УДК 004.056.5

№ держреєстрації 0121U112489

Інв. № _____

Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

61022, м. Харків, майдан Свободи, 4, факс +38 057 705-02-41,

тел. +38 057 705-12-47, +38 057 707-52-31; E-mail: univer@karazin.ua

ЗАТВЕРДЖУЮ

Проректор з наукової роботи

доктор фізико-математичних наук, професор

_____ В.О. Катрич

«23» 12 2021 р.

ЗВІТ

ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

ТА ЗАКЛЮЧНІ РЕЗУЛЬТАТИ РЕАЛІЗАЦІЇ ПРОЄКТУ 2020.01/0351

за договорами від 18.05.2021 № 191/01/0351 та 28.10.2020 № 79/01.2020

АНАЛІЗ, ДОСЛІДЖЕННЯ, РОЗРОБКА ТА ВПРОВАДЖЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ГЛОБАЛЬНОГО МОНІТОРИНГУ КІБЕРНЕТИЧНОГО ПРОСТОРУ УКРАЇНИ В УМОВАХ КРИЗОВИХ ТА НАДЗВИЧАЙНИХ СИТУАЦІЙ

грантова підтримка Національного фонду досліджень України

у межах конкурсу «Наука для безпеки людини та суспільства»

(остаточний)

Науковий керівник НДР (проєкту)

д-р техн. наук, доцент Р.В. Олійников

2021

Результати роботи розглянуто Вченою радою Харківського національного університету імені В.Н. Каразіна, протокол від «14» грудня 2021 р. № 11

СПИСОК АВТОРІВ

Науковий керівник НДР /Головний науковий співробітник, д-р техн. наук, доцент	(підпис) „14" 12 2021 р.	Р.В. Олійников, (розділи 5, 6)
Відповідальний виконавець Основний виконавець /Провідний науковий співробітник, канд. техн. наук	(підпис) „14" 12 2021 р.	М.О. Полуяненко, (розділ 1, 2)
Основний виконавець /Головний науковий співробітник, д-р техн. наук, професор	(підпис) „14" 12 2021 р.	О.О. Кузнецов, (вступ, розділи 1, 2, висновки)
Основний виконавець /Головний науковий співробітник, д-р техн. наук, професор	(підпис) „14" 12 2021 р	В.А. Краснобаєв, (вступ, розділи 1, 2)
Основний виконавець /Головний науковий співробітник, д-р техн. наук, доцент	(підпис) „14" 12 2021 р.	С.О. Кошман, (розділи 1, 2, висновки)
Основний виконавець /Головний науковий співробітник, д-р техн. наук, професор	(підпис) „14" 12 2021 р.	Д.В. Агеєв, (розділи 3, 4, 7, 8)

Основний виконавець /Головний науковий співробітник, д-р техн. наук, професор	_____ (підпис) „14" 12 2021 р.	О.В. Лемешко, (розділи 3, 4, 7, 8)
Основний виконавець /Головний науковий співробітник, д-р техн. наук, професор	_____ (підпис) „14" 12 2021 р.	Л.В. Ковальчук, (розділи 5, 6)
Основний виконавець /Провідний науковий співробітник, канд. фіз.-мат. наук	_____ (підпис) „14" XII 2021 р.	Ю.М. Беспалов, (розділи 5, 6)
Основний виконавець /Старший науковий співробітник, канд. техн. наук	_____ (підпис) „14" 12 2021 р.	Д.В. Іваненко, (розділ 1, 2)
Виконавець/Провідний науковий співробітник, канд. техн. наук, доцент	_____ (підпис) „14" 12 2021 р.	Т.А. Радівілова, (розділи 3, 4, 7, 8)
Основний виконавець /Провідний науковий співробітник, канд. техн. наук	_____ (підпис) „14" 12 2021 р.	Ю.І. Горбенко, (розділ 1, 2)
Основний виконавець /Старший науковий співробітник	_____ (підпис) „14" 12 2021 р.	А.С. Кіян, (розділ 1, 2)

Основний виконавець /Старший науковий співробітник _____ (підпис) М.Ю. Родінко, (розділи 5, 6)

„14" 12 2021 р.

Асистент/Науковий співробітник _____ (підпис) Т.Ю. Кузнецова, (розділ 1, 2)

„14" 12 2021 р.

Погоджено
Головний метролог _____ (підпис) О.Л. Гостєв

„14" 12 2021 р.

РЕФЕРАТ

Заключний звіт про НДР: 411 с., 63 рис., 21 табл., 2 дод., 147 джерел.

КІБЕРНЕТИЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА, МОНІТОРИНГ КІБЕРНЕТИЧНОГО ПРОСТОРУ, ДЕЦЕНТРАЛІЗОВАНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ, ПОДОЛАННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТА ПАНДЕМІЙ

Об’єкт дослідження – процеси забезпечення інформаційної та кібербезпеки, моделі, методи та механізми моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Предмет досліджень – технології інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Метою НДР є аналіз та дослідження сучасних вимог та загроз національної безпеки в інформаційній сфері, обґрунтування, розробка та впровадження ефективних технологій захисту інформації для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Методи дослідження: методи теорії захисту інформації, криптології, сучасних протоколів та технологій комп'ютерних мереж та систем, теорії систем та системного аналізу, комп’ютерного та імітаційного моделювання тощо.

В заключному звіті наводяться результати з: аналізу та дослідження децентралізованих технологій для побудови надійних та безпечних систем моніторингу запобігання поширення інфекційних захворювань; розробка моделей, методів і протоколів моніторингової системи запобігання поширення інфекційних захворювань та безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

ABSTRACT

Interim report: 411 pages, 63 figures, 21 tables, 2 appendices, 147 resources.

CYBERSECURITY, INFORMATION SECURITY, CYBERSPACE MONITORING, DECENTRALIZED SYSTEMS AND TECHNOLOGIES, OVERCOMING EMERGENCIES AND PANDEMICS

The object of research is the processes of providing information security and cybersecurity, models, methods and mechanisms for monitoring Ukraine cyberspace in crisis and emergency situations.

The subject of research is information security technologies for global monitoring of Ukraine cyberspace in the crisis and emergency situations.

The purpose of the work is to analyze and study modern requirements and threats to national security in the information sector, substantiation, development and implementation of effective information protection technologies for global monitoring of Ukraine cyberspace in crisis and emergency situations.

Research methods are methods of information security theory, cryptology, modern protocols and technologies of computer networks and systems, systems theory and systems analysis, simulation, etc.

The final report presents the results of: analysis and research of decentralized technologies for the construction of reliable and secure monitoring systems designed to prevent the spread of infectious diseases; development of models, methods and protocols of the monitoring system designed to prevent the spread of infectious diseases and secure routing of confidential messages in infocommunication networks.

ЗМІСТ

Перелік скорочень, умовних познак, одиниць і термінів 15
Вступ 17
1 Аналіз та дослідження алгоритмів КЗІ та протоколів взаємодії в децентралізованому середовищі при побудові надійних та безпечних систем моніторингу запобігання поширенню інфекційних захворювань 32
1.1 Аналіз можливостей застосування симетричної криптографії у системах моніторингу запобігання поширення інфекційних захворювань 33
1.1.1 Характеристика основних елементарних криптоперетворень симетричного типу 36
1.1.2 Блочні симетричні шифри, що можуть бути застосовані у системах моніторингу, та їх властивості 41
1.1.3 Поточні шифри для застосування у реальних моніторингових системах 42
1.1.4 Спрощена схема застосування та математична модель ПСШ 43
1.1.5 Оцінка властивостей потокового симетричного шифру 45
1.1.6 Застосування БСШ у режимах потокового шифрування 47
1.1.7 Уніфікація функцій потокових симетричних шифрів 50
1.2 Асиметричні криптосистеми як альтернатива для використання у якості базових криптографічних перетворень у системах моніторингу контактів 52
1.2.1 Криптосистема RSA 56
1.2.2 Криптоперетворення НШ в кільцях (RSA) 59
1.2.3 Проблемні питання крипто перетворень типу RSA. 63
1.2.4 Направлене шифрування у кільці зрізаних поліномів. Алгоритм NTRU. 64
1.3 Протоколи взаємодії, що можуть бути використані при реалізації систем моніторингу контактів. 69
1.3.1 Термінологічна база застосування протоколів 69

1.3.2 Протоколи автентифікації 71
1.3.3 Фази автентифікації 73
1.3.4 Основні положення надання послуг автентифікації 75
1.3.5 Протокол автентифікації Шнора 76
1.3.6 Протокол автентифікації Шнора на основі ЦП 79
1.3.7 Криптографічні протоколи автентифікації на основі симетричних криптографічних перетворень 81
1.3.8 Модель автентифікації 81
1.3.9 Однобічна автентифікації з одним проходом 83
1.3.10 Однобічна автентифікація з двома проходами 84
1.3.11 Взаємна автентифікація 85
1.3.12 Аналіз криптопротоколів встановлення ключів (узгодження ключів) 88
1.3.13 Протокол з нульовим проходом і кофакторним множенням 89
1.3.14 Аналіз інтерактивного механізму узгодження спільної таємниці типу Ель-Гамаля 92
1.3.15 Аналіз інтерактивного двопрохідного протоколу узгодження спільної таємниці типу Діффі-Геллмана 96
1.3.16 Аналіз механізму узгодження ключів типу Діффі-Геллмана з 2-х ключовими парами 100
1.4 Висновки до першого розділу 103
2 Формулювання концептуальних положень з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань 105
2.1 Міжнародна практика та рекомендації щодо впровадження систем моніторингу запобігання поширення інфекційних захворювань 107
2.2 Концептуальні принципі застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу 111
2.2.1 Принцип контролю 112
2.2.2 Правова основа для обробки 113

2.2.3 Принцип мінімізації даних 114
2.2.4 Принцип обмеження розкриття/доступу даних 117
2.2.5 Принцип забезпечення точних цілей обробки 119
2.2.6 Принцип встановлення жорстких обмежень на зберігання даних . 120
2.2.7 Принцип забезпечення даних 121
2.2.8 Принцип забезпечення точності даних 122
2.2.9 Принцип залучення органів із захисту даних 122
2.3 Формування концепцій розробки протоколів взаємодії та криптографічних перетворень для додатку на основі блокчейн технологій 122
2.3.1 Аналіз вразливостей децентралізованих рішень 125
2.3.2 Використання найкращіх практик та принципів під час розробки блокчейну 127
2.4 Підґрунтя створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини ... 130
2.5 Висновки до другого розділу 131
3 Збір, аналіз та систематизація статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи 133
3.1 Порівняння наборів даних датасетів та їхня обробка 133
3.1.1 Набори даних 134
3.1.2 Вимоги до наборів даних для оцінки СВВ 138
3.1.3 Порівняння існуючих наборів даних 140
3.2 Аналіз параметрів безпеки та якості обслуговування мережі 141
3.2.1 Кількісно-вимірні характеристики СВВ 142
3.2.2 Часові та якісні показники роботи мережі 146
3.3 Оцінка характеристик ефективності виявлення вторгнень 147
3.3.1 Класи методів інтерпретації даних 147
3.3.2 Методи виявлення відомих порушень 147
3.3.3 Виявлення аномалій 147
3.3.4 Методи представлення результату 148

3.4 Аналіз методів виявлення вторгнень 148
3.4.1 Метод аналізу аномалій..... 148
3.4.2 Метод заснований на аналізі статистичних даних 150
3.4.3 Методи машинного навчання 151
3.5 Дослідження методів аналізу протоколів з відстеженням стану 153
3.5.1 Аналіз мережних пакетів з урахуванням стану потоків. 153
3.5.2 Приклад аналізу протоколів з відстеженням стану. 155
3.5.3 Вибір оптимальної сукупності ознак оцінки інформаційної системи..... 160
3.6 Висновки до третього розділу..... 163
4 Дослідження розроблених методів та протоколів безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах. оцінка ефективності запропонованих рішень та проведення порівняльного аналізу з відомими протокольними аналогами..... 165
4.1 Аналіз місця порогових криптографічних схем в інфокомунікаційних мережах 165
4.2 Метод безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах з використанням шляхів, які не перетинаються 169
4.2.1 Математична модель розрахунку маршрутів, які не перетинаються, в інфокомунікаційних мережах..... 169
4.2.2 Математична модель безпечного балансування фрагментів конфіденційного повідомлення у інфокомунікаційній мережі..... 173
4.2.3 Результати дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються. 175
4.3 Метод безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах з використанням шляхів, які перетинаються 180

