Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури

(реєстраційний номер 0122U200483,
термін виконання: 2022-2027р.)

Керівник наукової теми:

Наталія КОРШУН,
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, доктор технічних наук, професор

Мета дослідження:

забезпечення кібербезпеки
інформаційних систем переробки інформації
та функціональної безпеки програмно-технічних
комплексів управління критичної інфраструктури
в умовах впливу інформаційних загроз, ризиків
і невизначеностей.

Завдання:

розробка методик віднесення об’єктів інфраструктури до критично важливих та оцінки ступеню важливості інформаційних об’єктів критичної інфраструктури для безпеки держави;

аналіз основних інформаційних загроз, ризиків і невизначеностей для інформаційних систем переробки інформації та програмно-технічних комплексів управління критичної інфраструктури;

розробка методів та моделей забезпечення захисту систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури з урахуванням інформаційних загроз, ризиків і невизначеностей.

План реалізації наукової теми

Етап	Дата виконання	Очікувані результати
Організаційний/ аналітичний	06.2022 - 11.2023	Вивчення та узагальнення світового досвіду забезпечення інформаційної безпеки критично важливих об'єктів. Опрацювання ключових термінів і понять
Дослідницький	12.2023 - 02.2026	Розробка методики віднесення об’єктів інфраструктури до критично важливих. Обґрунтування та розроблення методів і моделей забезпечення кібербезпеки систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури.
Узагальнюючий	03.2026 - 06.2027	Розробка практичних рекомендацій для органів державної влади та установ, що відносяться до критично важливих об'єктів інформатизації з метою підвищення рівня їх захищеності

Напрями:

I. Формування політик інформаційної безпеки підприємства на основі методології ZERO-TRUST

II. Natural Language Processing для систем моніторингу та реагування на інциденти інформаційної безпеки

III. Забезпечення захисту інформації в мережах інтернету речей (IoT)

IV. Класична, квантова та постквантова криптографія

Основні проміжні теоретичні і практичні результати виконання наукової теми

Липень 2022 - Травень 2025

Напрями:

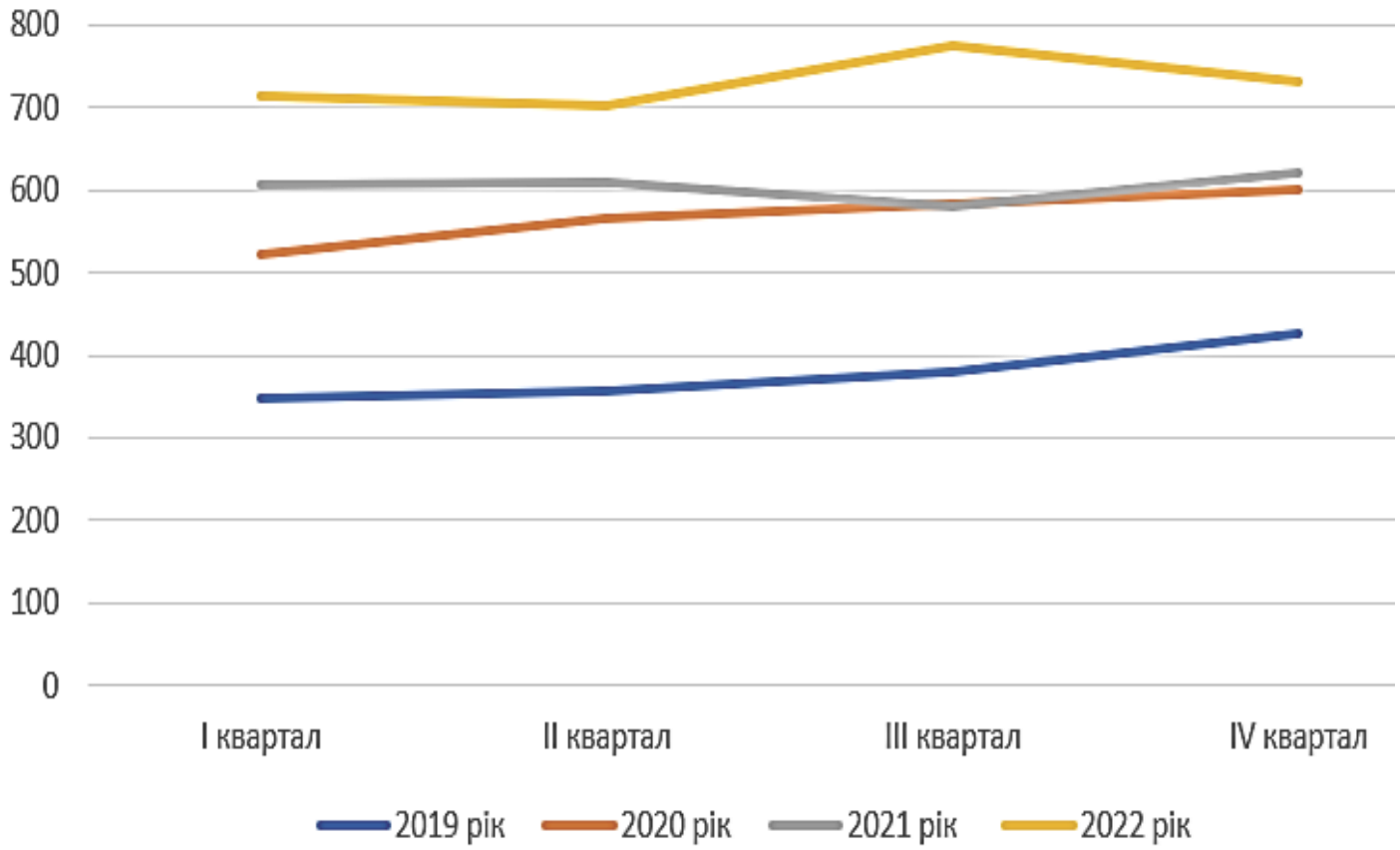
I. Формування політик інформаційної безпеки підприємства на основі методології ZERO-TRUST

