ПНЗІ - 8 - 2026

ДУІТЗ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНТЕЛЕКТУАЛЬНИХ
ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

ДУІКТ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

МАТЕРІАЛИ
VIII МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ

ПНЗІ — ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ 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

УДК 004.056
П26

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

П26 **Перспективні** напрями захисту інформації : матеріали VIII Міжнародної науково-практичної конференції (26-28 серпня 2026 р., м. Одеса) / Держ. ун-т інтелектуал. технологій і зв'язку ; Держ. ун-т інформ.-комунікац. 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

ISBN 978-617-8714-60-4

© ДУІТЗ, ДУІКТ, 2026

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;
Василіу 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	*Азаров Іван Сергійович, Азаров Ілля Сергійович* **НОРМАТИВНО-ПРАВОВІ АСПЕКТИ ІДЕНТИФІКАЦІЇ АНОНІМНИХ КОРИСТУВАЧІВ ДЛЯ ЗАХИСТУ КРИТИЧНИХ ІНФРАСТРУКТУР ВІД КІБЕРЗАГРОЗ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД**	8
2	*Соколов С.М.* **КІБЕРБЕЗПЕКА IIoT-ОРІЄНТОВАНОЇ СИСТЕМИ МОНІТОРИНГУ ТА АВТОМАТИЧНОГО ЗУПИНЕННЯ CNC-ОБЛАДНАННЯ**	12
3	*Грищук О. М., Грищук Р. В.* **ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ БЛОКЧЕЙН-ВУЗЛА ВІД КІБЕРАТАК НА ОСНОВІ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ МОДЕЛЕЙ**	15
4	*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**	17
5	*Черемнов М.В., Фразе-Фразенко О.О.* **СИНЕРГЕТИЧНИЙ МЕТОД БЕЗПЕРЕРВНОЇ АВТЕНТИФІКАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**	21
6	*Тимофєєв Д.С., Удовик І.М., Кручінін О.В.* **ПІДВИЩЕННЯ ОСВІЧЕНОСТІ З ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ В ПРОЦЕСІ ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ УНІВЕРСИТЕТУ**	23
7	*Гончаров М.О., Колованова Є.П., Малахов С.В.* **ОСНОВНІ СКЛАДОВІ КОНЦЕПЦІЇ БАГАТОРІВНЕВОГО МУЛЬТИПЛЕКСУВАННЯ ДАНИХ ПРИ РЕАЛІЗАЦІЇ ГІБРИДНОГО СТЕГАНОГРАФІЧНОГО АЛГОРИТМУ**	26
8	*Iurii Zhurov* **BASELINE CONTROL COVERAGE IN RESOURCE-CONSTRAINED ORGANIZATIONS: STRUCTURAL CAUSES OF CYBERSECURITY UNDERINVESTMENT IN SMALL BUSINESS**	30
9	*Зибін С.В., Прокопович-Ткаченко Д.І., Хохлачова Ю.Є.* **ПІДВИЩЕННЯ ЖИВУЧОСТІ МЕРЕЖІ В УМОВАХ ДЕФІЦИТУ ЕЛЕКТРОЕНЕРГІЇ ТА КІБЕРАТАК**	34
10	*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**	38
11	*Сіренко О. І.* **ОСОБЛИВОСТІ ВИЯВЛЕННЯ АТАК У КОНТЕЙНЕРИЗОВАНИХ СЕРЕДОВИЩАХ**	40
12	*Бектурсунов Д.Н., Копитін Ю.В., Копитіна М.В., Корчинський В.В., Мартинова О.М., Дунаєва В.В.* **МОДЕЛЬ ПРОЦЕСУ КІБЕРСТРАХУВАННЯ ДЛЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	43
13	*Царьов Р.Ю., Стайкуца С.В., Царьова Г.А.* **ЗАСОБИ ШТУЧНОГО ІНТЕЛЕКТУ, ЯК ПЕРСПЕКТИВНА МОДЕЛЬ ЗАГРОЗИ СИСТЕМІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	46
14	*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**	49
15	*Яневич О. К., Трифонова К. В., Чубарев О. В.* **ІНТЕРФЕРЕНЦІЙНІ ЗАВАДИ У СИСТЕМІ ПЕРЕДАЧІ BPLC ПРИ ВПЛИВІ ІМПУЛЬСНИХ БЛОКІВ ЖИВЛЕННЯ**	51
16	*Karpenko Y.V., Dubrovin V.I* **DETECT NETWORK ATTACKS: Quantum Implementation**	52
17	*Корченко А.О., Петченко М.В., Давиденко К.О.* **ПРОФІЛЮВАННЯ СОЦІОТЕХНІКА ЗА ОЗНАКАМИ ВИЯВЛЕНОЇ ФІШИНГ-АТАКИ**	56
18	*Шкурченко О.А., Аверічев І.М., Поночовний П.М.* **МЕТОД ДЕТЕКТУВАННЯ МУЛЬТИВЕКТОРНИХ АРТ-АТАК ІЗ ВИКОРИСТАННЯМ АНСАМБЛІВ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ**	58
19	*Бабенко К. Є.* **МОДЕЛЬ НАСКРІЗНОЇ ЗАТРИМКИ ДОСТУПУ ДО ОНОВЛЕНОГО СТАНУ ПРОГРАМОВАНИХ БЛОКЧЕЙН-СИСТЕМ ПЕРШОГО РІВНЯ**	60

