартизацію, а також етичні та соціальні аспекти [3].

Для цифрового міського середовища особливого значення набуває кібербезпека. Робот може містити значну кількість програмних компонентів, використовувати бездротові мережі, API, хмарні сервіси та механізми віддаленого оновлення програмного забезпечення. Систематичні дослідження кібербезпеки роботизованих систем показують, що до основних проблем належать вразливості програмного забезпечення, мережеві атаки, несанкціонований доступ, компрометація каналів зв'язку та інші загрози, здатні впливати на конфіденційність, цілісність і доступність інформації [4].

Окрему проблему становить захист даних. Функціонування гуманоїдного робота передбачає постійне або періодичне отримання інформації про людей та навколишній простір. У міському середовищі така інформація може включати відео-, аудіо-, просторові та поведінкові дані. Отже, поряд із традиційними вимогами кібербезпеки виникає необхідність забезпечення приватності та контролю за життєвим циклом даних.

Ще одним критичним компонентом є безпека штучного інтелекту. Автономна поведінка робота залежить від здатності правильно сприймати середовище, інтерпретувати отримані дані та формувати відповідні рішення. NIST AI Risk Management Framework визначає безпечність, захищеність і стійкість як важливі характеристики надійних систем штучного інтелекту та рекомендує управляти відповідними ризиками протягом життєвого циклу AI-систем [5]. Для гуманоїдної робототехніки це набуває особливого значення, оскільки помилка цифрового компонента може безпосередньо впливати на фізичну поведінку робота.

Важливою особливістю функціонування гуманоїдного робота у Smart City є багаторівнева взаємодія з цифровою інфраструктурою. На відміну від автономного робота, який функціонує у відносно ізольованому середовищі, міський робот може одночасно взаємодіяти з IoT-пристроями, системами позиціонування, транспортними сервісами, інформаційними платформами та хмарними ресурсами. Це розширює функціональні можливості системи, але водночас збільшує кількість потенційних точок компрометації.

Окрему увагу необхідно приділяти цілісності даних, які надходять від сенсорів. Для автономного робота помилкова або навмисно змінена інформація про місцезнаходження об'єктів, людей чи перешкод може спричинити неправильне планування маршруту або небезпечну фізичну дію. Тому захист сенсорного рівня має передбачати не лише конфіденційність передавання інформації, а й контроль її достовірності, виявлення аномалій та можливість переходу системи у безпечний режим функціонування.

Не менш важливим є забезпечення кіберстійкості мережевої взаємодії. У разі втрати зв'язку з хмарною платформою, затримки передавання даних або блокування окремого сервісу робот не повинен автоматично переходити до неконтрольованої поведінки. Доцільним є застосування принципів defense-in-depth, сегментації мережі, автентифікації компонентів, шифрування каналів зв'язку та мінімізації привілеїв. Для критичних операцій необхідно передбачати локальні механізми прийняття рішень, які забезпечують безпечне завершення дії навіть за відсутності зовнішніх сервісів.

Перспективним напрямом є використання edge computing для оброблення частини сенсорної інформації безпосередньо на роботі або поблизу джерела її формування. Такий підхід може зменшити затримку передавання даних, підвищити автономність і водночас обмежити обсяг інформації, що передається до зовнішніх платформ. У контексті захисту приватності це також створює можливість реалізації принципу мінімізації даних, коли до міської інформаційної системи передається лише інформація, необхідна для виконання конкретного завдання.

Таким чином, забезпечення безпеки гуманоїдних роботів потребує переходу від захисту окремого пристрою до системного управління ризиками на всіх етапах його життєвого циклу — від проектування та розроблення програмного забезпечення до експлуатації, оновлення та виведення з експлуатації. Особливого значення набуває принцип security by design, відповідно до якого вимоги кібербезпеки мають бути інтегровані в архітектуру роботизованої системи ще на етапі її створення.

Узагальнення наведених положень дозволяє сформулювати принципову особливість кібербезпеки гуманоїдних роботів у Smart City: кібернетичний ризик потенційно може трансформуватися у фізичний. У спрощеному вигляді такий ланцюг можна представити як: **компрометація даних → порушення роботи інтелектуального компонента → формування неправильного рішення → зміна керуючої дії → фізичний**

вплив робота. Саме тому безпеку гуманоїдної робототехніки необхідно розглядати комплексно — на рівні робота, комунікаційної інфраструктури та міської цифрової екосистеми.

Висновки. Гуманоїдні роботи формують перспективний напрям розвитку кіберфізичних систем і можуть стати складовою майбутньої цифрової інфраструктури Smart City. Їх інтеграція з міськими цифровими платформами, IoT та системами штучного інтелекту одночасно розширює функціональні можливості та формує нові загрози безпеці. Для подальших досліджень доцільно розробити багаторівневу модель кібербезпеки гуманоїдного робота, яка враховуватиме фізичний, сенсорний, програмний, інтелектуальний, мережевий і платформний рівні. Перспективним напрямом є також дослідження взаємозв'язку між кібербезпекою окремого робота та кіберстійкістю цифрової екосистеми Smart City.