II. Natural Language Processing для систем моніторингу та реагування на інциденти інформаційної безпеки

III. Забезпечення захисту інформації в мережах інтернету речей (IoT)

IV. Класична, квантова та постквантова криптографія

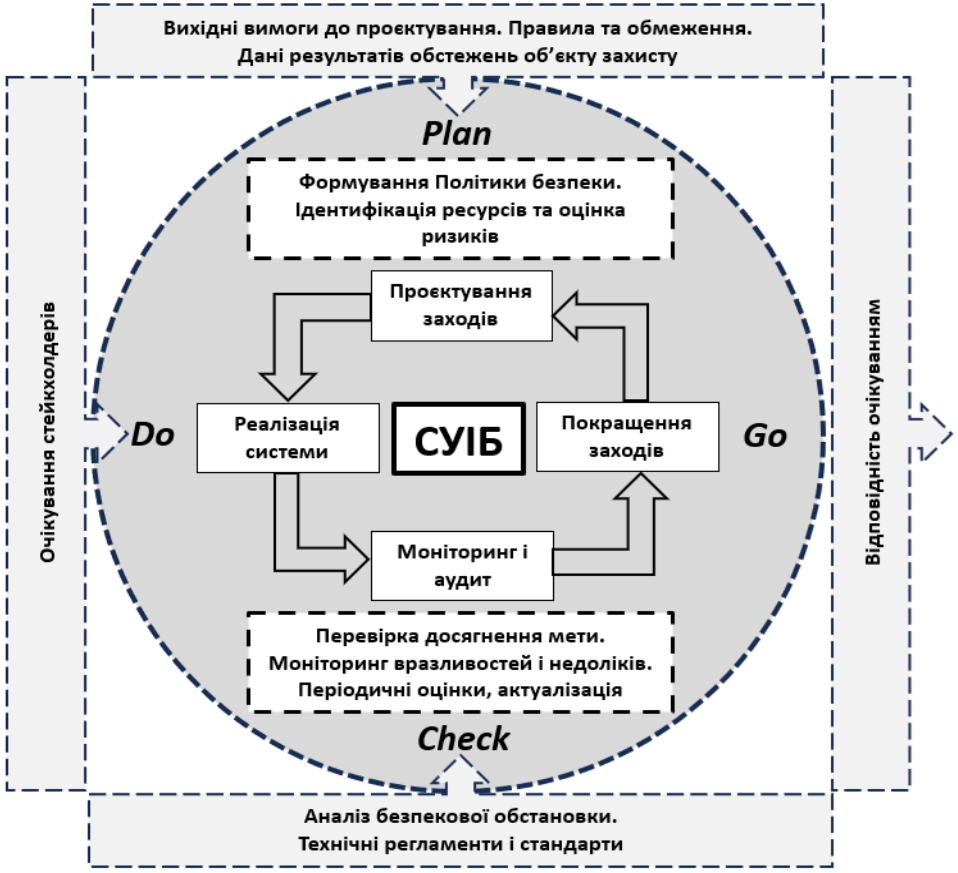
Діаграма кількості випадків кіберінцидентів за кварталами



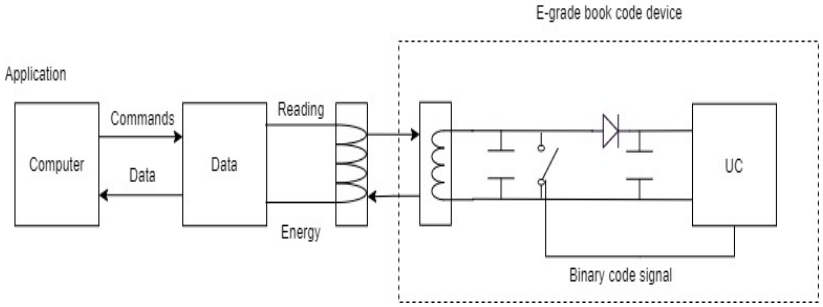
Узагальнені дані щодо кількості кіберінцидентів в світі в 2019–2022 роках

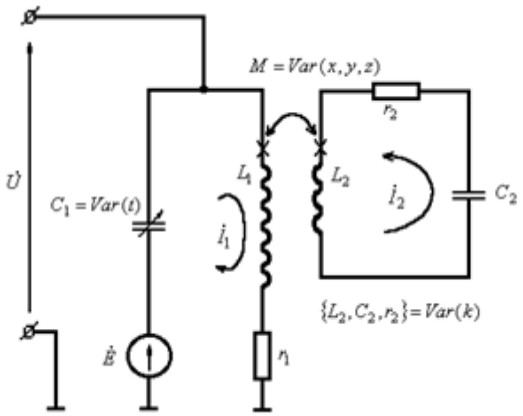
Квартал / Рік	I	II	III	IV	Загалом за рік	Середнє a	Стандартне відхил. σ
2019	347	357	379	425	1508	377,00	60,1
	0,2301	0,2368	0,2513	0,2818	← Відносні частоти		
2020	521	567	583	600	2271	567,75	58,81
	0,2294	0,2497	0,2567	0,2642	← Відносні частоти		
2021	607	609	580	622	2418	604,50	30,55
	0,2510	0,2519	0,2399	0,2572	← Відносні частоти		
2022	714	702	774	731	2921	730,25	50,12
	0,2444	0,2403	0,2650	0,2503	← Відносні частоти		
Загалом за квартал	2189	2235	2316	2378	9118	2279,50	145,62
	0,2401	0,2451	0,2540	0,2608	← Відносні частоти		