4.3.1 Математична модель розрахунку ймовірності компрометації конфіденційних повідомлень, які фрагментовано передаються за шляхами, які перетинаються 182
4.3.2 Результати дослідження ймовірності компрометації конфіденційних повідомлень, яке фрагментовано передається в ІКМ за шляхами, що перетинаються 192
4.3.3 Метод балансування фрагментів конфіденційного повідомлення за шляхами, які перетинаються 194
4.4 Висновки до четвертого розділу 197
5 Обґрунтування пропозицій з практичної реалізації запропонованих криптографічних примітивів та протоколів взаємодії для відомих застосувань і нових систем відстеження контактів, обробки та деперсоналізації даних .. 200
5.1 Поняття кільцевого підпису та огляд основних робіт 202
5.2 Загальна ідея побудови алгоритмів кільцевих підписів 206
5.2.1 Алгоритм формування підпису (у загальному вигляді) 207
5.2.2 Алгоритм перевіряння підпису (у загальному вигляді) 208
5.3 Кільцеві підписи, що використовують симетричні алгоритми шифрування 208
5.3.1 Алгоритм формування підпису 209
5.3.2 Алгоритм перевіряння підпису 210
5.4 Кільцеві підписи, що використовують криптографічну геш-функцію ... 210
5.4.1 Алгоритм формування підпису 210
5.4.2 Алгоритм перевіряння підпису 214
5.5 Кільцеві підписи, що використовують операцію спарювання на еліптичних кривих 215
5.5.1 Алгоритм формування підпису - 1 216
5.5.2 Алгоритм перевіряння підпису - 1 216
5.5.3 Алгоритм формування підпису - 2 218
5.5.4 Алгоритм перевіряння підпису - 2 218
5.6 Безпосередня анонімна атестація (БАА) 219

5.7 Використання наведених криптографічних механізмів для побудови відповідних протоколів моніторингу з максимальним забезпеченням анонімності 220
5.8 Висновки до п’ятого розділу 221
6 Обґрунтування пропозицій з практичної реалізації систем зберігання та поширення інформації у децентралізованих середовищах 223
6.1 Основні позначення, поняття та визначення 230
6.1.1 Числа Стірлінга другого роду 231
6.1.2 Факторизація ланцюгів Маркова 233
6.1.3 Модель колекціонера купонів з використанням добутків та факторизації 235
6.2 Розподілена генерація наборів доведень 238
6.2.1 Модель розподіленої генерації наборів доведень 238
6.2.2 Асимптотика τ^{mn} 242
6.3 Розподілена генерація дерев доведень 250
6.3.1 Впорядковані множини та решітки 250
6.3.2 Модель колекціонера купонів з частково впорядкованими множинами 253
6.3.3 Про досконалі бінарні дерева 255
6.3.4 Розподілена генерація частково впорядкованих множин 258
6.3.5 Деяка асимптотика для τ^{mN} 261
6.3.6 Практична реалізація процесу генерації дерев доведень 265
6.4 Висновки до шостого розділу 270
7 Обґрунтування пропозицій з практичної реалізації запропонованих рішень як основи перспективної системи моніторингу, виявлення вторгнень та ідентифікації мережних атак. розробка рекомендацій щодо впровадження результатів досліджень через імплементацію розробленої системи моніторингу, виявлення вторгнень та ідентифікації атак у діючі інформаційні системи та мережі 271

7.1 Результати моделювання роботи методу аналізу сигнатур заснованого на глибокому аналізі пакетів та рейтингуванні бази сигнатур 273
7.1.1 Опис СВВ на основі сигнатур Snort 273
7.1.2 Практичне використання запропонованого методу. 275
7.2 Розробка комплексного методу виявлення вторгнень, який базується на використанні аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів 281
7.3 Результати моделювання роботи комплексного методу виявлення вторгнень 284
7.4 Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак що базується на хмарному підході машинного навчання для умов низької продуктивності кінцевих пристроїв 288
7.5 Висновки до сьомого розділу 293
8 Обґрунтування науково-методичних рекомендацій щодо практичного впровадження розроблених моделей і методів як основи математичного та алгоритмічно-програмного забезпечення оновлених протоколів безпечної маршрутизації в сучасних та перспективних інфокомунікаційних мережах 295
8.1 Система загальних рекомендації щодо практичного використання запропонованих рішень в інфокомунікаційних мережах 295
8.2 Особливості практичного використання запропонованих рішень щодо безпечної маршрутизації у традиційних IP/MPLS-мережах 298
8.3 Особливості практичного впровадження запропонованих моделей та методів безпечної маршрутизації у програмно-конфігурованих мережах 301
8.4 Особливості практичної реалізації впровадження запропонованих моделей та методів безпечної маршрутизації у мережах MANET 303
8.5 Висновки до восьмого розділу 305
Висновки 307
Перелік джерел посилання 368

Додаток А Публікації авторського колективу за результатами виконання проєкту 384
А.1 Монографії (розділи монографій) за напрямом проєкту, виданих міжнародними видавництвами офіційними мовами Європейського Союзу та українською мовою 384
А.2 Статті у журналах, що індексуються в наукометричних базах даних WoS та/або Scopus. 392
А.3 Статті у наукових фахових журналах України, що відносяться до категорії «Б», статті у закордонних наукових виданнях, що не оцінені за попереднім пунктом, а також англомовні тези доповідей у матеріалах міжнародних конференцій, що індексуються науково-метричними базами даних WoS або Scopus..... 394
А.4 Патенти України або інших країн на винахід чи охоронних документів на промисловий зразок/корисну модель чи інші отримані охоронні документи на об’єкти права інтелектуальної власності..... 405
А.5 Підручники, навчальні посібники України. 406
А.6 Перелік поданих до публікації матеріалів 407
А.7 Захищені дисертації доктора філософії (кандидата наук) авторами проєкту або під керівництвом авторів проєкту 408
А.8 Захищені дисертації доктора наук авторами проєкту або під консультуванням авторів проєкту 409
Додаток Б Довідка про впровадження 411

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

БАА – Безпосередня Анонімна Атестація

БСШ – блоковий симетричний шифр

ЕП, ЕЦП – електронний підпис, електронний цифровий підпис

ІБ – інформаційна безпека

ІКМ – інфокомунікаційна мережа

ІТС – інформаційно-телекомунікаційна система

КЗІ – криптографічний захист інформації

КП – конфіденційне повідомлення

H-SPREAD – англ. Hybrid Secure Protocol for Reliable dAta Delivery – гібридний безпечний протокол для надійної доставки даних

НСД – несанкціонований доступ

ПСШ – потоковий симетричний шифр

СВВ – Система виявлення вторгнень

ТКМ – телекомунікаційна мережа

CRT – англ. Chinese Remainder Theorem – китайській теоремі про остачі

DAA – англ. Direct Anonymous Attestation – безпосередня анонімна атестація

DPI – англ. Deep Packet Inspection – глибокий аналіз пакетів

GRSP – англ. General Ring Signature Parameters – загальні параметри кільцевого підпису

ILP – англ. Integer Linear Programming – цілочисельне лінійне програмування

IoT – англ. Internet of Things – Інтернет речей

IP – англ. Internet Protocol – інтернет протокол

MaaS – англ. Model as a Service – Модель як послуга

MANET – англ. Mobile Ad hoc Network – мобільні самоорганізовані мережи

PR – англ. Precomputation Routing – маршрутизації з передрозрахунком

шляхів

QoS – англ. Quality of Service – якість обслуговування

RSA – криптографічний алгоритм з відкритим ключем (абревіатура від прізвищ Rivest, Shamir та Adleman) , що базується на обчислювальній складності задачі факторизації великих цілих чисел

SDN – англ. Software Defined Networks – програмно-конфігурована мережа

SPREAD – англ. Secure Protocol for Reliable dAta Delivery – безпечний протокол для надійної доставки даних

TCP – англ. Transmission Control Protocol – протокол управління передачею

USM – англ. Unified Security Management – система уніфікованого управління безпекою

UTM – англ. Unified Threat Management – система уніфікованого управління загрозами

zk-SNARK – англ. zero-knowledge Succinct Non-interactive Argument of Knowledge – стислий неінтерактивний аргумент знань з нульовим знанням

ВСТУП

Для забезпечення безпеки людини та суспільства в різних країнах створюються та постійно вдосконалюються національні системи запобігання кризовим та надзвичайним ситуаціям. Вони призначені для запобігання та реагування на негативні події техногенного та природного характеру, пов'язаних, зокрема, із боротьбою із злочинністю та моніторингом пенітенціарної системи, контролем за пожежною ситуацією та потенційнонебезпечними сховищами, охороною громадського порядку та проведення масових заходів, локалізацією і протидією терористичним загрозам та масовим заворушенням, порушеннями медико-санітарних вимог та поширенням особливо небезпечних інфекцій, і т.д. Однак останні події свідчать, що традиційні підходи щодо запобігання кризовим та надзвичайним ситуаціям не завжди ефективні. Поява нових форм і методів інформаційного впливу на різні за призначенням, ієрархічністю, формою власності та спрямованістю інформаційно-керуючі системи зумовлює підвищення вимог до їх надійності та безпеки. Особливу гостроту у цьому розумінні становлять питання інформаційної та кібербезпеки критично важливих інформаційних систем і технологій, в яких збій, відмова або вихід певних параметрів за встановлені межі може призвести до катастрофічних наслідків в енергетиці, на транспорті, в банківському секторі, у військовій сфері, екології, тощо.

Сучасні інформаційні технології можуть бути корисними для вирішення низки цих важливих питань. Зокрема, з появою нової загрози пандемії COVID19 провідними компаніями світу та окремими країнами вже розроблено та впроваджено в дослідну експлуатацію елементи системи глобального моніторингу кібернетичного простору. Наприклад, в рамках спільних зусиль для боротьби з пандемією COVID-19, корпораціями Apple Inc. та Google Inc. розроблено технологію відстеження контактів, щоб допомогти урядам та медичним установам зменшити розповсюдження вірусу. Однак слід виділити головне: кожна країна, уряд або корпорація в такий спосіб ставить за мету

застосувати кібернетичний простір для глобального моніторингу населення, шляхом спостереження та відслідковування контактів спрогнозувати можливі сценарії та запобігти поширенню інфекції. Звісно, що ці новації будуть розвинуті та застосовані і для інших потреб, зокрема, для виявлення небезпечних злочинних контактів, порушення митних правил та торгівлі, попередження та запобіганню терористичних актів, тощо.

Однак поява нових системних технологій завжди несе і додаткові загрози. Наприклад, авторитарний уряд може застосувати їх для нечесної політичної боротьби, корпорації – для промислового шпигунства та шахрайства, окремі особи для шантажу, вимагання, тощо. Дослідники вже аналізують технологічні інструменти глобального моніторингу, що запроваджені Apple Inc. та Google Inc., на відповідність вимогам захисту персональних даних, конфіденційності та анонімності, можливості несанкціонованого витоку приватних даних або зловмисного застосування цієї технології. Наприклад, отримавши доступ до технологічних інструментів моніторингу хакер зможе нав’язати хибну інформації щодо помилкових контактів та ізолювати конкурента силами правоохоронців. І це буде виглядати повністю законно та підтримуватиметься спільнотою.

Отже, при розробці, дослідженні, розгортанні та впровадженні систем глобального моніторингу кібернетичного простору необхідно враховувати низку складних та пов’язаних між собою нормативно-правових, моральноетичних, соціальних, технологічних та суто технічних обмежень та вимог як міжнародного так і національного рівнів. Аналіз цих вимог та загроз, їх дослідження, обґрунтування, розробка та впровадження ефективних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій є головними завданнями цього проекту.