Література

1. Zhao W., Yuan Y. Development of intelligent robots in the wave of embodied intelligence // National Science Review. 2025. Vol. 12, Issue 7. Art. nwaf159. DOI: 10.1093/nsr/nwaf159.
2. Chand R., Sharma B., Kumar S. A. Systematic review of mobile robots applications in smart cities with future directions // Journal of Industrial Information Integration. 2025. Vol. 100821. DOI: 10.1016/j.jii.2025.100821.
3. Kóczy D., Sárosi J. Safety Engineering for Humanoid Robots in Everyday Life — Scoping Review // Electronics. 2025. Vol. 14, No. 23. Art. 4734. DOI: 10.3390/electronics14234734.
4. Verma N., Kumar N., Verma C., Illés Z., Singh D. et al. A systematic review on cybersecurity of robotic systems: vulnerabilities trends, threats, attacks, challenges, and proposed framework // International Journal of Information Security. 2025. Vol. 24. Art. 127. DOI: 10.1007/s10207-025-01041-z.
5. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : National Institute of Standards and Technology, 2023. NIST AI 100-1. DOI: 10.6028/NIST.AI.100-1.

УДК 004.056:004.8

Хомутов О.О., Онацький О.В.

СЕМАНТИЧНО ОРІЄНТОВАНА СИСТЕМА ВИЯВЛЕННЯ КІБЕРАТАК НА ОСНОВІ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ У SOC

Державний університет інтелектуальних технологій і зв'язку
aleksandrr.khomutov@gmail.com, onatsky@meta.ua

Анотація. Розглянуто застосування великих мовних моделей (Large Language Models, LLM) для побудови семантично орієнтованих систем виявлення кібератак у центрах моніторингу інформаційної безпеки (Security Operations Center, SOC). На відміну від традиційних сигнатурних та аномалійних підходів, запропонований метод використовує глибинне розуміння контексту подій, що дає змогу знизити рівень хибних спрацьовувань і підвищити пояснюваність рішень. Проаналізовано сучасні англомовні дослідження 2024–2025 років у напрямках аналізу журналів, інтеграції кіберрозвідки через генерацію з доповненням через пошук (Retrieval-Augmented Generation, RAG) та зіставлення поведінки з MITRE ATT&CK. Запропоновано концепцію контрольованого семантичного шару, що поєднує нормалізацію подій, RAG, структурований вихід і принцип участі людини в контурі прийняття рішень (human-in-the-loop), як основу для подальшого дисертаційного дослідження.

Ключові слова: великі мовні моделі, кібербезпека, центр операцій безпеки, аналіз журналів, генерація з доповненим пошуком, MITRE ATT&CK, семантичний аналіз, explainability.

Сучасний центр моніторингу інформаційної безпеки працює в умовах постійного інформаційного перевантаження. Інфраструктура генерує події операційних систем, мережевих пристроїв, хмарних платформ, засобів виявлення та реагування на кінцевих пристроях (Endpoint Detection and Response, EDR), поштових шлюзів і бізнес-застосунків. Навіть добре налаштована система керування подіями та інформацією безпеки (Security Information and Event Management, SIEM) формує велику кількість сповіщень, частина яких є хибнопозитивні або потребує додаткового контексту. Наслідком є втома від сповіщень (alert fatigue), зростання часу реагування та ризик пропустити реальну атаку. Сигнатурні системи ефективні лише для відомих шаблонів, а класичні моделі машинного навчання виявляють аномалії, проте дають мало пояснень, чому подія вважається підозрілою. Крім того, такі моделі важко адаптувати до нових тактик зловмисників без повторного навчання на великих обсягах розмічених даних.

Великі мовні моделі дають змогу перейти від суто синтаксичного аналізу подій до семантично орієнтованого підходу. Йдеться не про заміну SIEM чи систем виявлення вторгнень (Intrusion Detection System, IDS), а про додатковий інтелектуальний шар, який пояснює події, узагальнює журнали, нормалізує неструктуровані записи, співвідносить поведінку з тактиками, техніками та процедурами (Tactics, Techniques, and Procedures, TTP) MITRE ATT&CK і допомагає аналітикові на етапі первинного сортування (triage). На відміну від традиційних підходів, LLM здатні враховувати природномовні описи атак, історичний контекст і

навіть неявні зв'язки між різними джерелами даних, що робить їх особливо цінними для виявлення багатоетапних атак (Advanced Persistent Threats, APT). Оглядові праці [1, 2] та емпіричне дослідження [3] наголошують, що в реальних SOC доцільно застосовувати LLM, як інструмент підтримки аналітика, залишаючи остаточне рішення за людиною. При цьому ключовою вимогою є забезпечення пояснюваності (explainability) – аналітик має розуміти, на яких підставах модель робить той чи інший висновок.

Аналіз журналів є центральним напрямом для семантично орієнтованих систем. У роботі LogParser-LLM [4] показано, що врахування семантики повідомлення, а не лише його синтаксичної форми, підвищує якість парсингу динамічних журналів; модель викликається не для кожного запису, а в контрольованих точках, що забезпечує масштабованість. LogPrecis [5] переходить від окремих команд оболонки до послідовності намірів зловмисника та формує відбиток атаки, наближаючи аналіз до методології ATT&CK. Підхід LogPrompt [6] демонструє інтерпретований аналіз журналів із застосуванням стратегій формування запитів (zero-shot, few-shot, chain-of-thought) і одночасним генеруванням текстових пояснень, що зменшує когнітивне навантаження на аналітика. Окремої уваги заслуговує можливість використання LLM для збагачення журналів додатковими метаданими, зокрема геолокацією, типами активності користувачів або історією їхніх дій, що дозволяє будувати більш повну картину інциденту.