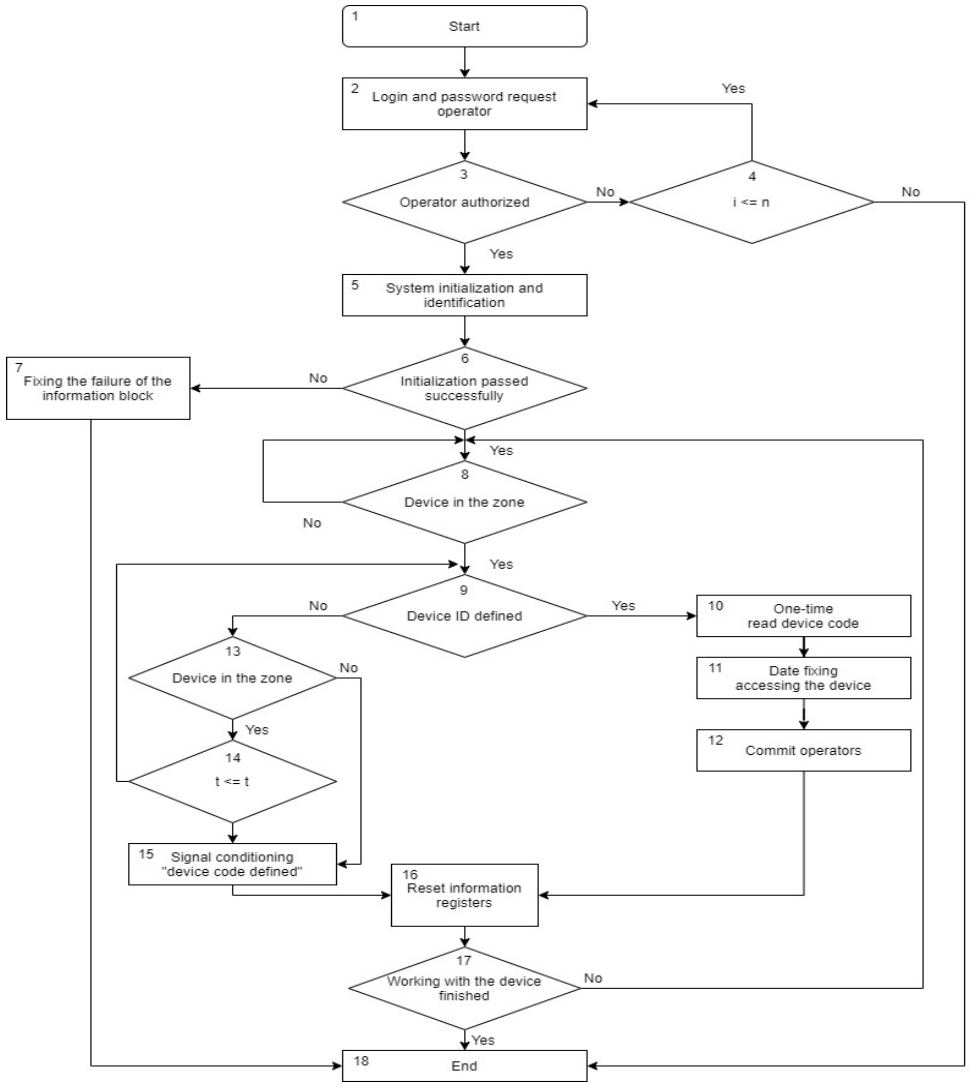
Вдосконалено методику оперативної оцінки поточного стану корпоративної кіберкультури на основі анкетування персоналу та математичного апарату обробки даних, що сукупно з методикою оцінки трендів загроз кібербезпеки дає **можливість оперативного реагування** з боку менеджменту безпеки в частині корегування політики безпеки та впровадження організаційних і навчальних заходів.



Запропоновано та математично обґрунтовано метод автентифікації користувачів корпоративної мережі на основі стеганографічного протоколу обміну даними автентифікації згідно з політикою безпеки з урахуванням концепції zero-trust.







Напрями:

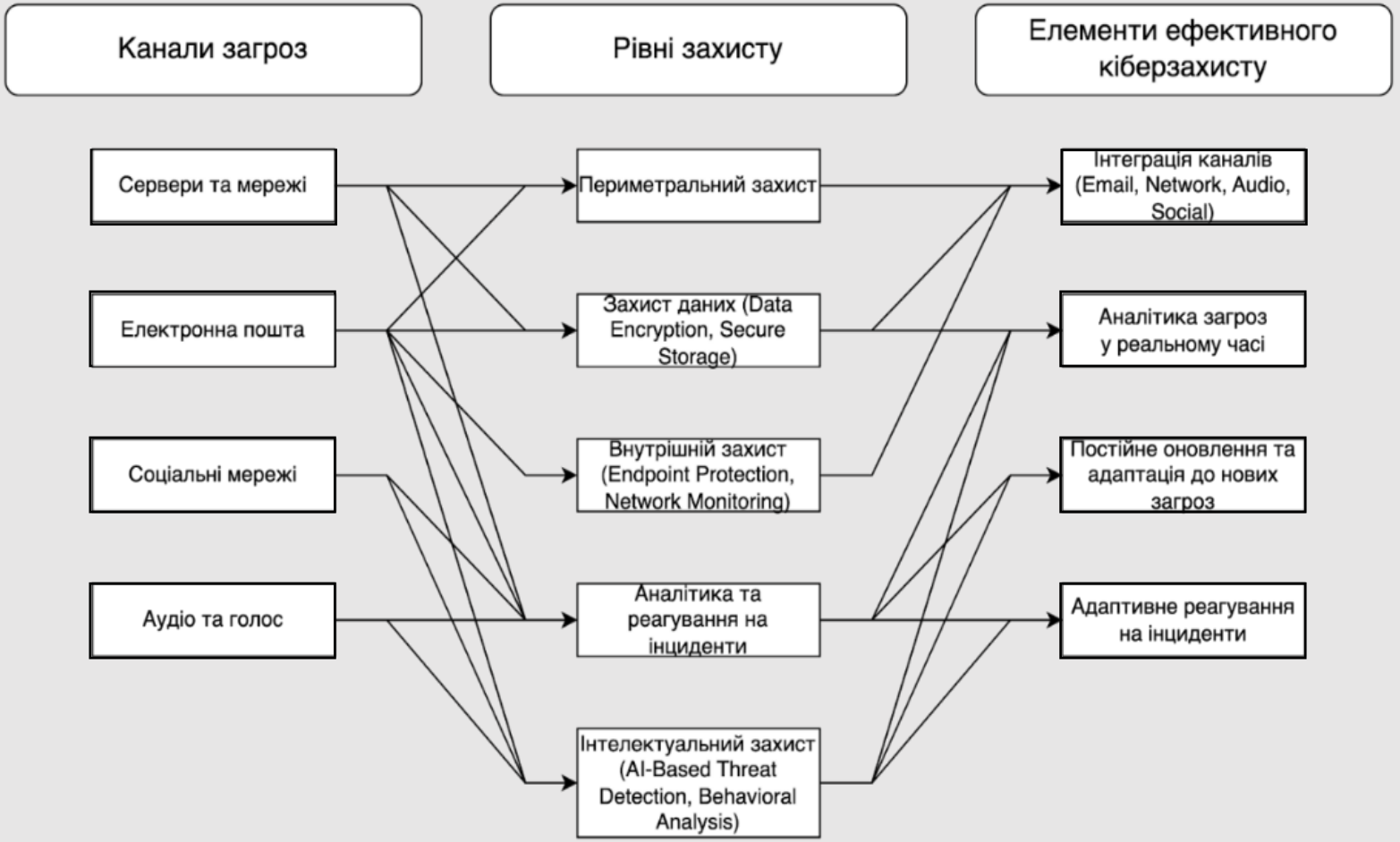
I. Формування політик інформаційної безпеки підприємства на основі методології ZERO-TRUST