Метою проєкту «Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій» є аналіз та

дослідження сучасних вимог та загроз національної безпеки в інформаційній сфері, обґрунтування, розробка та впровадження ефективних технологій захисту інформації для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Об’єктом дослідження є процеси забезпечення інформаційної та кібербезпеки, моделі, методи та механізми моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Предметом досліджень є технології інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Методи дослідження. При виконанні проєкту застосовувалися методи теорії захисту інформації, криптології, сучасних протоколів та технологій комп'ютерних мереж та систем, теорії систем та системного аналізу, комп’ютерного та імітаційного моделювання тощо. Зокрема, дослідження розподілених децентралізованих систем проводяться на основі сучасних методів побудови децентралізованих криптографічних протоколів з нульовим розголошенням (zero knowledge proofs), в тому числі неінтерактивних (ZK-SNARKs), кільцевих підписів тощо. При розробці загальної архітектури системи моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій застосовуються методи побудови розподілених децентралізованих систем, а також механізми економічного стимулювання, засновані на результатах новітніх досліджень у галузі криптоекономіки (cryptoeconomics) з використанням досвіду низки успішних сучасних криптовалют.

Проєкт виконувався у три етапи.

Етап 1 (за 2020 рік): дослідження сучасних моніторингових систем запобігання поширення інфекційних захворювань, механізмів та протоколів використання технологій Bluetooth, Wi-Fi, GPS та моделей взаємодії пристроїв, а також моделей, методів та технологій моніторингу, швидкого та раннього виявлення вторгнень та ідентифікації мережних атак різного типу, виявлення

фактів несанкціонованого доступу на основі використання сигнатур поведінки мережі та методів машинного навчання, обґрунтування критеріїв та показників ефективності, розробка методики оцінки та порівняльних досліджень технологій інформаційної безпеки для моніторингових систем запобігання поширенню інфекційних захворювань.

За результатами цього проміжного (за перший етап 2020 року) етапу викладено результати з аналізу, дослідження та обґрунтування моделей, методів та протоколів захисту персональних даних з урахуванням вимог децентралізованого середовища; застосування сучасних технологій у засобах відстеження контактів; моделей загроз, порушника та безпеки, деперсоналізації даних та побудови мережі; криптографічних примітивів та протоколів взаємодії; швидкого та раннього виявлення вторгнень та ідентифікації мережних атак, виявлення фактів несанкціонованого доступу; критеріїв та показників ефективності механізмів криптографічного захисту; методики оцінки та порівняльних досліджень криптографічних примітивів та протоколів взаємодії; забезпечення мережної безпеки засобами управління трафіком та маршрутизації, тощо.

Етап 1 (за 2021 рік): отримання нового науково обґрунтованого знання з аналізу безпеки моніторингових систем, що використовують однорангові мережі, а також моделей, методів та алгоритмів взаємодії, зберігання та обробки даних, стійких до його можливого застосування. Розробка та дослідження криптографічних примітивів та протоколів взаємодії для побудови безпечних моніторингових систем запобігання поширенню інфекційних захворювань, що функціонують в умовах децентралізованої взаємодії.

За результатами цього проміжного (за перший етап 2021 року) етапу викладено результати з отримання нового науково обґрунтованого знання з аналізу безпеки моніторингових систем, що використовують однорангові мережі, а також моделей, методів та алгоритмів взаємодії, зберігання та обробки даних, стійких до його можливого застосування; розробки та дослідження криптографічних примітивів та протоколів взаємодії для побудови безпечних

моніторингових систем запобігання поширенню інфекційних захворювань, що функціонують в умовах децентралізованої взаємодії.

За результатами виконання проміжного (за перший етап 2021 року) етапу отримано такі наукові та науково-технічні результати.

1. Комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних без наявності будь-якої довіреної сторони, які надають можливість виконувати задану обробку виключно у зашифрованому вигляді з гарантією конфіденційності інформації та доступністю відповідного фрагменту оригінальних та/або перетворених даних виключно учаснику, який є власником відповідного фрагменту даних і при цьому не має довіри до решти учасників.

2. Протоколи взаємодії для побудови системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань.

3. Результати з обґрунтування створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

4. Методи моніторингу та аналізу мультифрактальних та рекурентних характеристик мережного трафіка з формуванням та рейтингуванням бази сигнатур.

5. Методи виявлення вторгнень на підставі аналізу сигнатур та аномалій в поведінці (зміні стану) мережі. Для їх розробки залучаються засоби машинного навчання та методи фрактального аналізу. Реалізація запропонованих методів сприятиме підвищенню швидкості та точності виявлення вторгнень в широкому діапазоні атак на мережу.

За результатами виконання проміжного (за перший етап 2021 року) етапу Отримано такі наукові та науково-технічні результати.

1. Комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних без наявності будь-якої довіреної сторони, які надають

можливість виконувати задану обробку виключно у зашифрованому вигляді з гарантією конфіденційності інформації та доступністю відповідного фрагменту оригінальних та/або перетворених даних виключно учаснику, який є власником відповідного фрагменту даних і при цьому не має довіри до решти учасників.

2. Протоколи взаємодії для побудови системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров'я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань.

3. Результати з обґрунтування створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

4. Методи моніторингу та аналізу мультифрактальних та рекурентних характеристик мережного трафіка з формуванням та рейтингуванням бази сигнатур.

5. Методи виявлення вторгнень на підставі аналізу сигнатур та аномалій в поведінці (зміні стану) мережі. Для їх розробки залучаються засоби машинного навчання та методи фрактального аналізу. Реалізація запропонованих методів сприятиме підвищенню швидкості та точності виявлення вторгнень в широкому діапазоні атак на мережу.

Етап 2 (за 2021 рік, заключний): аналіз та дослідження децентралізованих технологій для побудови надійних та безпечних систем моніторингу запобігання поширення інфекційних захворювань. Розробка моделей, методів і протоколів моніторингової системи запобігання поширення інфекційних захворювань та безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

Метою цього заключного етапу дослідження є отримання нових науково обґрунтованих знань з моніторингових систем запобігання поширенню інфекційних захворювань. Запропонування механізму безпечного моніторингу контактів користувачів та надійного децентралізованого середовища для обміну

та зберігання необхідних для системи даних, а також забезпечення підвищення рівня мережної безпеки та якості обслуговування конфіденційних повідомлень на підставі впровадження розроблених методів і протоколів безпечної маршрутизації в інфокомунікаційних мережах.

Запланованими завданнями заключного етапу дослідження є наступні.

1. Аналіз та дослідження алгоритмів КЗІ та протоколів взаємодії в децентралізованому середовищі при побудові надійних та безпечних систем моніторингу запобігання поширенню інфекційних захворювань.

2. Формулювання концептуальних положень з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань.

3. Збір, аналіз та систематизація статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи.

4. Дослідження розроблених методів та протоколів безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах. Оцінка ефективності запропонованих рішень та проведення порівняльного аналізу з відомими протокольними аналогами.

5. Обґрунтування пропозицій з практичної реалізації запропонованих криптографічних примітивів та протоколів взаємодії для відомих застосувань і нових систем відстеження контактів, обробки деперсоналізації даних.

6. Обґрунтування пропозицій з практичної реалізації систем зберігання та поширення інформації у децентралізованих середовищах.

7. Обґрунтування пропозицій з практичної реалізації запропонованих рішень як основи перспективної системи моніторингу, виявлення вторгнень та ідентифікації мережних атак. Розробка рекомендацій щодо впровадження результатів досліджень через імплементацію розробленої системи моніторингу, виявлення вторгнень та ідентифікації атак у діючі інформаційні системи та мережі.

8. Обґрунтування науково-методичних рекомендацій щодо практичного впровадження розроблених моделей і методів як основи математичного та алгоритмічно-програмного забезпечення оновлених протоколів безпечної маршрутизації в сучасних та перспективних інфокомунікаційних мережах.

Індикатори виконання заключного етапу проєкту.

1. Результати дослідження алгоритмів криптографічного захисту інформації та протоколів взаємодії в децентралізованому середовищі при побудові надійних та безпечних систем моніторингу запобігання поширення інфекційних захворювань.

2. Концептуальні положення з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у системах моніторингу запобігання поширення інфекційних захворювань.

3. Науково-методичні рекомендації щодо практичного впровадження розроблених моделей, методів і протоколів безпечної маршрутизації конфіденційних повідомлень в сучасних та перспективних інфокомунікаційних мережах.

4. Обґрунтовані пропозиції з практичної реалізації запропонованих криптографічних примітивів та протоколів взаємодії для відомих застосувань і нових систем відстеження контактів, обробки деперсоналізації даних.

5. Обґрунтовані пропозиції з практичної реалізації систем зберігання та поширення інформації у децентралізованих середовищах.

6. Розробка рекомендацій щодо створення інфраструктури системи моніторингу, раннього виявлення вторгнень та ідентифікації атак різного типу, виявлення фактів несанкціонованого доступу та несанкціонованих користувачів.

7. Опис підходу щодо побудови прототипів протоколів безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

8. Інформаційний науковий звіт про проміжні результати реалізації проєкту (за шостий етап);

9. Серія наукових публікацій (із залученням молодих вчених) за результатами проведених досліджень в фахових наукових та міжнародних індексованих виданнях;

10. Виступи (із залученням молодих вчених) на міжнародних наукових конференціях та семінарах (в тому числі англійською) з публікацією доповідей (в тому числі у індексованих виданнях);

11. Наукові, навчальні та методичні матеріали для впровадження отриманих результатів до начального процесу.

12. Захист дисертаційних робіт на основі отриманих наукових результатів дослідження.

В цьому заключному звіті викладаються результати з нових науково обґрунтованих знань з моніторингових систем запобігання поширенню інфекційних захворювань; механізмів безпечного моніторингу контактів користувачів та надійного децентралізованого середовища для обміну та зберігання необхідних для системи даних, а також забезпечення підвищення рівня мережної безпеки та якості обслуговування конфіденційних повідомлень на підставі впровадження розроблених методів і протоколів безпечної маршрутизації в інфокомунікаційних мережах.

У заключному етапі отримано наступні наукові та науково-технічні результати.

1. Запропоновано та досліджено два методи безпечної маршрутизації, які можуть бути використані при фрагментованій передачі конфіденційних повідомлень в інфокомунікаційній мережі (ІКМ). Перший метод заснований на розрахунку та використанні шляхів, які не перетинаються, та є подальшим узагальненням механізму безпечної маршрутизації SPREAD. В основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв’язання двох оптимізаційних задач:

– розрахунку маршрутів, що не перетинаються, в інфокомунікаційній мережі;

– безпечного балансування фрагментів конфіденційного повідомлення за множиною попередньо розрахованих шляхів.

2. Модель розрахунку маршрутів, що не перетинаються, обрана для використання з причини її корисних властивостей щодо розрахунку максимальної кількості шляхів із включенням у них каналів зв’язку з мінімальною ймовірністю компрометації. Модель безпечного балансування фрагментів конфіденційного повідомлення використана з метою забезпечення мінімально можливої ймовірності компрометації повідомлень, які передавались за попередньо розрахованою множиною шляхів, що не перетинались.

3. Запропоновано метод безпечної маршрутизації конфіденційних повідомлень, заснований на використанні шляхів, які можуть перетинатись. Це дозволяє більш повно використати наявний в мережі ресурс щодо пропускної здатності та кіберресурс. В межах даного методу ймовірність компрометації повідомлень розраховується за формулою повної ймовірності з врахуванням рівня мережної безпеки «містків» у структурі ІКМ. Метод не вимагає попереднього розрахунку множини шляхів, які не перетинаються, що спрощує його реалізацію на практиці.