Другу групу становлять завдання виявлення вразливостей і атак. APPATCH [7] використовує адаптивне формування запитів і врахування семантики під час аналізу коду; Rondanini та співавтори [8] досліджують виявлення шкідливого програмного забезпечення на периферії за допомогою полегшених (lightweight) LLM; Alnahdi та Narain [9] зосереджуються на узгодженості пояснень IDS із доменними знаннями; AECR [10] автоматично вилучає відомості про техніки атак із звітів кіберрозвідки (Cyber Threat Intelligence, CTI) на основі донавченої моделі. Спільним висновком є те, що LLM працюють краще, коли отримують структурований контекст і керований процес міркування, а не весь інформаційний шум. Це підтверджує доцільність побудови гібридних систем, де LLM взаємодіє з класичними детекторами, отримуючи від них попередньо відфільтровані дані та зосереджуючись на найбільш складних або неоднозначних випадках.

Ключовим механізмом підвищення надійності є генерація з доповненням через пошук (RAG). Система RAGIntel [11] поєднує генеративні можливості LLM із пошуком у структурованих джерелах MITRE ATT&CK, що зменшує ризик галюцинацій і дає відповіді, підкріплені доказами. Для розроблення правил виявлення важливим є підхід Rule-ATT&CK Mapper (RAM) [12], що автоматично зіставляє правила SIEM із техніками ATT&CK за допомогою багатоетапного конвеєра та ланцюжка запитів без додаткового донавчання моделі. Це дає змогу оцінювати покриття технік і визначати прогалини у контенті виявлення.

На основі проаналізованих джерел запропоновано концепцію контрольованого семантичного шару для SOC. Він приймає нормалізовані події або групи сповіщень, використовує RAG для отримання релевантного контексту з бази знань (MITRE ATT&CK, сценарії реагування, історія інцидентів) і формує пояснювальну картку інциденту зі структурованим виходом: короткий опис, докази, підозрілі ознаки, ймовірні техніки ATT&CK, рівень упевненості, альтернативні пояснення та рекомендовані кроки перевірки. Такий шар не замінює SIEM, а доповнює його, скорочуючи час первинного сортування та підвищуючи якість розуміння складних атак. Провідним напрямом дисертаційного дослідження обрано поєднання семантичного збагачення сповіщень із RAG-інтеграцією кіберрозвідки за принципом human-in-the-loop.

Практичне впровадження потребує врахування обмежень LLM. Основними ризиками є галюцинації, ін'єкція інструкцій у запит (prompt injection), конфіденційність журналів, вартість і продуктивність, а також складність оцінювання пояснень. Це формує вимоги до методу: розділення даних та інструкцій, маскування чутливих полів, обмеження відповіді доказами, структурований вихід, аудит запитів і багаторівневе оцінювання якості (технічна правильність, корисність для аналітика, стійкість до маніпуляцій).

Висновки. Аналіз літератури 2024–2025 років свідчить, що великі мовні моделі доцільно застосовувати в SOC не як автономний засіб прийняття рішень, а як семантичний шар підтримки аналітика. Найперспективнішими напрямками є аналіз журналів на основі LLM та інтеграція знань через RAG із зіставленням поведінки з MITRE ATT&CK. Встановлено, що ключовою умовою успішного впровадження є поєднання трьох факторів: перше – керованої взаємодії з моделлю через структуровані запити, друге – зовнішнього контексту з перевірених джерел (RAG), третє – обов'язкової участі людини на етапі прийняття рішень. Науковою новизною подальшого дослідження є метод побудови контрольованого семантичного шару, що поєднує нормалізацію подій, пошук релевантних знань, структурований вихід, оцінювання достовірності та участь людини в контурі прийняття рішень. На відміну від існуючих підходів, запропонований метод забезпечує не лише пояснюваність і відтворюваність, але й адаптивність до змін у ландшафті загроз за рахунок інтеграції з актуальними базами знань і зворотним зв'язком від аналітиків. Такий підхід забезпечує пояснюваність, відтворюваність та інтеграцію з наявними засобами SOC. Перспективи подальших досліджень включають експериментальну верифікацію запропонованої архітектури на реальних даних SOC, порівняльний аналіз з класичними методами виявлення, а також дослідження впливу різних стратегій формування запитів на якість виявлення багатоетапних атак.

Література

1. Habibzadeh A., Feyzi F., Atani R. E. Large Language Models for Security Operations Centers: A Comprehensive Survey. arXiv:2509.10858. 2025.

2. Srinivas S., Kirk B., Zendejas J. et al. AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. Journal of Cybersecurity and Privacy. 2025. Vol. 5(4). 95.
3. Singh R., Tariq S., Chhetri M. B. et al. LLMs in the SOC: An Empirical Study of Human-AI Collaboration in Security Operations Centres. arXiv:2508.18947. 2025.
4. Zhong A., Mo D., Liu G. et al. LogParser-LLM: Advancing Efficient Log Parsing with Large Language Models. Proc. of the 30th ACM SIGKDD Conf. (KDD '24). 2024. DOI: 10.1145/3637528.3671810.
5. Boffa M., Drago I., Mellia M. et al. LogPrecis: Unleashing language models for automated malicious log analysis. Computers & Security. 2024. Vol. 141. 103805.
6. Liu Y., Tao S., Meng W. et al. Interpretable Online Log Analysis Using Large Language Models with Prompt Strategies. Proc. of ICPC 2024. arXiv:2308.07610.
7. Nong K., Yang K., Chen Z. et al. APPATCH: Automated Adaptive Prompting LLMs for Real-World Software Vulnerability Patching. USENIX Security. 2025.
8. Rondanini C., Carminati B., Ferrari E. et al. Malware Detection at the Edge with Lightweight LLMs: A Performance Evaluation. arXiv:2503.04302. 2025.
9. Alnahdi A., Narain S. Towards Transparent Intrusion Detection: A Coherence-Based Framework in Explainable AI Integrating LLMs. IEEE TPS-ISA. 2024.
10. Chen M., Wang J., Xue F., Wu Z. AECR: Automatic Attack Technique Intelligence Extraction Based on Fine-Tuned LLM. Computers & Security. 2025. Vol. 150. 104213.
11. Alhuzali A. LLM-powered threat intelligence: a retrieval-augmented generation approach for cyber attack investigation. PeerJ Computer Science. 2025. Vol. 11. e3371.
12. Wudali P. N., Malul E., Gandhi P. A. et al. Rule-ATT&CK Mapper (RAM): Mapping SIEM Rules to TTPs Using LLMs. arXiv:2502.02337. 2025.