II. Natural Language Processing для систем моніторингу та реагування на інциденти інформаційної безпеки

III. Забезпечення захисту інформації в мережах інтернету речей (IoT)

IV. Класична, квантова та постквантова криптографія

ПРОБЛЕМА: сучасні загрози складні + інтегровані в декілька каналів одночасно.



Взаємозв'язок каналів загроз, рівнів захисту та елементів кіберзахисту

Одним з найскладніших для аналізу і водночас найбільш натуральним є **канал голосової інформації.** Аудіоінформація вбудована в усі сфери життя людини і тим чи іншим чином в більшість каналів придатних для атаки.

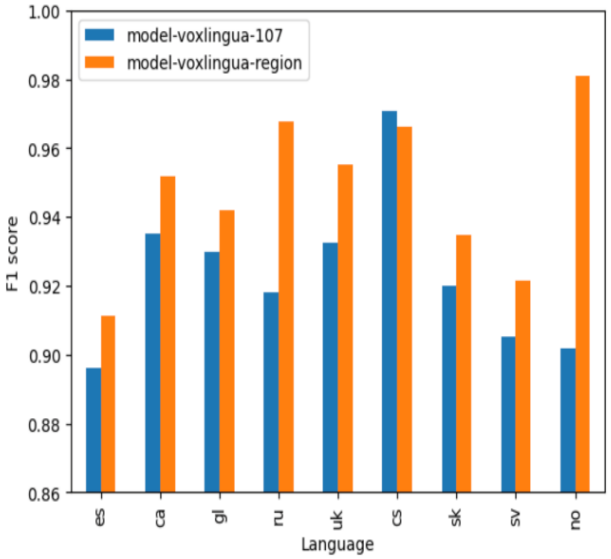
Елементи кібербезпеки в системах розпізнавання голосової інформації

Запропоновано метод підвищення точності розпізнавання природної мови для близькоспоріднених мов:
при розпізнаванні природної мови пріоритет – на точності.

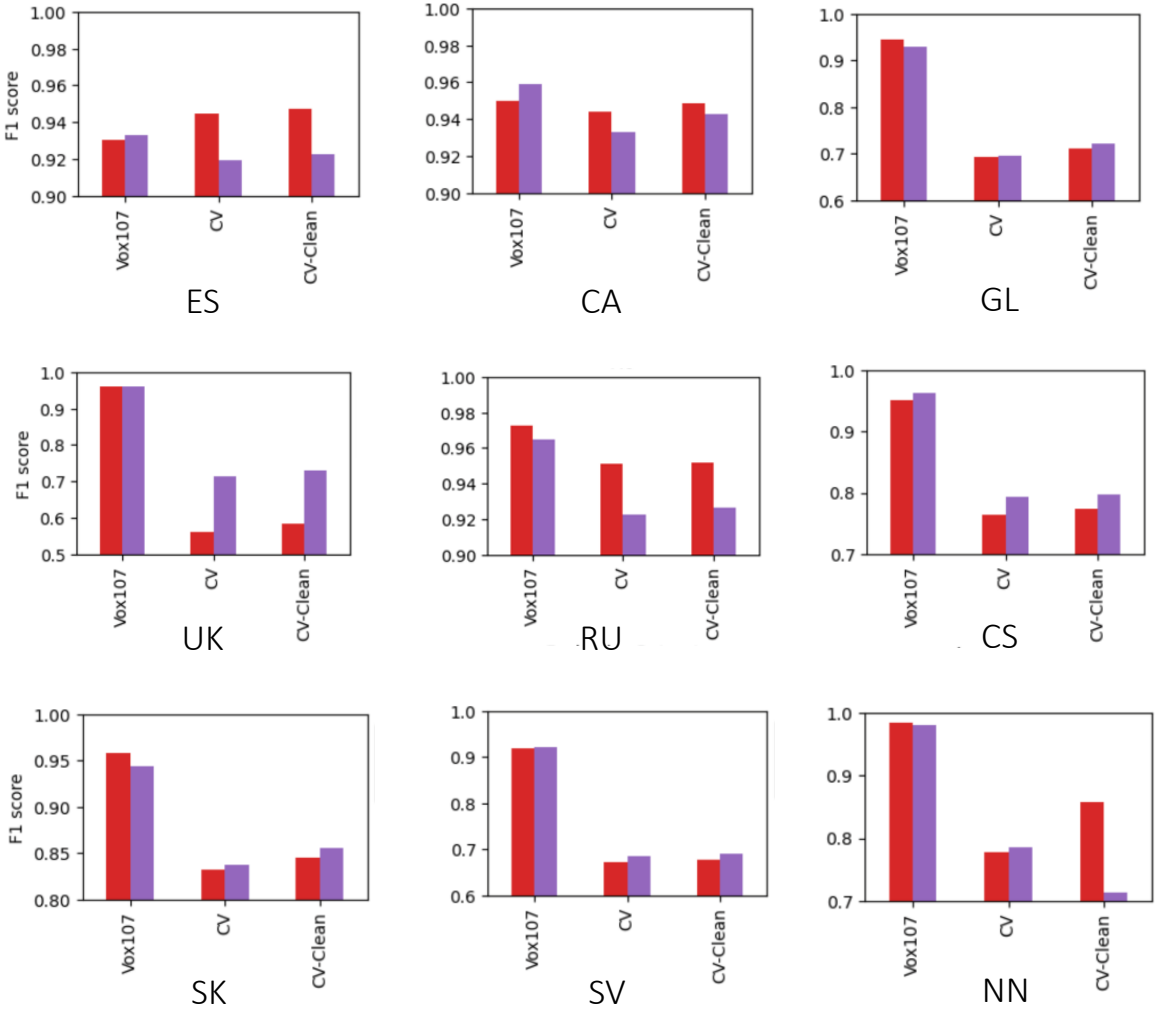
Результати моделей оцінювання для різних мов для чотирьох емоцій