4. В межах запропонованих методів рівень мережної безпеки маршрутів, мережі та конфіденційних повідомлень взагалі оцінювався через ймовірність компрометації каналів зв’язку. За необхідності врахування рівня мережної безпеки вузлів (маршрутизаторів) ІКМ вони можуть бути логічно представлені віртуальними каналами зв’язку, які мають вузлову ймовірність компрометації, без зміни змісту запропонованих методів безпечної маршрутизації конфіденційних повідомлень.

5. Механізми економічного стимулювання функціонування системи моніторингу й протоколи активної взаємодії як звичайних громадян (що отримують інформацію у системі й розповсюджують її у визначених безпечних рамках), так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури.

6. Розроблено рекомендації щодо практичної реалізації результатів проєкту, які стосуються впровадження запропонованих моделей та методів безпечної маршрутизації в ІКМ. Рекомендації базуються на результатах дослідження запропонованих рішень. Виконання рекомендацій передбачає проведення комплексу організаційно-технічних заходів, спрямованих на забезпечення ефективного функціонування ІКМ на основі запропонованих принципів структурно-топологічної, технологічної та алгоритмічно-програмної реалізації.

7. Запропоновані математичні моделі та обчислювальні методи безпечної маршрутизації можуть знайти своє практичне застосування в сучасних та перспективних інфокомунікаційних мережах (ІКМ). В традиційних IP/MPLS-мережах запропоновані моделі та методи мають стати основою математичного та алгоритмічно-програмного забезпечення маршрутизаторів та використовуватись при розрахунку та формуванні маршрутних таблиць. В залежності від топології мережі, її завантаженості та вимог щодо рівня якості обслуговування та мережної безпеки запропоновані рішення можуть базуватись на використанні маршрутних метрик, концепції Traffic Engineering. Для підвищення рівня кіберстійкості ІКМ в межах реалізації реактивного підходу запропоновані моделі та методи можуть бути використані для швидкої безпечної перемаршрутизації із реалізацією схем захисту вузла, каналу або маршруту.

8. При реалізації запропонованих рішень в програмно-конфігурованих мережах розроблені моделі та методи безпечної маршрутизації можуть стати основою алгоритмічно-програмного забезпечення SDN-контролерів, які здійснюють управління інформаційним обміном в межах певного мережного сегмента або домену.

9. При реалізації запропонованих у межах проєкту моделей та методів безпечної маршрутизації в безпроводових мережах, які самоорганізуються (MANET), рішення можуть стати основою алгоритмічно-програмного забезпечення мережних вузлів, які в залежності від стану мережі виконуються функції термінального пристрою, точки доступу, маршрутизатора та/або сервера

послуг. Запропоновані рішення в MANET можуть використовуватись як для безпечної маршрутизації трафіка користувачі, так і для передачі конфіденційних даних і секретів.

Заключний звіт складено з 8 розділів.

У першому розділу розглядається декілька напрямків реалізації криптографічних механізмів, асиметричні та симетричні криптоалгоритми: базові основи їх функціонування, переваги та недоліки, а також конкретні приклади реалізації, що можуть бути застосовані у реальних системах моніторингу запобігання поширення інфекційних захворювань. Також проаналізуємо криптографічні протоколи взаємодії, які є необхідними для застосування, синтезуємо конкретні алгоритми їх реалізації, які є перспективними та ефективними для імплементації на практиці.

У другому розділу сформовано концептуальні положення з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань.

У третьому розділу розглядаються системи виявлення вторгнень для виявлення та ідентифікації спроб вторгнення в систему або мережу. Використовуючи набір апаратних і програмних ресурсів, системи виявлення вторгнень намагається виявити вторгнення, відстежуючи дані, зібрані з одного хоста або мережі, і генерувати тривогу в разі виявлення спроб вторгнення.

Було обрано набір ознак для розробки методів моніторингу та виявлення вторгнень. Наведено забезпечення своєчасного і економічно ефективного механізму поновлення існуючих систем виявлення вторгнень згідно з новими шаблонами даних, який зазначено як критичну вимогу під час розробки систем виявлення вторгнень.

У четвертому розділі запропоновано та досліджено два методи безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційній мережі (ІКМ). Перший метод заснований на розрахунку та використанні шляхів, які не перетинаються, та є подальшим узагальненням механізму безпечної

маршрутизації SPREAD. Запропонована оптимізаційна модель розрахунку шляхів, які не перетинаються, з врахуванням їх рівня мережної безпеки дозволила знизити ймовірність компрометації конфіденційних повідомлень в залежності від сценарію компрометації елементів мережі від 23-27% до 47-56%.

Другий метод безпечної маршрутизації конфіденційних повідомлень заснований на використанні шляхів, які можуть перетинатись. В межах даного методу ймовірність компрометації повідомлень розраховується за формулою повної ймовірності з врахуванням рівня мережної безпеки «містків» у структурі ІКМ. Як показали результати дослідження запропонованого методу, найбільший виграш щодо значень ймовірність компрометації повідомлень (у середньому від 20-60%) вдалося отримати в умовах відносно невисокого рівня кіберзагроз у ІКМ, тобто коли ймовірність компрометації каналів (вузлів) зв’язку не перевищувала 0,4. При збільшенні рівня загроз, коли ймовірність компрометації каналів (вузлів) зв’язку збільшувалась до 0,7, виграш щодо значень ймовірність компрометації повідомлень складав у середньому від 3-20%.

У п’ятому розділу наведені протоколи взаємодії для системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань.

Докладно розглянуто механізми кільцевого підпису та безпосередньої анонімної атестації. Сформульовано, як саме можна використовувати вказані механізми для побудови відповідних протоколів. Наведено новий алгоритм кільцевого підпису, який має наступні переваги: суттєво менша довжина підпису та час роботи алгоритму, у порівнянні з тими алгоритмами, що використовують функцію типу RSA; суттєво вища стійкість, у порівнянні з тими алгоритмами, що використовують функцію типу RSA; вдвічі менша довжина ключа та у стільки ж менший обсяг обчислень у порівнянні з іншими алгоритмами, що використовують операцію спарювання.

Показано, як наведені криптографічні механізми дозволяють підтверджувати валідність інформації стосовно певної особи, зберігаючи при цьому її анонімність та, за необхідності, не розкриваючи деталі цієї інформації.

У шостому розділу наведені механізми економічного стимулювання підключення до системи моніторингу й протоколи активної взаємодії як звичайних громадян (що отримують інформацію у системі й розповсюджують її у визначених безпечних рамках), так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури. Запропоновані протоколи взаємодії забезпечуватиме максимальну децентралізацію системи, а механізм економічного стимулювання має виключно добровільний характер з відсутністю будь-якої каральної складової. Кінцевою метою таких механізмів є охоплення системою переважної більшості суспільства із загальним позитивним сприянням.

У сьомому розділі розглянуто система виявлення вторгнень (СВВ) на основі сигнатур намагаються ідентифікувати шкідливі дії в системі, порівнюючи спостерігаючу поведінку з відомими моделями атак. У системах такого типу база даних використовується для зберігання поведінки раніше відомих атак, які закодовані як сигнатури. Отже, ці системи здатні виявляти атаки, знаходячи схожі сигнатури в базі даних.

Завдяки застосуванню хмарного рішення вдалось розв’язати завдання моніторингу, виявлення вторгнень та ідентифікації мережних атак для кінцевих пристроїв системи з обмеженими ресурсами. Запропоновано та проведено порівняльний аналіз комплексного методу виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Запропонований метод дозволяє підвищити як достовірність, так і точність виявлення вторгнень, та уможливлює раннє виявлення вторгнень в широкому діапазоні кібератак на систему.

У восьмому розділі розроблено рекомендації щодо практичної реалізації результатів проєкту, які стосуються впровадження запропонованих моделей та

методів безпечної маршрутизації в ІКМ. Рекомендації базуються на результатах дослідження запропонованих рішень. Виконання рекомендацій передбачає проведення комплексу організаційно-технічних заходів, спрямованих на забезпечення ефективного функціонування ІКМ на основі запропонованих принципів структурно-топологічної, технологічної та алгоритмічно-програмної реалізації.

Запропоновані математичні моделі та обчислювальні методи безпечної маршрутизації можуть знайти своє практичне застосування в IP/MPLS-мережах, програмно-конфігурованих мережах та в безпроводових мережах, які самоорганізуються (MANET), як основа математичного та алгоритмічно-програмного забезпечення маршрутизаторів та SDN-конролерів мереж при розрахунку та формуванні маршрутних таблиць. Для підвищення рівня кіберстійкості ІКМ в межах реалізації реактивного підходу запропоновані моделі та методи можуть бути використані для швидкої безпечної перемаршрутизації із реалізацією схем захисту вузла, каналу або маршруту.

1 АНАЛІЗ ТА ДОСЛІДЖЕННЯ АЛГОРИТМІВ КЗІ ТА ПРОТОКОЛІВ ВЗАЄМОДІЇ В ДЕЦЕНТРАЛІЗОВАНОМУ СЕРЕДОВИЩІ ПРИ ПОБУДОВІ НАДІЙНИХ ТА БЕЗПЕЧНИХ СИСТЕМ МОНІТОРИНГУ ЗАПОБІГАННЯ ПОШИРЕННЮ ІНФЕКЦІЙНИХ ЗАХВОРЮВАНЬ

Всесвітня організація охорони здоров’я офіційно проголосила коронавірусну хворобу пандемією на початку березня 2020 року. За цей час пандемія суттєво вплинула на тренди розвитку світової економіки, не залишивши осторонь жодної країни. Перш за все, це пов’язано із жорсткими карантинними заходами, які ввели уряди багатьох країн: закриття торгово-розважальних центрів, заборона відвідання усіх масових заходів, обмеження у пересуванні як у межах країни, так і при перетині її кордонів, скорочення виробництва (через встановлення лімітів одночасного перебування працівників в одному приміщенні) тощо. Окремі компанії перевели своїх працівників на режим роботи «на дому», інші ж змушені відправляти своїх працівників у відпустку. Все це негативно позначається на добробуті населення, їх фінансовому становищі і у недалекому майбутньому призведе до скорочення їх попиту на ряд товарів і послу. Під загрозою опинилися світові виробничі ланцюжки – від електроніки й авто до курятини. Провідні авіакомпанії світу тимчасово скасували рейси [1].

Аналітики прогнозують, що збитки світової економіки через пандемію коронавірусу за найгіршого сценарію можуть досягнути межі у $ 2,7 трлн. Однак точно розрахувати очікувані втрати неможливо. Голова Європейського центрального банку Крістін Лагард[1] заявила, що Європа може зіткнутися з серйозним економічним шоком, який перегукується із світовою фінансовою кризою 2008 р., якщо світові лідери не вживатимуть термінових заходів проти спалаху коронавірусу.

[1] Коронавірус може призвести до масштабного економічного шоку в Європі – Лагард. URL: https://suspilne. media/18912-koronavirus-moze-prizvesti-do-masstabnogoekonomicnogo-soku-v-evropi-lagard/

Одним із шляхів виходу з кризи та відновлення звичайного способі життя людей є контроль за розповсюдженням захворювання. Для цього є необхідним впровадження систем моніторингу контактів, що дозволить попередити потенційних хворих про небезпеку та зменшить поширення інфекції серед населення.

Для ефективної реалізації систем моніторингу контактів необхідним є застосування криптографічних протоколів та механізмів, що забезпечують кінцевих користувачів впевненістю в секретності їх даних, а також попереджують атаки зловмисників, що направлені на фіктивне оповіщення населення.

У рамках даного розділу ми розглянемо декілька напрямків реалізації криптографічних механізмів, асиметричні та симетричні криптоалгоритми: базові основи їх функціонування, переваги та недоліки, а також конкретні приклади реалізації, що можуть бути застосовані у реальних системах моніторингу запобігання поширення інфекційних захворювань. Також проаналізуємо криптографічні протоколи взаємодії, які є необхідними для застосування, синтезуємо конкретні алгоритми їх реалізації, які є перспективними та ефективними для імплементації на практиці.