УДК 621.396.2:004.85

Сідень С.В., Кутовий М.Г.

АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G/6G

Державний університет інтелектуальних технологій і зв'язку
ssiden@suitt.edu.ua, mishakutovoy@ukr.net

Анотація. Проаналізовано можливості застосування методів машинного навчання у задачах планування та керування мобільними мережами сучасних та майбутніх поколінь з врахуванням міжсистемних завад. Розглянуті архітектурні особливості мереж 5G New Radio та 6G. Проведено порівняння детермінованих, статистичних та методів машинного навчання для врахування завад, при цьому методи глибокого навчання з підкріпленням та графові нейронні мережі визначено як перспективні підходи для узгодженого керування ресурсами. Розроблено імітаційну модель міжсистемних завад у смузі 3,5 ГГц та наведено кількісні оцінки впливу завад на SINR, захисних відстаней і точності різних підходів до прогнозування завад.

Ключові слова: машинне навчання, 5G/6G, мережеве планування, міжсистемні перешкоди, глибоке навчання з підкріпленням, O-RAN, імітаційне моделювання, SINR.

Розвиток мережі 5G NR та формування концепції мереж 6-го покоління в рамках програми IMT-2030 забезпечують складне завдання планування та управління безпроводовими мережами. Використання міліметрових хвиль, технології Massive MIMO, методів спільного використання спектру створює комплексне електромагнітне середовище, в якому традиційні методи планування мають низьку ефективність. Особливо актуальною є проблема міжсистемних завад, наприклад 5G NR, Wi-Fi, супутниковими та радіолокаційними системами. Згідно з рекомендаціями ITU-R M.2160-0, мережі 6G повинні реалізовувати концепцію AI-native, що враховує глобальну інтеграцію методів штучного інтелекту в структуру мережі. Цей фактор зумовлює необхідність глибокого вивчення методів машинного навчання для таких задач планування та керування мережею.

Впровадження мереж 5G супроводжується рядом невирішених задач, що пов'язані з забезпеченням стабільної якості зв'язку в складних умовах міської забудови. На ефективність мереж впливають завади, затухання сигналу, багатопромєневе поширення та зростання кількості підключених пристроїв. Тому задача систематизації методів машинного навчання саме у контексті задач планування мереж 5G/6G з урахуванням міжсистемних завад є актуальною.

Архітектура мереж 5G NR, базується на дезагрегації базової станції gNB на центральний (CU), розподілений (DU) та радіоблок (RU). Радіоінтерфейс використовує гнучку нумерологію OFDM:

$$\Delta f = 2^{\mu} \cdot 15\text{кГц}, \quad T_{\text{sym}} = \frac{1}{\Delta f}, \quad \mu \in \{0,1,2,3,4\}, \quad (1)$$

Δf – відстань між піднесучими, μ – індекс нумерології, T_{sym} – тривалість OFDM-символу. Це дозволяє адаптувати мережу до вимог пропускної здатності, затримки та стійкості до доплерівських зсувів. У 5G підтримуються сценарії eMBB, URLLC та mMTC, які відрізняються вимогами до швидкості передачі, надійності та затримки. Концепція 6G розвиває принципи 5G у напрямках AI-native, ISAC, RIS, XL-MIMO та субтерагерцового зв'язку. На відміну від 5G, де алгоритми машинного навчання працюють поверх існуючої архітектури, у 6G штучний інтелект інтегрується безпосередньо у фізичний рівень та механізми керування мережею.

Методи машинного навчання поділяються на навчання з учителем, без учителя, напівкероване та навчання з підкріпленням. Задача навчання з учителем формулюється як мінімізація емпіричного ризику:

(2)

$L(\cdot)$ – функція втрат, $\Omega(\theta)$ – регуляризаційний параметр, λ – коефіцієнт регуляризації. N – кількість тренувальних вибірок.

Навчання з підкріпленням ґрунтується на марковських процесах прийняття рішень, а оптимальна функція визначається рівнянням Беллмана. Для складних задач керування мережами застосовується Deep Reinforcement Learning (DRL). Графові нейронні мережі (GNN) описують мережу як граф та виконують оновлення вузлів за схемою message-passing.:

$$H_v^{(k+1)} = \sigma \left(W^{(k)} h_v^{(k)} + \sum_{u \in N(v)} W_N^{(k)} h_u^{(k)} \right), \quad (3)$$

$h_v^{(k)}$ – вектор представлення вузла v на k -му шарі, $N(v)$ – множина сусідів, $\sigma(\cdot)$ – нелінійна функція активації [6].

Для розподіленого навчання використовується федеративний алгоритм FedAvg.:

$$\theta_{t+1}^{global} = \sum_{k=1}^K \frac{n_k}{n} \theta_{t+1}^{(k)}, n = \sum_{k=1}^K n_k \quad (4)$$

K – кількість локальних вузлів, n_k – розмір локальної вибірки. Такий підхід забезпечує приватність даних та зменшує навантаження на транспортну мережу.