Мова набору даних	Мова моделі							
	ZN	DE	ET	EN	FA	FR	UR	Медіана
ZN	0,90	0,47	0,34	0,31	0,48	0,44	0,52	0,47
DE	0,39	0,73	0,49	0,41	0,53	0,36	0,25	0,41
ET	0,26	0,30	0,34	0,30	0,26	0,30	0,26	0,30
EN	0,27	0,45	0,33	0,86	0,33	0,37	0,39	0,37
FA	0,21	0,19	0,48	0,24	0,55	0,29	0,33	0,29
FR	0,28	0,27	0,30	0,23	0,25	0,66	0,23	0,27
UR	0,27	0,17	0,32	0,29	0,36	0,25	0,83	0,29
Медіана	0,27	0,30	0,34	0,30	0,36	0,36	0,33	

Діаграми точності



для моделі, навченої регіонами, порівняно з уніфікованою VoxLingua107 моделлю



для моделей, навчених на наборах даних

Напрями:

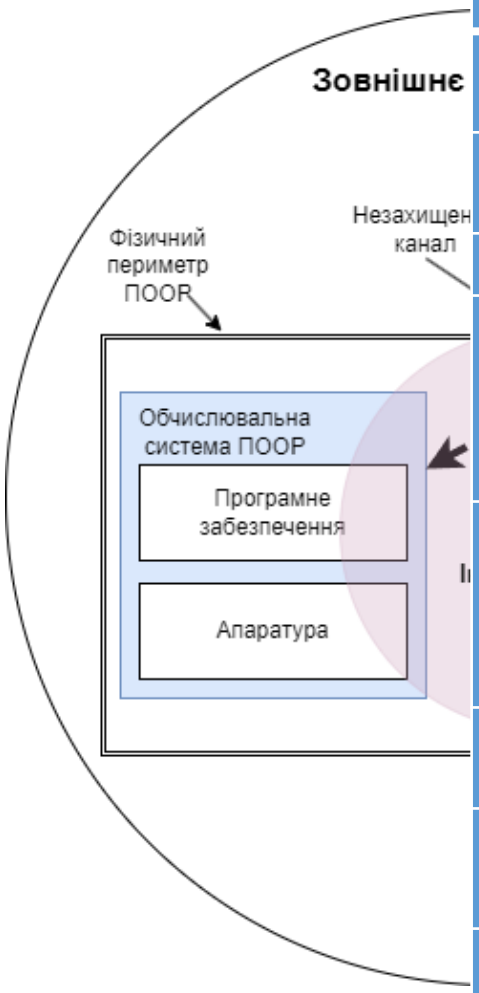
I. Формування політик інформаційної безпеки підприємства на основі методології ZERO-TRUST

II. Natural Language Processing для систем моніторингу та реагування на інциденти інформаційної безпеки

III. Забезпечення захисту інформації в мережах інтернету речей (IoT)

IV. Класична, квантова та постквантова криптографія

Розроблено модель загроз для побудови системи захисту інформації, що обробляється пристроями з обмеженими обчислювальними ресурсами в мережі IoT



№	Загроза	Зміст загрози	Ймовірність	Рівень шкоди
1.	Перехоплення	Отримання доступу до конфіденційної інформації	Висока	Високий
2.	Модифікація	Порушення цілісності даних що передаються	Висока	Високий
3.	Фальсифікація	Створення фіктивних даних	Середня	Високий
4.	НСД	Доступ до критичних параметрів віддалених пристроїв з метою їх спотворення або перехоплення	Висока	Високий, підвищує небезпеку реалізації інших загроз
5.	Підміна	Підміна блоків та вузлів віддалених пристроїв з метою імітації недійсної обстановки	Середня	Високий, підвищує небезпеку реалізації інших загроз
6.	Вірус	Ураження злоякісними кодами з боку мережі	Середня	Середня
7.	DDoS	Блокування роботи віддалених пристроїв з боку мережі	Середня	Середня
8.	Фізичний доступ	Отримання фізичного доступу до пристрою з метою порушення його функціональності, доступу до прошивки.	Середня	Середня

Розроблено метод криптографічного захисту інформації в мережі IoT, який забезпечує підвищену стійкість шифрування та імітостійкість. Метод базується на модифікованому алгоритмі A5/1 із застосуванням байтової обробки інформації та вузла накладання шифру на основі змінного латинського квадрату.