1.1 Аналіз можливостей застосування симетричної криптографії у системах моніторингу запобігання поширення інфекційних захворювань

Спочатку розглянемо докладніше поняття «симетрична криптосистема». Криптографічну систему називають симетричною, якщо ключ прямого перетворення $K_{пр.пер.}$ збігається з ключем $K_{зв.пер.}$ зворотного перетворення чи обчислюється один з іншого не вище чим з поліноміальною складністю. Для випадків автентифікації ознаку симетричності ключа будемо записувати як

$$K_j^a = K_j^{a*}$$

а для шифрування

$$K_j^з = K_j^p$$

Криптографічну систему називають асиметричною, якщо ключ прямого перетворення $K_{пр.пер.}$ не збігається з ключем $K_{зв.пер.}$ зворотного перетворення або може бути обчислений один при знанні іншого не нижче ніж з субекспоненційною складністю. Обчислюється один з іншого не вище чим з поліноміальною складністю [2]. Для випадків автентифікації ознаку асиметричності ключа будемо записувати як

$$K_j^a \neq K_j^{a*}$$

а для шифрування

$$K_j^з \neq K_j^p$$

Симетричні крипто перетворення діляться на блокові шифри, потокові шифри та функції хешування (геш – функції) (Рис. 1.1).

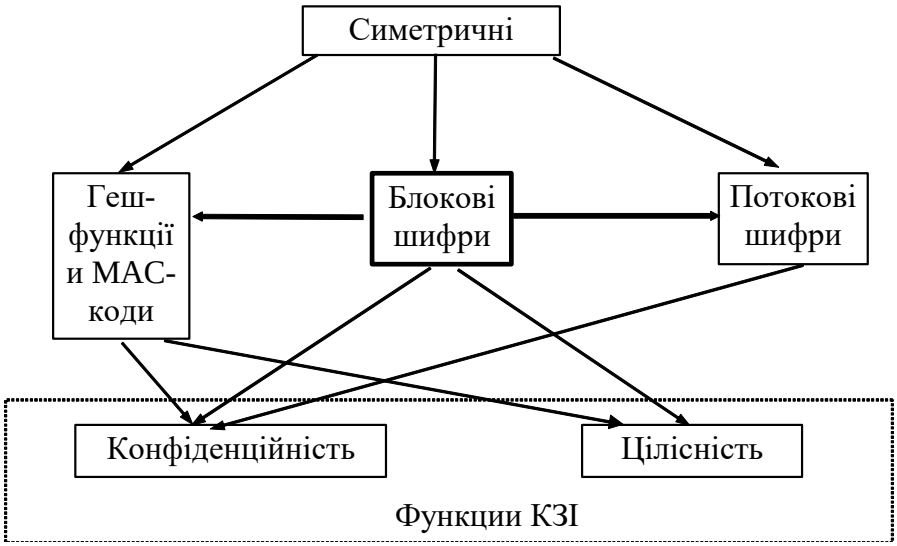


Рисунок 1.1 – Класифікація та призначення симетричних крипто перетворень

В цілому необхідно відмітити, що побудування шифрів та функцій гешування, пов’язане з використанням елементарних табличних та /або криптографічних перетворень. Табличним є перетворення, яке здійснюється без використання ключа (ключів), тобто з урахуванням криптографічних перетворень та його можна подати як

$$F_a\left(M_i, \Pr\right) = M_i^з$$

або $F_{зш}\left(M_i^a, \Pr\right) = C_i$

До елементарних криптографічних перетворень (шифрів) відносяться:

– гамування, тобто складання символів інформації M_i (повідомлення) з ключем К $_i$ чи гамою шифрування $Г_i$ за відповідним модулем m ;

– перетворення типу підстановка символів повідомлення M_i згідно ключа $K_i\left(Г_i\right)$;

– перетворення типу перестановка символів повідомлення M_i згідно ключа $K_i\left(Г_i\right)$;

– зсув бітів, символів, слів згідно ключа $K_i\left(Г_i\right)$ тощо;

– афінні перетворення бітів, символів, слів згідно ключа $K_i\left(Г_i\right)$ тощо;

– аналітичні перетворення згідно правил, формул, залежностей згідно ключа $K_i\left(Г_i\right)$ тощо;

– До елементарних табличних перетворень відносяться:

– перетворення типу підстановка символів повідомлення M_i згідно даних;

– перетворення типу перестановка символів повідомлення M_i згідно даних;

– зсув бітів, символів, слів згідно даних;

– афінні перетворення бітів, символів, слів згідно даних;

– аналітичні перетворення згідно правил, формул, залежностей згідно даних

– зв’язування символів строчок, стовбців згідно правил, формул, залежностей [3].

1.1.1 Характеристика основних елементарних криптоперетворень симетричного типу

Криптографічні перетворення (шифри) типу перестановка

Розглянемо відкрите повідомлення $M = (M_0, M_1, \ldots, M_{l-1})$ довжини l з алфавітом Z_m. Застосуємо до повідомлення перестановку χ, причому $\chi = \{\chi(0), \chi(1), \ldots, \chi(l-1\})$, в результаті отримаємо криптограму $\{C\,\chi(0), C\,\chi(1), \ldots, C\,\chi(l-1)\}$. Сімейство таких криптографічних перетворень називають шифром перестановки.

В такій трактовці перестановка є у пере упорядкуванні символів відкритого тексту, що робиться з метою придання криптограмі певного рівня конфіденційності засобом застосування ключа χ .

Розшифрування криптограми $C\,\chi(0), C\,\chi(1), \ldots, C\,\chi(l-1)$ здійснюється засобом застосування до неї однозначно зворотної перестановки χ^{-1} .

Як правило ключ χ використовують певної довжини v, але меншої довжини повідомлення l. За таких умов відкритий текст розбивають на $l\ /\ v$ відрізків довжини v , до кожного з яких в подальшому застосовують перестановку згідно ключа χ [3].

Такий елементарний шифр перестановки має такі властивості:

– Відносні частоти появи символів в відкритому повідомленні і криптограмі співпадають, оскільки вони інваріантні до перестановки символів тексту.

– Існують обмеження на довжину ключа v, що використовують.

– При уже незначних довжинах повідомлення, що зашифровують, необхідно ключ застосовувати багато разів, що спрощує крипто аналіз таких криптограм.

Тому, як свідчить практика, шифр перестановки застосовують як елементарний, разом х іншими шифрами, наприклад підстановки (заміни).

Основним показником криптографічної стійкості шифру перестановки є число різних ключів, що можуть бути використаними при шифруванні. Так якщо довжина ключа ν ,то загальне число різних ключів перестановки можна визначити [2]

$$N_к = v!$$

Аналіз показує, що при значення v порядку 32 та більше забезпечується формування великого простору ключів $N_к$, але як уже вказувалось вище окремо застосований шифр перестановки не забезпечує криптографічної стійкості.

Криптографічні перетворення (шифри) типу підстановки (заміни)

Розглянемо знову відкрите повідомлення $M = (M_0, M_1, \ldots, M_{l-1})$ довжини l з алфавітом $Z^s{}_m$.

Нехай існує система Φ відображення множини (заміни) $Z^s{}_m$ в алфавіт Y шифротексту C , де s – характеристика перетворення заміни, причому

$$\Phi = \{\varphi_0, \varphi_1, \ldots, \varphi_{l-1}\},$$

Значить криптограма С обчислюється по відкритому повідомленню $M = (M_0, M_1, \ldots, M_{l-1})$ з використанням відображення згідно ключа Φ , причому Φ виконує функції ключа. За даних умов

$$C = (\varphi_0(M_0), \varphi_1(M_1), \ldots, \varphi_{l-1}(M_{l-1})$$

Тепер, якщо φ_i є бієктивним (однозначним) відображенням, то систему відображення Φ називають шифром підстановки(заміни).

В подальшому покладемо, без втрати загальності, що алфавіти криптограм та вхідних символів співпадають, тобто що

$$Z^s{}_m = Y ,$$

а $\varphi_0, \varphi_1, \ldots, \varphi_{l-1}$ = підстановки на множині $Z^s{}_m$.

Далі, якщо прийняти, що $\varphi = \varphi_i$ для усіх $i = 0, 1, \ldots, l-1$, то такий шифр є шифром простої заміни (монопідстановки) на множині $Z^s{}_m$. В такому шифрі заміна виконується по окремим знакам алфавіту. Якщо $\varphi_0, \varphi_1, \ldots, \varphi_{l-1}$ є різними, то шифр називають шифром з багато алфавітної заміни (с).

Історично шифри підстановки у свій час знаходили застосування. Серед них потрібно назвати шифри Цезаря, Віжінера, латинського квадрату, пропорційної заміни, заміни біграм та s грам.

За виконання умови шифр простої заміни можна розглядати як відображенням алфавіту вхідного повідомлення самого в себе. Для такого шифру при основі вхідного алфавіту m, число ключів, тобто різних замін, визначається як

$$N_k = m!$$

Взагалі шифри простої заміни, навіть починаючи з англійського алфавіту ($m = 27$), мають великий простір ключів. Але якщо використовується алфавіт натуральної мови, символи якої залежні та нерівно ймовірні, то існують афективні методи крипто аналізу, які отримали назву частотного аналізу.

В суттєвій мірі від такого недоліку вільний шифр полі підстановки. В такому шифрі один вхід і k виходів. Тому для шифру полі підстановки число можливих ключів, з урахуванням визначається як

$$N_к = (m!)^k,$$

де k – кількість виходів.

На відміну від шифрів простої заміни, шифри полі підстановки мають багату історію застосування, наприклад у вигляді шифрів колонної заміни. При числі виходів $k = 12$ та більше отримувані з його використанням шифри мають високій рівень криптографічної стійкості.

На практиці при побудові блочних та поточних шифрів широке застосування знайшли шифри підстановки типу « чотири біти в чотири біти», « байт в байт», рідше «слово в слово», коли має довжину 16 і більше бітів тощо. Для таких шифрів важливою задачею є побудова таблиць підстановки, які забезпечили б необхідний рівень стійкості. Тому розглянемо декілька прикладів таблиць підстановки [4].

Аналітична підстановки в полі Галуа

Аналітична підстановка в полі Галуа[2] $F\left(2^8\right)$ ґрунтується на заміні кожного елемента поля $F\left(2^8\right)$на мультиплікативно зворотний. Наприклад, якщо a_i вхідний байт, а a' вихідний, тобто результат підстановки, то для знаходження a' можна вирішить порівняння

$$a_i \cdot a_i' = 1\left(\bmod x^8 + x^4 + x^3 + x + 1\right)$$

Для побудови таблиці підстановки «байт в байт» в полі Галуа $F\left(2^8\right)$подамо вхідні символи, тобто числі від 1 до 255 у вигляді поліномів над вказаним полем Галуа. Для повідомлення M_i це будуть поліноми на вище 8 – го степеню a_1, a_2, a_3 ,…, a_{255} та нульовий байт a_0. Знайти потрібно a_0^{-1}, a_1^{-1}, a_2^{-1},…, a_{255}^{-1} . Оскільки для нульового поліномаa_0 в полі Галуа $F\left(2^8\right)$мультиплікативно зворотнього не існує, то будемо його заміняти самим собою [25].

Далі, розв’язок порівняння зведемо до розв’язку діафантового рівняння:

$$ax + by = 1.$$

Таким чином маємо порівняння

$$a_i \cdot a_i^{-1} = k\left(x^8 + x^4 + x^3 + x + 1\right) + 1 \quad ,$$

яке зведемо до порівняння

$$\left(x^8 + x^4 + x^3 + x + 1\right)\left(-k\left(x\right)\right) + a_i \cdot a_i^{-1} = 1$$

Однозначне рішення цього порівняння існує у вигляді

$$\begin{cases} y = \left(-1\right)^{\mu} a_{\mu-1} \\ x = \left(-1\right)^{\mu+1} b_{\mu-1} \end{cases}.$$

Як правило, таке перетворення використовується як табличне. Так в блочному симетричному шифрі Rijndael та його звуженій версії – стандарті США FIPS 1987 для побудови таблиці підстановки «байт в байт», в тому числі, використовується таке порівняння.