Задача планування мережі 5G з урахуванням міжсистемних завад можна представити як нелінійну змішано-цілочисельну оптимізацію, в якій потрібно максимізувати пропускну здатність мережі при врахуванні обмежень на допустимі рівні завад для інших систем радіозв'язку. Через надзвичайно великий простір рішень таких задач, класичні методи оптимізації є малоефективними. Саме через це доцільним є використання методів машинного навчання. Оцінювання міжсистемних завад виконується через показник SINR:

$$SINR = \frac{P_S G_S L_S^{-1}}{N_0 + \sum_{k=1}^K P_k G_k L_k^{-1}}. \quad (5)$$

P_S – потужність корисного сигналу, G_S – коефіцієнт підсилення антени, L_S – втрати при поширенні сигналу. Потужність теплового шуму у смузі B визначається наступним чином:

$$N_0 = k_B T B F, \quad (6)$$

– постійна Больцмана, $T = 290K$ – температура у Кельвінах, F – коефіцієнт шуму приймача. Зазвичай критерій прийнятності завад встановлюється на рівні $I/N \leq -6$ дБ.

Існують чотири базові підходи до моделювання рівня міжсистемних завад: детермінований, статистичний, на основі методів машинного навчання та гібридний [7]. Детерміновані методи (такі як метод трасування променів) забезпечують високу точність, але потребують значних обчислювальних ресурсів. Статистичні моделі 3GPP та ITU-R простіші, однак не враховують локальних особливостей середовища. Методи машинного навчання демонструють високу адаптивність, а фізично обґрунтовані підходи поєднують переваги фізичних моделей і нейронних мереж.

В архітектурі мереж O-RAN ключовим компонентом є RAN Intelligent Controller (RIC), представлений рівнями Near-RT RIC та Non-RT RIC. Моделі машинного навчання реалізуються у вигляді xApp і rApp. Для керування мікромірковими завадами застосовуються DRL-агенти, функція винагороди яких враховує пропускну здатність мережі та штраф за інтерференцію:

$$r_t = \sum_{n=1}^N R_n(t) - \lambda_I \sum_{\substack{n'=1 \\ n' \neq n}}^N I_{n,n'}(t), \quad (7)$$

де $R_n(t)$ – агрегована пропускна здатність n -ї комірки, $I_{n,n'}(t)$ – міжкоміркова інтерференція, λ_I – ваговий коефіцієнт штрафу.

Для кількісної перевірки сформульованих залежностей розроблено імітаційну модель низхідної лінії 5G NR мовою Python. Параметри сценарію: несійна частота $f_c = 3,5$ ГГц (смуга n78), ширина смуги $B = 100$ МГц, рівень шуму приймача $F = 5$ дБ, відповідно за формулою (6) – $N_0 = -89$ дБм, потужність БС – 46 дБм, підсилення антени – 15 дБі, відстань абонента до неї – 200 м. У якості моделі поширення радіохвиль було обрано модель 3GPP TR 38.901 для сценарію макро середовища.

Вираз (5) узагальнено на завади по сусідньому каналу введенням коефіцієнта його придушення $ACIR$:

$$SINR(d_I) = \frac{P_S G_S L_S^{-1}}{N_0 + \sum_{k=1}^K P_k G_k L_k^{-1} \cdot 10^{-ACIR_k/10}} \quad (11)$$

Результати моделювання наведено на рис. 1. Суміщений за каналом передавач з EIRP 43 дБм знижує відношення SINR абонента нижче порогу демодуляції QPSK (0 дБ) на відстанях до 90 м, а рівень 20 дБ, потрібний для модуляції 64QAM, досягається лише за $d_I > 221$ м (рис. 1, а). Фільтрація сусіднього каналу з ACIR = 30 і 45 дБ скорочує цю відстань до 55 і 21 м відповідно. За критерієм $I/N \leq -6$ дБ захисна відстань становить 408, 846 і 1503 м для EIRP 30, 43 і 53 дБм (рис. 1, б), тобто зростає приблизно у 1,8 раза на кожні 10 дБ потужності джерела завади.

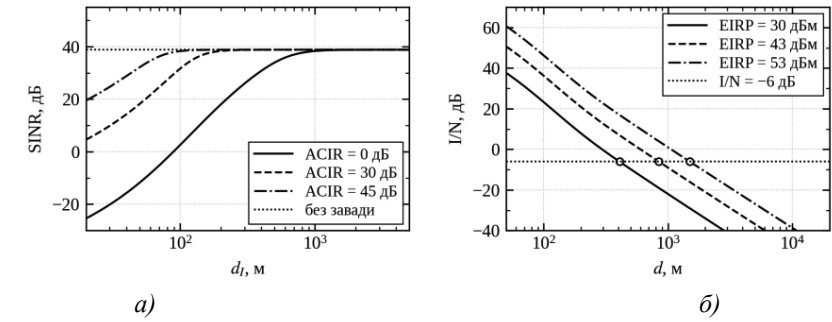


Рисунок 1 - Вплив завади на SINR абонента (а) та визначення захисної відстані за критерієм I/N (б)

Точність оцінювання рівня завад досліджено методом Монте-Карло. Складові похибки кожного підходу задано за узагальненими даними [4, 5], тому порівняння є відносним. Статистичні моделі 3GPP/ITU-R дають RMSE 7,5 дБ і похибку 12,4 дБ на рівні 90-го перцентилля, модель машинного навчання – 3,1 і 5,1 дБ, гібридна фізично-обґрунтована модель – 1,9 і 3,1 дБ проти 1,2 і 2,0 дБ у детермінованого розрахунку (рис. 2).