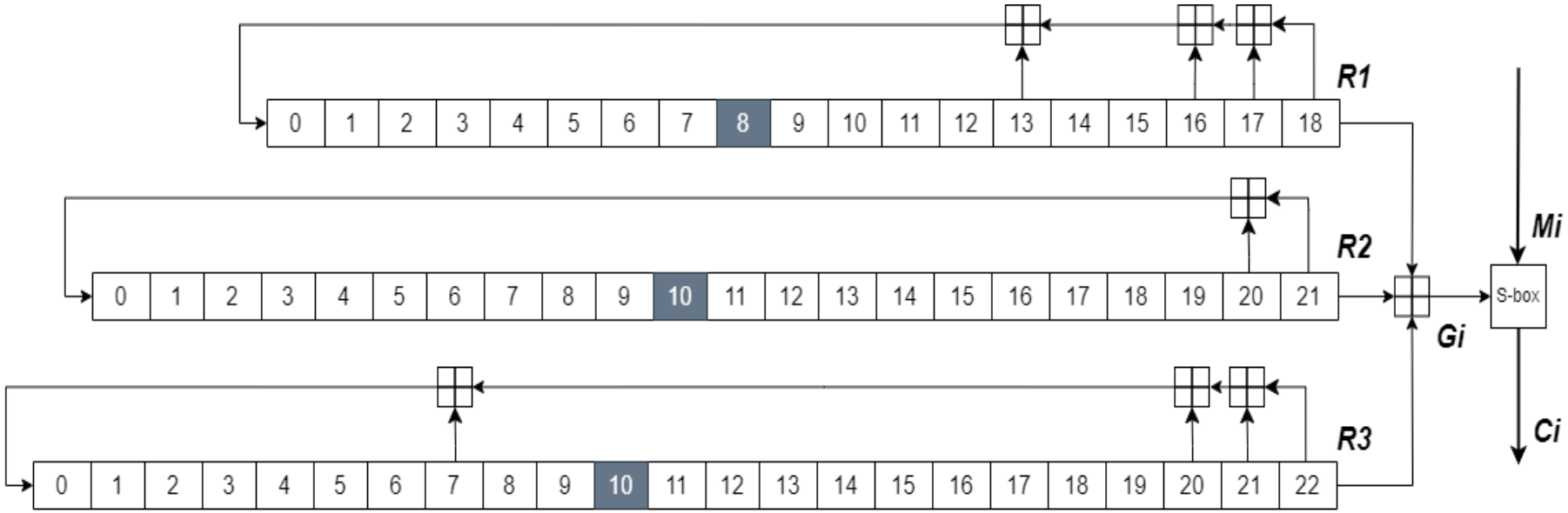
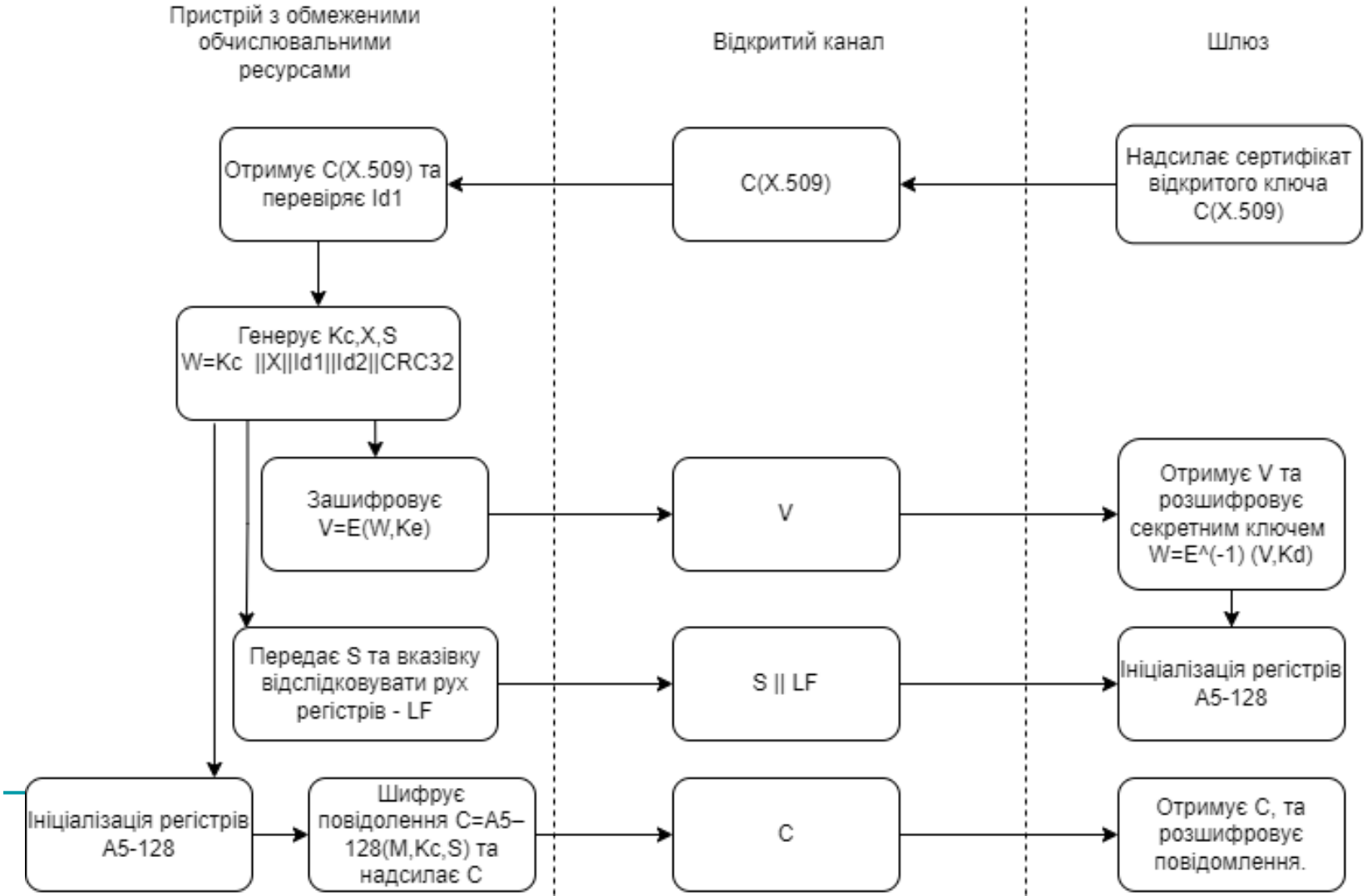


Схема керування рухом регістрів

$F = R1[8] \,\&\, R2[10] \mid R1[8] \,\&\, R3[10] \mid R2[10] \,\&\, R3[10]$

$Rn == F \rightarrow Rn = Rn+1$

Вдосконалено стандартний протокол Shockburst безпроводового інформаційного обміну в мережі з метою безпечного формування сеансових ключів та забезпечення криптографічно захищеної передачі даних від пристроїв з обмеженими обчислювальними ресурсами до шлюзу.