Криптографічні перетворення (шифри) типу зсув символів

[2] Лідл Р., Нідеррайтер Г. . Кінцеві поля. В 2-х тт. — М.: Мир, 1988. — 430 с.

Перетворення типу «зсув вхідних символів» може бути як криптографічним, коли конкретне значення зсуву визначається ключем, так і табличним, коли значення зсуву в шифрі є постійним. Зсув може здійснюватись циклічно в тетрадах, байтах, 16, 32, 64, 128, та 256 бітних словах. Окремо перетворення типу зсув не забезпечує криптграфічної стійкості, але коли воно застосовується разом з іншими криптографічними чи табличними перетвореннями, то при певних умовах може забезпечуватись якісне шифрування.

Важливим для шифру типу зсув є визначення вимог до ключа при криптографічному перетворення та визначення величини зсуву при табличному. У випадку використання ключа величина значення зсуву повинна бути випадковою величиною з рівноймовірним розподілом величини зсуву. При табличному заданні величини зсуву, як слідує із практики, величина зсуву повинна бути числом, взаємо простим є довжиною слова, відносно якого виконується перетворення типу зсуву.

В цілому, якщо довжина слова, що перетворюється, має значення L_c , то величина ключа може визначатись як [4]

$$l_k = Lg_2(L_c)$$

Зрозуміло що для доброго узгодження довжина слова, яке підлягає зсуву, повинна бути кратною 2.

На практиці в блочних та потокових симетричних шифрах перетворення типу керуємий зсув, знаходять застосування. При цьому табличне перетворення застосовується у більшості блокових шифрів.

На рис. 1.2 показано перетворення зсув байтів ShiftRows для стандарту США FIPS 197[3]. В цьому стандарті використовується, за нашою термінологією, табличне перетворення тину циклічний зсув вліво байтів 32 бітних слів 128 (192, 256) бітних блоків. Причому, перше 32 бітне слово 128 бітного блоку залишається без змін, друге слово зсувається циклічно на 1 байт вліво, третє

[3] Advanced Encryption Standard (AES) [Electronic resource]: FIPS PUB 197. - 2001 - Mode of access: www. URL: http://csrc.nist.gov/ publica-tions / fips / fips197 / fips-197.pdf.

слово зсувається циклічно на 2 байти вліво, четверте слово зсувається циклічно на 3 байти вліво [5].

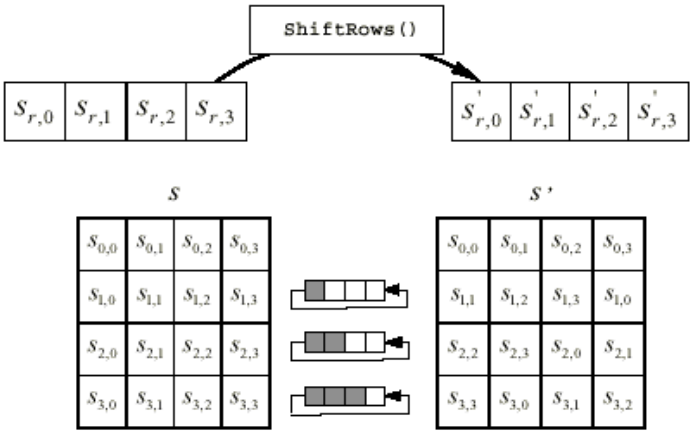


Рисунок 1.2 – Перетворення ShiftRows циклічного зсуву останніх трьох рядків в масиву State

1.1.2 Блочні симетричні шифри, що можуть бути застосовані у системах моніторингу, та їх властивості.

Симетричне криптографічне перетворення у вигляді блокового симетричного шифру (БСШ) знайшло широке застосування на практиці. БСШ будуються на основі використання декількох симетричних криптографічних перетворень (елементарних шифрів). Хоча кожен з таких елементарних шифрів є нестійким, застосування декількох з них послідовно чи паралельно, та багатократно, дозволяє отримати звіря з «товстою шкірою». Вказане визначило появу, широке застосування та розвиток БСШ.

В цьому розділі ми робимо спробу розглянути сутність, проблемні питання, в межах обмежень обсягом викладення результатів досліджень, застосування та можливі напрями розвитку БСШ.

Необхідно відмітити, що при побудові БСШ знайшли застосування декілька концептуальних підходів, які будемо називати методологічними принципами. Серед них необхідно виділити, на наш погляд, три основні:

– на основі ланцюгів Фейстеля (Data Encryption Standard[4], ГОСТ 28147 – 89 тощо);

– IDEA подібні шифри(Європейський стандарт IDEA та його модифікації і удосконалення);

– SPN структури(перше за все Rijndael[5], FIPS – 197 тощо).

Ми вважаємо, що сьогодні системне викладення теорії та практики блочного симетричного шифрування вимагає написання багатотомної роботи. Тому нижче викладення теоретичних та практичних питань є обмеженим. Крім того , в цьому розділі, ми практично не розглядаємо питання крипто аналізу, так як вони системно викладаються в 8 розділі цієї роботи.

1.1.3 Поточні шифри для застосування у реальних моніторингових системах

БСШ знайшли широке застосування на практиці для вирішення задач забезпечення конфіденційності, цілісності, доступності, захисту від НСД тощо. Разом з тим, БСШ мають ряд недоліків, серед яких необхідно відмітити:

– достатньо велика складність перетворень при шифруванні, треба виконувати багато (10–32) і більше ідентичних циклів;

– недостатня швидкодія прямих і зворотних криптоперетворень, можна говорити, що забезпечується середня швидкодія. Так, при прикладенні суттєвих зусиль досягти швидкодії порядку одного Гбітів/сек практично неможливо;

– складність, а в ряді випадків і неможливість розпараллелювання процесів криптоперетворень;

– всі блоки зашифровуються з використанням одного і того самого ключа тощо.

---

[4] Data Encryption Standard (DES) [Electronic resource]: FIPS 46-3 / National Bureau of Stand-ards, USA. - 1993. - Mode of access: www. URL: http://csrc.nist.gov/publications/fips/fips46-3/fips 46-3.pdf.

[5] Daemen J. AES proposal: Rijndael [Text] / J. Daemen, V. Rijmen // First Advanced Encryption Standard (A ES) Conference, Ventura, CA, August 20-22, 1998.

У той же час, у ряді застосувань необхідно забезпечувати швидкодії в десятки та й сотні Гбітів/сек [6].

Вирішення цього протиріччя покладається на потокові симетричні перетворення – потокові симетричні шифри (ПСШ). Необхідно відмітити, що зважаючи на вказані переваги ПСШ, на міжнародному рівні проведено та виконано ряд науково-практичних результативних проектів – Nessie[6], eSTREAM. Так, за результатами виконання міжнародного проекту eSTREAM[7] створено:

– програмні шифри – HC 128, Rabbit, Salsa20/12, Sosemanuk;
– апаратні шифри – F-FCSR-H v2, Grain v1, MISKEYv2, Trivium.

Надалі наведено основні положення, вимоги та приклади реалізації ПСШ, перш за все таких, що здобули визнання на міжнародних рівнях.

Особливістю ПСШ є те, що в них, як і БСШ, використовується тільки таємні (секретні) ключі. Розголошення ключів призводить до повної компрометації системи. Ключі мають бути надзвичайно захищені.

1.1.4 Спрощена схема застосування та математична модель ПСШ

Розглянемо особливості організації захищеного зв’язку з використанням ПСШ. На рис.1.3 наведена структурна схема каналу захищеного інформаційного обміну користувачів A та B, які застосовують ПСШ. Нехай M_i – мова деякого алфавіту m джерела інформації A. Символи повідомлення m алфавіту M_i послідовно подаються на вхід шифратора. З ключового засобу попередньо або за необхідністю у шифратор зчитується початковий ключ K_n. Якщо шифрування здійснюється з безумовною стійкістю, то довжина такого ключа має бути не менше довжини повідомлення, що належить зашифруванню. Якщо потрібно забезпечити гарантовану (обчислювальну стійкість), у шифраторі на основі початкового ключа генерується гама зашифрування згідно з правилом [7]:

---

[6] New European Schemes for Signatures, Integrity, and Encryption (NESSIE), IST-1999-12324 [Electronic resource]. - Mode of access: www. URL: https://www.cosic.esat.kuleuven.be/nessie
[7] eStream Project [Electronic resource].-URL: https://www.ecrypt.eu.org/stream/timetable.html

$$\Gamma_i = \phi(K_n, \Pr),$$

де P_r – параметри потокового шифру, у тому числі послідовність C_n або вектор ініціалізації.

Рисунок 1.3 – Схема застосування ПСШ

При організації зв'язку на першому етапі кожен раз здійснюється передача вектора ініціалізації IV, яка разом із ключем визначає правило формування гам зашифрування та розшифрування. На другому етапі на передачі здійснюється потокове зашифрування згідно з правилом:

$$C_i = (M_i + \Gamma_i) \bmod m.$$

Джерело ключів забезпечує управління ключами і забезпечує їх конфіденційність, цілісність, доступність і справжність. Джерело ключів також забезпечує генерування ключової інформації, до складу якої може входити синхропослідовність (вектор ініціалізації). Таке зашифровування називається потоковим.

Далі символи криптограми передаються по відкритому каналу зв'язку, до якого має повний доступ порушник (криптоаналітик).

Спочатку на прийомі виділяється вектора ініціалізації, IV символи якої використовуються разом з ключем для генерування гами розшифрування. Але для правильного розшифрування C_n має бути прийнятою правильно. За наявності хоча б однієї не виявленої помилки гама розшифрування буде генерована з помилками і здійснити розшифрування буде неможливо [7].

Одержавши криптограму та правильний вектор ініціалізації IV послідовності, користувач B здійснює потокове, тобто послідовно, розшифровування криптограми C_i згідно з правилом:

$$M_i = \left(C_i - \Gamma_i\right) \bmod n.$$

На останок символи розшифрованого повідомлення надходять одержувачу В.

1.1.5 Оцінка властивостей потокового симетричного шифру

Основним показником якості ПСШ є рівень криптографічної стійкості, що ним забезпечується. В узагальненому вигляді вона може оцінюватися кортежем параметрів: $(N_{кл}, H(k), l_0, t_б, S_{скр})$[8]

– кількість ключів з довжиною l_k , що можуть застосовуватись:

$$N_{кл} = 2^{l_k}$$

– ентропія джерела ключів:

$$H(k) = \log N_{кл} = l_k$$

– відстань єдності шифру:

$$l_0 = \frac{H(k)}{2\log_2 m}$$

– безпечний час:

$$t_б = \frac{N_в}{\gamma \cdot K} P_{KPA}$$

де $N_в$ – кількість групових операцій, що потрібно виконати;

γ – потужність криптосистеми;

K – кількість секунд у році – 3.15 10^7 сек/рік;

P_{KPA} – ймовірність успішного виконання криптоаналізу.

Якщо це атака типу «брутальна сила», то $N_в = N_{кл}$.

---

[8] Menezes AJ Handbook of applied cryptography [Text] / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. - CRC press, 2010

– структурна скритність Γ_i:

$$S_{скр} = \frac{l_H}{L_n}$$

де l_H – мінімальна кількість символів Γ_i, які необхідно правильно перехопити для того, щоб визначити закон формування Γ_i.