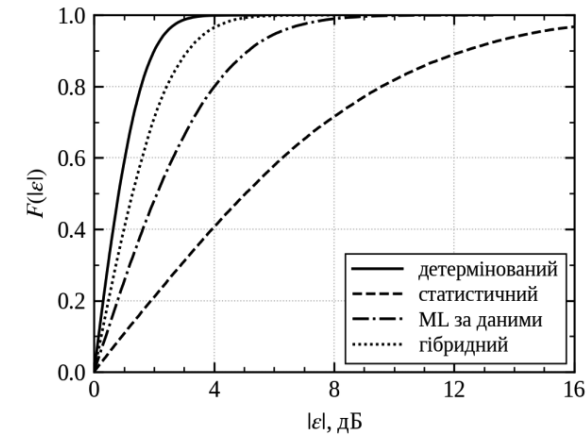


Рисунок 2 - Функції розподілу модуля похибки оцінювання SINR для різних підходів

Висновки. У роботі проаналізовано застосування методів машинного навчання в мережах сучасних та майбутніх поколінь з урахуванням міжсистемних завад та виконано імітаційне моделювання. Визначено, що традиційні методи планування не масштабуються через надзвичайно велику кількість можливих конфігурацій, що зумовлює використання методів машинного навчання для рішення такого типу задач. Систематизовано підходи машинного навчання та визначено найперспективніші, а саме DRL, GNN і FL. Моделювання показало, що завада по суміщеному каналу унеможливорює зв'язок на відстанях до 90 м, тоді як придушення сусіднього каналу на 45 дБ скорочує цю відстань до 21 м, а захисна відстань за критерієм $I/N = -6$ дБ зростає з 408 до 1503 м у разі збільшення потужності джерела завади з 30 до 53 дБм. Гібридні фізично-обґрунтовані моделі зменшують RMSE оцінювання SINR з 7,5 до 1,9 дБ. Подальші дослідження будуть спрямовані на розробку

таких фізично-обґрунтованих моделей прогнозування рівня завад та багатафакторних алгоритмах керування ресурсами мережі.

Література

1. Letaief K. B., Chen W., Shi Y., Zhang J., Zhang Y.-J. A. The Roadmap to 6G: AI Empowered Wireless Networks. IEEE Communications Magazine. 2019. Vol. 57, No. 8. P. 84–90. DOI: 10.1109/MCOM.2019.1900271.

2. 3GPP TS 38.300 V18.2.0. NR; NR and NG-RAN Overall description; Stage 2 (Release 18). Sophia Antipolis : 3GPP, p. 167. (2024).

3. ITU-R Recommendation M.2160-0. Framework and overall objectives of the future development of IMT for 2030 and beyond. Geneva : International Telecommunication Union, p. 25. (2023).

4. Alhammadi A., Shayea I., El-Saleh A. A., Azmi M. H., Daradkeh Y. I., Mohamad H. Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges. International Journal of Intelligent Systems. 2024. Vol. 2024. Article ID 8845070. DOI: 10.1155/2024/8845070.

5. Lohan P., Kantarcı B., Ferrag M. A., Tihanyi N., Shi Y. From 5G to 6G Networks: A Survey on AI-Based Jamming and Interference Detection and Mitigation. IEEE Open Journal of the Communications Society. 2024. Vol. 5. P. 3920–3974. DOI: 10.1109/OJCOMS.2024.3416808.

6. Shen Y., Shi Y., Zhang J., Letaief K. B. Graph Neural Networks for Scalable Radio Resource Management: Architecture Design and Theoretical Analysis. IEEE Journal on Selected Areas in Communications. 2021. Vol. 39, No. 1. P. 101–115. DOI: 10.1109/JSAC.2020.3036965

7. Siden S., Tsarov R., Stepanov D., Shulakova K., Pavlov A. Hybrid AI-Based Path Loss Prediction Model for 5G/6G Networks. *Proceedings of International Conference on Applied Innovation in IT*. 2026. Vol. 14, Issue 2. P. 21–27. DOI: <https://doi.org/10.25673/123804>

УДК 342.922:004.056.5

Большакова О.В.

АДМІНІСТРАТИВНО-ПРАВОВІ ІНСТРУМЕНТИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: ПРАВОВІ КОЛІЗІЇ ТА НАПРЯМИ РЕФОРМУВАННЯ

ВСП «Фаховий коледж вимірювань Державного університету інтелектуальних технологій і зв’язку»
z0634280810@gmail.com

***Анотація.** Тези доповіді присвячено комплексному аналізу сучасного стану, проблем та перспектив розвитку адміністративно-правових методів забезпечення інформаційної безпеки в Україні в умовах євроінтеграції. У роботі виявлено ключові матеріальні колізії чинного законодавства. Зокрема, досліджено кризу санкцій Кодексу України про адміністративні правопорушення (КУпАП) за делікти у сфері захисту персональних даних. Особливу увагу приділено нормативному розриву перехідного періоду після прийняття Закону України № 4336-IX та правовому вакууму в регулюванні використання генеративного штучного інтелекту персоналом. На основі аналізу доктрини інформаційного права та європейських стандартів запропоновано конкретні напрями реформування вітчизняного законодавства, включаючи перехід до системи диференційованих оборотних штрафів та автоматизованого комплаєнсу.*