Напрями:

I. Формування політик інформаційної безпеки підприємства на основі методології ZERO-TRUST

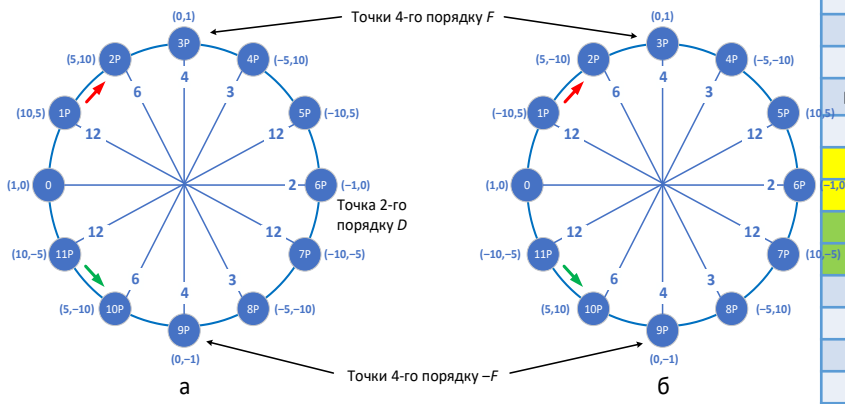
II. Natural Language Processing для систем моніторингу та реагування на інциденти інформаційної безпеки

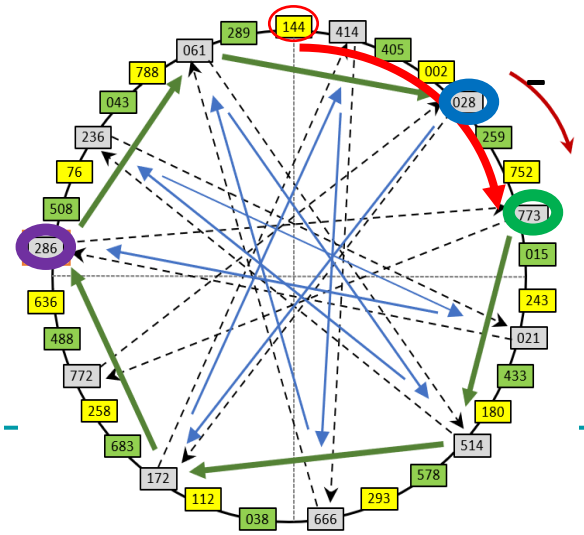
III. Забезпечення захисту інформації в мережах інтернету речей

IV. Класична, квантова та постквантова криптографія

Розроблено метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари

Модель 12-го порядку циклічних груп точок:

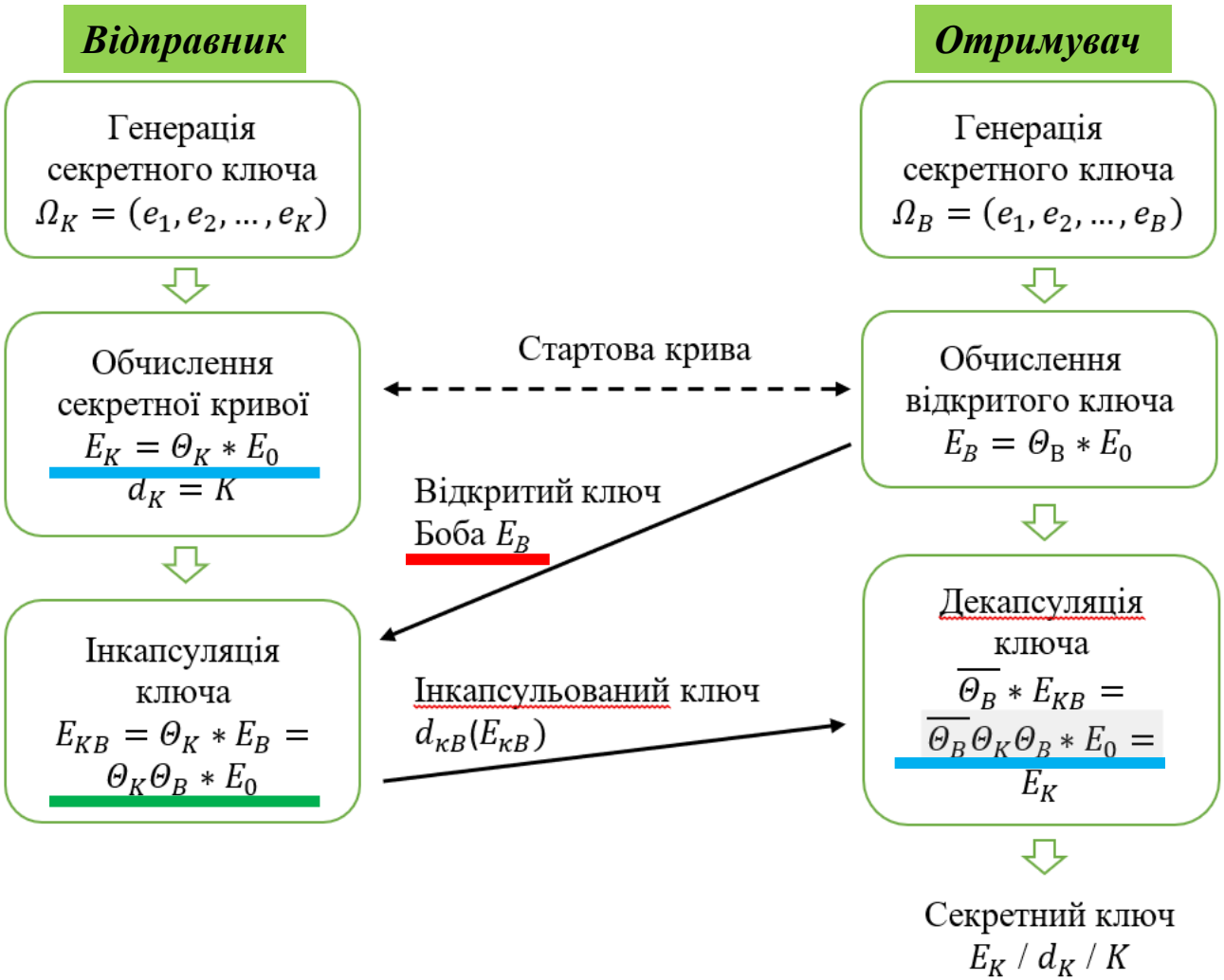




Група	Порядок	1P	2P	3P	4P	5P	6P
1	6	(5,10)	(–5,10)	(–1,0)	(–5,–10)	(5,–10)	(1,0)
2	6	(5,–10)	(–5,–10)	(–1,0)	(–5,10)	(5,10)	(1,0)
пункт	6	6	3	2	3	6	—
		1P	2P	3P	4P	5P	6P
3	3	(–5,10)	(–5,–10)	(1,0)	—	—	—
4	3	(–5,–10)	(–5,10)	(1,0)	—	—	—
пункт	3	3	3	—	—	—	—
		1P	2P	3P	4P	5P	6P
5	12	(10,5)	(5,10)	(0,1)	(–5,10)	(–10,5)	(–1,0)
6	12	(10,–5)	(5,–10)	(0,–1)	(–5,–10)	(–10,–5)	(–1,0)
7	12	(–10,5)	(5,–10)	(0,1)	(–5,–10)	(10,5)	(–1,0)
8	12	(–10,–5)	(5,10)	(0,–1)	(–5,10)	(10,–5)	(–1,0)
9	12	(6,11)	(5,–10)	(∞,9)	(–5,–10)	(–6,11)	(–1,0)
10	12	(6,–11)	(5,10)	(∞,–9)	(–5,10)	(–6,–11)	(–1,0)
11	12	(–6,11)	(5,10)	(∞,9)	(–5,10)	(6,11)	(–1,0)
12	12	(–6,–11)	(5,–10)	(∞,–9)	(–5,–10)	(6,–11)	(–1,0)
пункт	12	12	6	4	3	12	2
		7P	8P	9P	10P	11P	12P
5	12	(–10,–5)	(–5,–10)	(0,–1)	(5,–10)	(10,–5)	(1,0)
6	12	(–10,5)	(–5,10)	(0,1)	(5,10)	(10,5)	(1,0)
7	12	(10,–5)	(–5,10)	(0,–1)	(5,10)	(–10,–5)	(1,0)
8	12	(10,5)	(–5,–10)	(0,1)	(5,–10)	(–10,5)	(1,0)
9	12	(–6,–11)	(–5,10)	(∞,–9)	(5,10)	(6,–11)	(1,0)
10	12	(–6,11)	(–5,–10)	(∞,9)	(5,–10)	(6,11)	(1,0)
11	12	(6,–11)	(–5,–10)	(∞,–9)	(5,–10)	(–6,–11)	(1,0)
12	12	(6,11)	(–5,10)	(∞,9)	(5,10)	(–6,11)	(1,0)
пункт	12	12	3	4	6	12	—
		1P	2P	3P	4P	5P	6P
13	6	(11,6)	(–5,–10)	(–9,∞)	(–5,10)	(11,–6)	(1,0)
14	6	(11,–6)	(–5,10)	(–9,∞)	(–5,–10)	(11,6)	(1,0)
15	6	(–11,6)	(–5,10)	(9,∞)	(–5,–10)	(–11,–6)	(1,0)
16	6	(–11,–6)	(–5,–10)	(9,∞)	(–5,10)	(–11,6)	(1,0)
пункт	6	6	3	2	3	6	—

Розроблено модель інкапсуляції ключа CSIKE з рандомізацією з одним сеансом передачі і одним відкритим ключем замість двох у порівнянні з CSIDH.

Розроблено метод обчислення і вибору структури ізогеній у криптоалгоритмах CSIDH на кривих Едвардса



Розроблено метод CRS на несуперсингулярних кривих Едвардса та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса.

Масив значень 62-х параметрів *d* квадратичних та скручених несуперсингулярних кривих Едвардса ($a=\pm1$) при $p=863$, $\#E_d=840$, $\#E_{(-1,-d)}=888$ ($t=24$)

169*	400*	729	161*	818	210*	436*	309	43*	665*	840*
19	779	111	308	253*	116	705*	503*	32	573	472*
71	616*	618*	444*	302*	192	486	318*	852*	231	728*
300	113*	311*	858*	673*	725	589	75	684	551*	307
688	843	339	623	706	281	181*	27*	186*	652*	130
835*	409	345	283*	596	326*	236				

Масив значень 62-х параметрів *d* квадратичних та скручених несуперсингулярних кривих Едвардса ($a=\pm1$) при $p=863$, $\#E_d=888$, $\#E_{(-1,-d)}=840$ ($t=24$)

6*	678*	703*	212*	611*	420*	248*	159*	821*	562*	538*
546*	12*	581*	136*	654*	464*	438*	313*	361*	191*	392*
837*	29*	199*	246*	683*	695*	751*	24*	553*	—	—
144	849	685	460	613	150	87	38	226	453	470
49	72	254	514	128	478	664	670	153	122	284
697	744	425	214	513	488	732	36	103	—	—

Публікації

Статті – 128,
з них – **64** у виданнях, що індексуються
в НМБД Scopus та Web of Science.

Захист дисертацій - 4

Студентська наука

- Всеукраїнська науково-практична конференція молодих науковців «Інформаційні технології», ISSN: 2664-2638 (Online) (щороку)
- Студентська наукова конференція «Студентський науковий пошук» (щороку)
- Публікації у фахових наукових виданнях

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Факультет інформаційних технологій та математики
Кафедра комп'ютерних наук
Кафедра математики і фізики
Кафедра інформаційної та кібернетичної безпеки
ім. професора Володимира Бурячка

ISSN: 2664-2638 (Online)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ – 2024

Збірник тез
XI Всеукраїнської науково–практичної конференції молодих учених

Секція 4
ТЕХНОЛОГІЇ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО–КОМУНІКАЦІЙНИХ СИСТЕМАХ

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра комп'ютерних наук

Затверджено на засіданні кафедри
комп'ютерних наук
протокол №10 від 06.11.2024

Студентський науковий пошук - 2024

Збірник тез
студентської наукової конференції

4 ЯКІСНА ОСВІТА

8 ГІДНА ПРАЦЯ ТА ЕКОНОМІЧНЕ ЗРОСТАННЯ

Впровадження

Наукові дослідження

Інститут програмних систем НАН України

Інститут телекомунікацій та глобального інформаційного простору НАН України

Ender Turing OÜ (Естонія)

PP 2 SPV Limited Liability Company (Польща)

Освітній процес, студентська наукова робота

Оновлення змісту навчальних дисциплін ОПП спеціальності «Кібербезпека та захист інформації»

Курсові роботи, магістерські кваліфікаційні роботи, участь у наукових конференціях, публікації у фахових виданнях

ДЯКУЮ ЗА УВАГУ!