Відмітимо також, що гама шифрування у більшості випадків має задовольняти ряду вимог. Основними з них є такі:

1) період повторення l_n повинний бути не менше допустимого $l_д$:

$$l_n \geq l_д$$

У реальних ПСШ величина $l_д$ може змінюватись у межах

$$l_g = 2^{128} \div 2^{256} \approx 10^{77}.$$

2) ймовірність перекриття шифру не повинна перевищувати допустиму величину $P_п$. Перекриття шифру – це факт генерування та зашифровування різних повідомлень однаковими відрізками гами шифрування, тобто

$$\begin{cases} C_i = M_i \oplus \Gamma_i, & i = \overline{1,k} \\ C_i' = M_i' \oplus \Gamma_i, & i = \overline{1,k} \end{cases}.$$

Складемо за модулем 2 обидві криптограми:

$$C_i + C_i' = (M_i \oplus M_i') + (\Gamma_i \oplus \Gamma_i) = M_i \oplus M';$$

Дешифрування суми двох повідомлень є нескладним, що дозволяє знайти повідомлення;

3) можливість відновлення Γ_i у просторі й часі;

4) структурна скритність (секретність) гами:

$$S_{скр} \to 1, S_{скр} > S_{доп};$$

5) безпечний час має бути набагато більше часу цінності інформації:

$$t_б >> t_ц$$

Необхідно відмітити, що ПСШ може застосовуватись у двох основних режимах – потокового гамування та зі зворотним зв’язком по шифрованому тексту (самосинхронізації).

1.1.6 Застосування БСШ у режимах потокового шифрування

БСШ найбільш широко застосовуються в режимах потокового симетричного шифрування. В цьому випадку перший режим БСШ простої заміни застосовується для виробки блоків гами шифрування. Хоча цим режимам роботи наявний основний недолік – не достатня швидкодія, але вони знайшов застосування і дозволений для усіх існуючих БСШ. Розглянемо ці режими для випадку застосування міждержавного стандарту – ГОСТ 28147-89 (ДСТУ ГОСТ 28147-2009)[9].

Робота алгоритму ГОСТ 28147-89 у режимі гамування

У цьому режимі відкриті дані *M*, які підлягають шифруванню, розбиваються на блоки M_i довжиною по 64 біти. Алгоритм зашифрування у режимі гамування наведено на рис. 1.4. Рівняння зашифрування даних може бути подане в такому вигляді [8]:

$$\Gamma(i) = A\big(Y(i-1)\ [+]\ C2,\ Z(i-1)\ \{+\}\ C1\big),$$

$$C(i) = (i)M(i)\ ,$$

Де $C(i)$ – 64-розрядний блок зашифрованого тексту;

А – функція шифрування в режимі простої заміни;

$C1\ i\ C2$ – константи: C1 = 01010101h, C2 = 01010104h;

Y(i) і Z(i) – 32-розрядні числа, які визначаються ітеративно за формулами:

$$\big(Y(0),\ Z(0)\big) = A(S),$$

$$\big(Y(i),\ Z(i)\big) = \big(Y(i-1)\ [+]\ C2,\ Z(i-1)\ \{+\}\ C1\big)$$

де S – 64-розрядна посилка вектора ініціалізації *IV*.

Посилка вектора ініціалізації *IV* не є секретним елементом шифру і передається разом із зашифрованим повідомленням. При розшифруванні вектора ініціалізації *IV* посилка відокремлюється та формується вектор $\big(Y(0),\ Z(0)\big)$, а

[9] ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. – Введ. 01–07–1990. – М. : Изд-во стандартов, 1989. – 28 с.

потім формується гама розшифрування $\Gamma(i)$, яка має бути ідентичною гамі зашифрування.

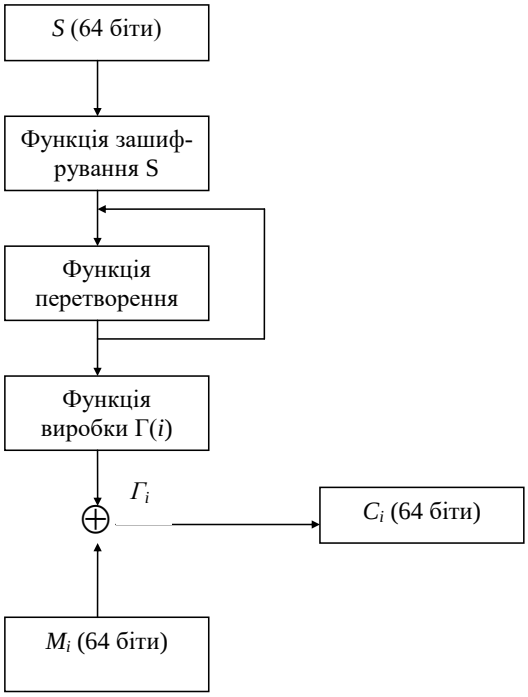


Рисунок 1.4 – Режим гамування ГОСТ 28147-89

Далі, 64-розрядний блок відкритого тексту $M(i)$ обчислюється за формулою:

$$M(i) = \Gamma(i) \oplus C(i),$$

де $\Gamma(i)$ – блок гами розшифрування.

Робота алгоритму ГОСТ 28147-89[10] у режимі гамування зі зворотним зв'язком по шифр-тексту

У цьому режимі відкриті дані *M*, які підлягають зашифруванню, розбиваються на блоки $M(i)$ довжиною 64 бітів (рис. 1.5). Рівняння зашифрування даних у цьому режимі може бути подане у вигляді:

$$C(1) = A(S) \oplus M(1),$$

[10] ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. – Введ. 01–07–1990. – М. : Изд-во стандартов, 1989. – 28 с.

$$C(i) = A(C(i-1)) \oplus M(i) = \Gamma(i) \oplus M(i)$$

де $C(i)$ – 64-розрядний блок зашифрованого тексту;

A – функція зашифрування у режимі простої заміни;

S – 64-розрядна вектора ініціалізації *IV* посилка.

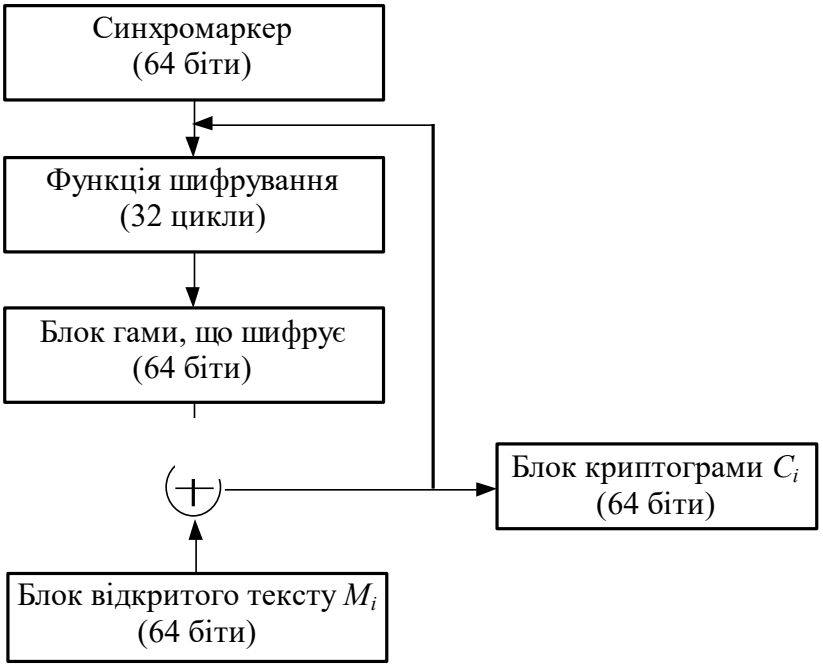


Рисунок 1.5 – Режим гамування зі зворотним зв’язком за шифр-текстом

Рівняння розшифрування у режимі гамування зі зворотним зв’язком може бути подано рівняннями:

$$M(1) = A(S) \oplus C(1),$$

$$M(i) = A(C(i-1)) \oplus C(i) = \Gamma(i) \oplus C(i)$$

Основною особливістю режиму гамування зі зворотним зв’язком за шифр-текстом є те, що в ньому не гарантується період повторення гами, оскільки це випадкова велична. Його можна дослідити використовуючи математичний апарат узагальненого парадоксу про день народження. Іншою, такою ж важливою особливістю режиму гамування зі зворотним зв’язком за шифр-текстом є залежність від якості каналу зв’язку. У сенсі, що при появі у криптограмі помилок, отримують розмноження помилок, що виявляється і здійснюється повторна синхронізація (автоматичний перезапуск) [28].

Таким чином, БСШ ГОСТ 28147-89 може застосовуватись у двох режимах потокового симетричного шифрування – гамування та гамування із самосинхронізацією. Основними недоліками цих режимів роботи є невиконання сучасних вимог до періоду повторення гами шифрування. Так, можна показати, що період гами в режимі лічильника (гамування) складає $2^{64} – 2^{32}$-1, а в режимі зі зворотним зв'язком по шифр-тексту менше вказаної величини і є випадковою величиною.

1.1.7 Уніфікація функцій потокових симетричних шифрів

Для уніфікації й застосування подання нові потокові шифри подаються як генератори гами. Такий підхід суттєво спростив їх реалізацію та впровадження. Генератори гами можна поділити на два великі класи: синхронні, або потокового шифрування, та генератори гами з самосинхронізацією.

Синхронні генератори гами

Синхронний генератор гами є скінченним автоматом. Він визначається через такі складові:

1. Функцію ініціалізації $Init$, яка приймає у якості вхідних даних ключ K і вектор ініціалізації IV, і виводить початковий стан S_0 для генератора гами. Причому вектор ініціалізації має вибиратися таким чином, щоб ніякі два повідомлення ніколи не були зашифровані з використанням одного й того самого ключа іта одного й того самого IV.

2. Функцію наступного стану $Next$, яка приймає в якості вхідних даних поточний стан генератора гами S_i і виводить наступний стан генератора гами S_{i+1}.

3. Функцію гами $Strm$, яка приймає в якості вхідних даних стан генератора гами S_i і виводить блок гами Z_i.

Коли синхронний генератор гами ініціюється вперше, то він вводить початковий стан S_0, визначений як

$$S_0 = Init(IV, K).$$

За запитом синхронний генератор гами для $i = 0,1,...$ виконує:

1. Виведення блока гами

$$Z_i = Strm(S_i, K).$$

2. Оновлення стану скінченного автомата

$$S_{i+1} = Next(S_i, K).$$

Тому для визначення синхронного генератора гами необхідно тільки описати функції $Init$, $Next$ і $Strm$, разом з довжинами і алфавітами ключа, вектором ініціалізації, станом і вихідним блоком.

Генератори гами з самосинхронізацією

Генерація гами для потокового шифру із самосинхронізацією залежить тільки від попередніх зашифрованих текстів, ключа і вектора ініціалізації. Нижче визначається загальна модель для генератора гами для потокового шифру із самосинхронізацією.

При цьому потоковий шифр із самосинхронізацією відрізняється від синхронного потокового шифру залежністю гами тільки від попереднього шифр-тексту, вектора ініціалізації та ключа, тобто генератор гами працює без внутрішнього стану. У результаті, алгоритм розшифрування для такого шифру може відновлюватися зі стану втрати синхронізації, після отримання достатньої кількості блоків шифр-тексту. Метод генерації гами залежить від вибраної вихідної функції Out, яка зазвичай представляє бінарний адитивний режим [29].

Основними функціями є наступні:

1. Функція ініціалізації $Init$, яка приймає в якості вхідних даних ключ K і вектор ініціалізації IV і виводить внутрішні вхідні дані для генератора гами.

2. Функція гами $Strm$, яка приймає як вхідні дані S і r блоків шифр-тексту $C_{i-1}, C_{i-2}, ..., C_{i-r}$ і виводить блок гами Z_i.

Для визначення генератора гами з самосинхронізацією необхідно тільки визначити число блоків зворотного зв’язку r і функції $Init$ і $Strm$.

Вихідні функції потокового шифру

Нижче надається опис двох вихідних функцій потокового шифру, що використовуються в потоковому шифрі для комбінування гами з відкритим текстом для отримання шифр-тексту.

Вихідна функція виводу для синхронного потокового шифру або потокового шифру з самосинхронізацією є оборотною функцією Out, у якій для отримання блоку шифр-тексту $C_i (i \geq 0)$ комбінується блок відкритого тексту P_i, блок гами Z_i і, необов'язково, деякі інші вхідні дані.