***Ключові слова:** інформаційне право, адміністративна відповідальність, захист інформації, штучний інтелект, кібербезпека, персональні дані, правова колізія.*

Стрімкий розвиток цифрових технологій, масштабне впровадження хмарних обчислень та систем штучного інтелекту, а також перманентні кіберзагрози в умовах воєнного стану вимагають радикального переосмислення системи забезпечення інформаційної безпеки України. Адміністративно-правові інструменти захисту інформації (інститути ліцензування, сертифікації, державного нагляду та адміністративної відповідальності) є базисом, що визначає легітимні межі та правила поведінки суб'єктів інформаційних правовідносин. Проте діюче законодавство України наразі демонструє системний розрив між технологічними реаліями та правовим інструментарієм його регулювання, що актуалізує необхідність виявлення наявних колізій та обґрунтування векторів реформування.

Так, першою проблемою, яку хотілося б відзначити, є певна диспропорція між реальним характером кіберзагроз і заходами адміністративного примусу, закріпленими у КУпАП. Зокрема, санкції за ст. 188-31

(невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України) та ст. 188-39 (порушення законодавства у сфері захисту персональних даних) передбачають максимальні штрафи на рівні від 100 до 2000 неоподатковуваних мінімумів доходів громадян (що еквівалентно кільком тисячам або десяткам тисяч гривень) [4]. У наукових працях вітчизняних адміністративістів (зокрема, у дослідженнях І. Ковбаса, А. Стрельникова та ін.) наголошується, що за таких умов адміністративне стягнення повністю втрачає свою превентивну (запобіжну) та правовідновлювальну функції, перетворюючись на суто номінальний «податок на правопорушення». Науковці підкреслюють, що чинний каральний інструментарій КУпАП моделювався за радянським зразком і розрахований на індивідуальних суб'єктів або дрібні посадові провини, а тому є абсолютно неадаптованим до деліктів у цифровому середовищі.

Юристи-практики (зокрема, експерти з Digital Law та комплаєнсу) констатують, що для ІТ-компаній або операторів критичної інфраструктури сплата мінімального штрафу є економічно вигіднішою, ніж фінансування високовартісних організаційно-технічних заходів із кіберзахисту. В умовах, коли масштабний витік інформації здатний завдати матеріальних збитків на мільйони гривень, призвести до компрометації військовослужбовців або підірвати національну безпеку держави, такий правовий лібералізм є недопустимим [5].

Додатково виникає гостра правова колізія із євроінтеграційними зобов'язаннями України. Генеральний регламент про захист даних ЄС (GDPR) та нова європейська Директива з кібербезпеки NIS2 оперують концепцією «ефективних, пропорційних та стримувальних» санкцій, встановлюючи штрафи до 10–20 мільйонів євро або до 2–4% від загального світового річного обороту компанії за аналогічні правопорушення. Відтак, подолання кризи матеріальних санкцій КУпАП вимагає не просто механічного підвищення фіксованих штрафів, а концептуального переходу до диференційованих оборотних фінансово-адміністративних санкцій для юридичних осіб [2]. Вважаємо, що необхідно здійснити перехід від фіксованих мізерних штрафів до європейської практики оборотних штрафів - стягнення відсотків від загального річного обороту компанії-порушника.

Істотним деструктивним чинником у системі адміністративно-правових методів є інституційна криза перехідного періоду, викликана прийняттям Закону України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [6]. Цей нормативно-правовий акт ознаменував довгоочікувану відмову від архаїчної та надмірно бюрократизованої моделі Комплексних систем захисту інформації (КСЗІ) на користь сучасного ризикоорієнтованого підходу та впровадження інституту CISO (офіцерів з кібербезпеки). Проте імплементація закону натрапила на класичну юридичну проблему - системне відставання підзаконного нормативно-правового регулювання.

У сучасних дослідженнях Інституту держави і права імені В. М. Корецького НАН України та роботах фахівців з інформаційного права (зокрема, К. Белякова, Р. Гринюка та ін.) зазначається, що заміна застарілого закону без миттєвого оновлення масиву відомчих інструкцій породжує так звану «правову асиметрію». Прийнятий закон вимагає гнучкого управління ризиками, побудови профілів безпеки та оцінки реальної технологічної стійкості ІТ-інфраструктури. Водночас посадові особи контролюючих та наглядових органів під час проведення реальних перевірок керуються чинними підзаконними актами (наказами відомств, положеннями, методичними рекомендаціями НД ТЗІ), які де-юре залишаються орієнтованими на застарілу методологію КСЗІ [3].

Як свідчить сучасна правозастосовча практика та експертні звіти Держспецзв'язку щодо готовності суб'єктів до нових вимог, ці колізії змушують суб'єктів господарювання та державні установи функціонувати в умовах подвійних стандартів. Замість спрямування фінансових та інтелектуальних ресурсів на реальний кіберзахист і протидію актуальним загрозам, організації змушені утримувати «паперовий комплаєнс» - дублювати стоси застарілої звітності та журналів обліку, щоб формально уникнути адміністративних претензій регуляторів. Як зазначається в офіційних роз'ясненнях Держспецзв'язку України щодо розбудови оновленої нормативної бази на виконання Закону № 4336-IX, практична реалізація реформи потребує скасування або системного перегляду значного масиву підзаконних актів. Наукова спільнота та експерти з кіберкомплаєнсу наголошують, що збереження чинності застарілих інструкцій створює правову асиметрію і штучно утримує «паперовий» характер захисту інформації замість оцінки реальних ризиків за європейськими стандартами [1]