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

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

УДК 004(056.53::413.4)

[1]Мохор В.В., [2]Дорогий Я.Ю., [1]Ракович В.С., [1,3]Цуркан В.В.

ПОГЛЯД НА ПАРАДИГМУ ПОВІДОМЛЯННЯ ПРО ПОДІЇ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України [2]Донецький національний технічний університет
[3]Національний 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 виявляння і реагування на кіберінцидентах, кібератаках, кіберзагрозах. Серед основних джерел інформації про них виокремлено працівників об'єктів критичної інфраструктури. Ефективність даної діяльності зведено до необхідності визначання парадигми повідомляння 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 повідомляння 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, повідомляння про подію кібербезпеки, парадигма повідомляння, механізм повідомляння, погляд на парадигму.*

Унеможливлювання 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 виявляння 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 визначання і, як наслідок, викладання погляду на парадигму повідомляння 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 – імплементовувати найкращі світові практики для виявляння 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 виявляння, 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] виявляння 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, відновляння сталого та надійного надання життєво важливих функцій та/або послуг [8]. Так, за Національним планом реагуванню на інциденти передує підготовляння. У його межах передбачається вивчання і досліджування відомих кіберінцидентів, кібератак, кіберзагроз, а також розробляння відповідних методів і механізмів протидіяння. Завдяки цьому створюються організаційні, технічні, кадрові умови, зокрема, взаємодіяння з керівниками, підрозділами кіберзахисту. Протягом виявляння, аналізування, інформування про кіберінциденти отримується, обробляється і передається інформація про події. Вони можуть відноситися до одного з класів: кіберінцидент, кібератака, кіберзагроза. Повідомляння про них передбачено безперервно в режимі реального часу. Серед джерел виявляння кіберінцидентів, кібератак, кіберзагроз виокремлено суб'єктів національної системи реагування, забезпечування кібербезпеки та працівників. Тоді як протягом стримування, усування наслідків та відновляння 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 виявляння і реагування на інциденти кібербезпеки об'єктів критичної інфраструктури є повідомляння про події. Для цього передбачається збирання і обробляння наявної інформації. Тож доцільно визначати 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 визначання основ повідомляння працівниками об'єктів критичної інфраструктури про події кібербезпеки. Насамперед йдеться про потенційні джерала інформації, діяльність, дії, правила, формат повідомлення. Загалом це дозволить визначити парадигму і, як наслідок, механізм повідомляння про події кібербезпеки. Такий погляд підтверджується настановами гармонізованого в Україні міжнародного стандарту ISO/IEC 27001 (додаток A, 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 виявляння і реагування на інциденти є визначання основ повідомляння 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 повідомляння про події кібербезпеки враховуватимуться найкращі світові практики. Тоді як її використання для розробляння 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 джерала 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 повідомляння про події кібербезпеки об’єктів критичної інфраструктури. *Кібербезпека : освіта, наука, техніка*. 2026. Том 4, № 32. P. 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).