І на останок, хотілося б відзначити відсутність національного адміністративно-правового регулювання використання генеративного штучного інтелекту (аналога європейського AI Act), що унеможливорює притягнення працівників до відповідальності за передачу конфіденційної інформації чи комерційної таємниці на публічні сервери ШІ-платформ, оскільки юридичний статус таких дій у трудовому та адміністративному

праві не визначений. Найбільш динамічним і водночас найменш урегульованим викликом для сучасної системи адміністративно-правових методів захисту є стрімке впровадження генеративного штучного інтелекту в корпоративні та державні управлінські процеси. Головна проблема полягає у відсутності профільного національного законодавства (на кшталт Регламенту ЄС про штучний інтелект - EU AI Act), що створює глибокий правовий вакуум при спробах правової кваліфікації дій персоналу. Працівники масово використовують публічні хмарні платформи (ChatGPT, Microsoft Copilot тощо) для оптимізації роботи, завантажуючи туди фрагменти вихідного коду, бази даних клієнтів, фінансову звітність чи тексти конфіденційних службових документів.

У наукових дослідженнях проблем правового регулювання цифрових трансформацій (зокрема, у працях О. Баранова, Ю. Базанова, а також у звітах Науково-дослідного інституту інтелектуальної власності НАПрН України) акцентується увага на тому, що завантаження даних у публічні нейромережі де-факто є неконтрольованим витоком інформації (Data Leakage), оскільки ці дані стають власністю компаній-розробників ІІІ для подальшого навчання моделей. Проте де-юре притягнути такого працівника до адміністративної чи дисциплінарної відповідальності за розголошення комерційної таємниці чи конфіденційної інформації є вкрай складним юридичним завданням.

Юристи-практики та фахівці з трудового права зазначають, що чинний КЗпП України та КУпАП моделювалися в епоху матеріальних або класичних електронних носіїв. Оскільки чинне законодавство не визначає правового статусу «передачі даних третій стороні у вигляді ІІІ-запитів», суди часто трактують такі дії працівників як ненавмисні або як такі, що не мали прямого умислу на заподіяння шкоди. Наукова спільнота наголошує, що розв'язання цієї проблеми потребує негайної адаптації національного адміністративного права: закріплення легального визначення технологій ІІІ, розробки державних стандартів AI Governance для підприємств та нормативного визначення несанкціонованого вивантаження даних у публічні моделі як окремого складу адміністративного правопорушення у сфері інформаційної безпеки.

Висновки. Таким чином, адміністративно-правові інструменти захисту інформації в Україні потребують негайного звільнення від залишків застарілого бюрократичного підходу. Перехід до жорстких фінансових санкцій та нормативне врегулювання новітніх технологій є єдиним шляхом побудови дієвої та суверенної системи інформаційної безпеки держави, інтегрованої в європейський правовий простір.

Література

1. Де знайти всі документи, на які спирається реалізація Закону № 4336. *НВ Бізнес*. 2026. URL: <https://nv.ua/ukr/ukraine/events/zakon-4336-ix-klyuchovi-normativi-ta-pidzakonni-akti-dlya-kiberbezpeki-ukrajini-50624451.html> (дата звернення: 12.08.2026).

2. Духовна О. Вчимося на помилках: найбільші штрафи за порушення норм GDPR. *Юридична Газета*. 2020. № 10 (716). URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vchimosya-na-romilkah-nauybilshi-shtrafi-za-porushennya-norm-gdpr.html> (дата звернення: 12.08.2026).

3. Зміни в системі кіберзахисту України: фахівці кажуть, що більшість установ та компаній не готові до нових вимог. *Центр прав людини ZMINA*. 2026. URL: <https://zmina.info/news/zminy-u-systemi-kiberzahystu-ukrayiny-fahivczi-kazhut-shho-bilshist-ustanov-ta-kompanij-ne-gotovi-do-novyh-vymog/> (дата звернення: 12.08.2026).

4. Кодекс України про адміністративні правопорушення : Закон України від 07 груд. 1984 р. № 8073-X (із змінами та доповненнями). *Відомості Верховної Ради Української РСР*. 1984. Додаток до № 51. Ст. 1122. URL: rada.gov.ua (дата звернення: 10.08.2026).

5. Передача персональних даних третім особам: захист та відповідальність. *Digital Law*. 2025. URL: <https://digitallaw.com.ua/peredacha-personalnykh-danykh-tretim-osobam-zakhyst-ta-vidpovidalnist/> (дата звернення: 12.08.2026).

6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури: Закон України від 27 берез. 2025 р. № 4336-IX. *Відомості Верховної Ради України*. 2025. № 35. Ст. 134. URL: rada.gov.ua (дата звернення: 12.08.2026).

Наукове видання

ПЕРСПЕКТИВНІ НАПРЯМИ
ЗАХИСТУ ІНФОРМАЦІЇ

Матеріали
VIII Міжнародної
науково-практичної конференції

26—28 серпня 2026 року
м. Одеса

Надруковано з готового оригінал-макета
в авторській редакції

Завідувачка редакції Т. М. Забанова

Формат 60x84/8. Ум. друк. арк. 20,93.
Тираж 100 прим. Зам. № 234 (77).

Видавництво і друкарня «Астропринт»
65091, м. Одеса, вул. Разумовська, 21
Тел.: (0482) 37-14-25, 33-07-17, (048) 7-855-855
e-mail: astro_print@ukr.net; www.astroprint.ua

Свідоцтво суб'єкта видавничої справи ДК № 1373 від 28.05.2003 р.