Шифрування блоку відкритого тексту M_i за допомогою блоку гами Z_i подається таким чином:

$$C_i = Out(M_i, Z_i, R),$$

а розшифрування блоку шифр-тексту C_i за допомогою блока гами Z_i задається як:

$$M_i = Out^{-1}(C_i, Z_i, R)$$

Вихідна функція має бути такою, щоб для будь-якого блоку гами Z_i, блоку відкритого тексту M_i та інших вхідних даних R, виконувалась умова:

$$M_i = Out^{-1}(Out(M_i, Z_i, R), Z_i, R)$$

1.2 Асиметричні криптосистеми як альтернатива для використання у якості базових криптографічних перетворень у системах моніторингу контактів

Найбільшою особливістю асиметричних перетворень є використання асиметричної пари ключів, які містить відкритий ключ, що відомий всім, та особистого ключа, що пов'язаний з відкритим ключем за допомогою певного математичного перетворення. При цьому вважається що обчислення особистого ключа, при знанні загальносистемних параметрів та відкритого ключа, повинно мати в гіршому випадку субекспоненційну складність, за умови коли

обчислення відкритого ключа при формуванні асиметричної ключової пари – поліноміальну. Зрозуміло що вказана особливість несе в собі як переваги так і недоліки, що і є предметом розгляду в цьому розділі.

Важливим подальшому викладенні є визначення криптографічної стійкості асиметричного направленого шифрування, перше за все у порівняння зі стійкістю блочних симетричних шифрів. Такий підхід є загальновизнаним і широко застосовується на практиці. В таблиці 1.1 подаються рекомендації з оцінки криптографічної стійкості асиметричних крипто перетворень, що наведені в таблиці 1.2 [9].

У таблиці 1.3 наведено результати порівняння стійкості для визнаних крипто перетворень, що знайшли застосування в національних, регіональних та міжнародних стандартах. У стовпці 1 наведено число бітів ключа для блочного симетричного шифру. У стовпці 2 подано алгоритми симетричних криптографічних перетворень. У стовпці 3 поданий мінімальний розмір параметрів для крипто перетворень(стандартів0, що ґрунтуються на перетвореннях у кінцевих полях. Прикладами таких алгоритмів можуть бути FIPS 186-3 та ГОСТ 34.310-95[11] – для цифрових підписів, а також алгоритм Діффі - Геллмана (DH) і алгоритм узгодження ключів MQV, де Lв – розмір відкритого ключа, а Lo – розмір особистого ключа. У стовпці 4 подано значення k (розмір модуля перетворення) для криптографічних перетворень, що ґрунтуються на складності вирішення задач факторизації, наприклад RSA алгоритм ANSX10.31 і PKCS#1. Посилання на ці специфікації подані у FIPS 186-3 для цифрових підписів. Значення k зазвичай використовують для того, щоб указати розмір ключа.

[11] ГОСТ 34.310-95-[Electronic resource]- URL:ttps://files.stroyinf.ru/Index2/1/4294755/4294755676.htm

Таблиця 1.1 – Асиметричні криптографічні перетворення для реалізації направленого шифрування

Параметри НШ/ Математичний апарат	Особистий ключ НРШ	Відкритий ключ НЗШ (сертифікат)	Асиметрична пара (ключ)	Загальні параметри крипто перетворення	Сертифікати	Складність крипто аналізу
НШ в кільці (RSA)	D_i	E_i	$(D_i,\ E_i)$	$N\ =\ P\ Q$	E_i	Субекспоненційна
НШ в полі Галуа *F(P)*	X_i	$Y_i = g^{X}{}_i$ $(modP)$	$(X_i,\ Y_i)$	$P,\ q,\ g$	Y_i	Субекспоненційна
НШ в групі точок еліптичних кривих *E(F(q))*	d_i	$Q_i = d_i G$ $(modq)$	(d_i, Q_i)	$a,\ b,\ G,\ n,$ $f(x)(P),$ h	Q_i	Експоненційна
НШ в гіпереліптичних кривих	C_i	$D_2 =\ c_i D_1$	$(c_i,\ D_2)$	$f(x),\ g(x),$ $q,\ D_1,\ g,\ J$	D_2	Експоненційна
НШ зі спарюванням точок еліптичних кривих	$d_{iD} = s\ Q_{iD}$	$Q_{iD} = H_1$ (ID)	$(d_{iD},\ Q_{iD})$	$G_1,\ G_2,\ e,\ H_1,$ $P,\ H_2,\ H_3,$ $F_2{}^m,\ P_p$	Q_{iD}	Експоненційна – субекспоненційна
НШ в кільці зрізаних поліномів (NTRU)	$f\ =\ 1+\ pF$ $(modq)$	$h = f^1 * g * p$ $(modq)$	$(f,\ h)$	$N, q, p,\ f,$ $g, df,\ dg,\ c$		Експоненційна – субекспоненційна

Таблиця 1.2 – Порівняння стійкості стандартизованих асиметричних крипто перетворень

Рівень стійкості, в бітах	Симетричні	Оцінка часу крипто аналізу, MIPS-years	Геш функції	Параметри асиметричних перетворень				
				DSA	RSA	EC-DSA	IBE (BF, BB1)	NTRU
До 2010 р. (мін. 80 біт стійкості)	2TDEA 3TDEA AES-128 AES-192 AES-256	10^9	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160	Min.: p = 512 q = 160	N =263 q =2048 d_f = 113
До 2030 р. (мін. 112 біт стійкості)	3TDEA AES-128 AES-192 AES-256	10^{17}	SHA-224, SHA-256, SHA-384, SHA-512	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224	Min.: p = 1024 q = 224	N =401 q =2048 d_f = 113
Після 2030 (мін. 128 біт стійкості)	AES-128 AES-192 AES-256	10^{23}	SHA-256, SHA-384, SHA-512	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256	Min.: p = 1536 q = 256	N =449 q =2048 d_f = 134
Рівень стійкості 192 біта	AES-192 AES-256	10^{41}	SHA-384, SHA-512	Min.: L = 7680 N = 384	Min.: k=7680	Min.: f=384	Min.: p = 3840 q = 384	N =677 q =2048 d_f = 153
Рівень стійкості 256 біта	AES-256	10^{63}	SHA-512	Min.: L = 15360 N = 512	Min.: k=15360	Min.: f=512	Min.: p = 7680 q = 512	N =1087 q =2048 d_f = 120

Таблиця 1.3 – Алгоритми і параметри NTRU, що рекомендуються

Обмеження дії	Рівень безпеки	Блоковий шифр	Функція гешування	Множина параметрів NTRU X10.98
2030	112-біт	Triple-DES (тільки 3 ключі), AES-128, AES-192, AES-256	SHA-224, SHA-256, SHA-384, SHA-512	ees401ep1, ees541ep1, ees659ep1
2031 і пізніше	128-біт	AES-128, AES-192, AES-256	SHA-256, SHA-384, SHA-512	ees449ep1, ees613ep1, ees761ep1
	192-біт	AES-192, AES-256	SHA-384, SHA-512	ees677ep1, ees887ep1, ees1087ep1
	256-біт	AES-256	SHA-512	ees1087ep2, ees1171ep1, ees1499ep1

1.2.1 Криптосистема RSA

Історично першою у 80-і роки XX століття широке розповсюдження отримали асиметричні крипто перетворення(криптосистема) з відкритими ключами, що нині відома як RSA система.

Основною особливістю RSA крипто системи є її асиметричність, коли ключ зашифрування $K^з$ не співпадає з ключем розшифрування K^p , тобто

$$K_j^з \neq K_j^p,$$

а знайти один ключ при відомому другому для відповідних значень загальносистемних параметрів можна не нижче ніж з субекспоненційною складністю. Хоч на сьогодні RSA криптосистема піддається нападкам і відносно неї даються різні прогнози, але вона проіснувала майже 35років і дозволяє реалізувати НШ. Крім того, на наш погляд, RSA система дозволяє якісно реалізувати криптографічними методами таку основну функцію, як спостережливість, в змісті причетності відправника та отримувача. Так причетність відправника може бути забезпечена за рахунок здійснення цифрового підпису з використанням особистого (таємного) ключа, а перевірка цілісності та справжності підписаної інформації здійснюються з використанням особистого (публічного) ключа. Далі направлене шифрування може бути здійснене з використанням другої ключової пари, відкритий ключ отримувача якої застосовують для направленого шифрування, а особистий ключ застосовується для розшифрування повідомлення. Тому розглянемо цю класичну систему докладно.

Для великих N з великими простими множниками розкладання на множники є серйозною проблемою, але не настільки, як потрібно. Разючою ілюстрацією цього може служити наступна історія.

Наведемо також історію вирішення задачі факторизації. Для великих N з великими простими множниками розкладання на множники є серйозною проблемою, але не настільки, як потрібно. Разючою ілюстрацією цього може служити наступна історія. У 1977 році три винахідники алгоритму RSA

наважилися запропонувати читачам популярного журналу Scientific American дешифрувати направлено зашифроване повідомлення. Мартін Гарднер опублікував в журналі Scientific American зашифровану головоломку, для розшифрування якої потрібно було факторизувати RSA модуль перетворення-таке 129 розрядне число(428 бітів) [10].

Повідомлення, «The magic words are squeamish ossifrage», яке потрібно було зашифрувати, спочатку було записане у вигляді цілого числа ($a = 01,\ b = 02,\ c = 03,\ \ldots,\ z = 26$, прогалина 00). Потім воно було зашифроване направлено на відкритому ключі $Ek = 9007$.Наведені модуль перетворення та відкритий ключ , а також додаткова інформація що $N = P\,Q$, де $P\,i\,Q$ – прості числа є довжиною відповідно 64 та 65 десяткових розрядів, були опубліковані в указаному журналі.

За розшифровку цього повідомлення вони запропонували нагороду в 100 дол. За їхніми оцінками, задача не могла бути вирішена раніше, ніж приблизно через 40 квадрильйонів років. Але в квітні 1994 року D. Atkins, M. Graff, K. Lenstra і C. Leylang зажадали виплати призової суми за успішний крипто аналіз всього після восьми місяців спільної роботи в Internet. Для вирішення задачі факторизації вказаного модуля було використано 1600 комп’ютерів різної потужності - від найпростіших – до станції Gray C90. Задача факторизації, яка вимагала близько 5000 міпсороків, була вирішена з серпня 1993 по квітень 1994 року з застосуванням квадратичного решета. Одиницею вимірювання складності задачі в даному випадку є MIPS-рік – обсяг роботи, виконуваної протягом року процесором, що здійснює обробку одного мільйона команд у секунду, що приблизно еквівалентно виконанню $3*10^{13}$ команд. Так, машина на базі Pentium з частотою 2000 МГц показує швидкість 500 MIPS.

Необхідно відмітити, що згідно вимог нормативних документів та міжнародних стандартів в інформаційних технологіях повинні надаватися послуги причетності джерела та одержувача інформації (спостережливість). Причетність джерела, тобто авторство може бути забезпечено за рахунок

застосування ЦП. Складніше забезпечити причетність одержувача. Ця задача може бути розв'язана за рахунок використання направлених шифрів.

Особливістю крипто перетворень типу НШ є такі:

– пряме криптографічне перетворення виконується з використанням відкритого ключа $K_в$.

– зворотне криптографічне перетворення виконується з використанням особистого ключа $K_о$.

– Ключова пара ($К_о$, $Кв$) повинна бути випадковою та вибиратись із повної множини дозволених для використання ключових пар, причому $K_в \neq K_о$

Згідно вимог нормативних документів та міжнародних стандартів в інформаційних технологіях повинні надаватися послуги причетності джерела та одержувача інформації (спостережливість). Причетність джерела, тобто авторство може бути забезпечено за рахунок застосування ЦП. Складніше забезпечити причетність одержувача. Ця задача може бути розв'язана за рахунок використання направлених шифрів.

Особливість крипто перетворень типу НШ:

– пряме з використанням відкритого ключа $K_в$.

– зворотне з використанням особистого ключа $K_о$.

– Ключова пара ($К_о$, $Кв$) повинна бути випадковою та вибиратись із повної множини дозволених для використання ключових пар, причому $K_в \neq K_о$

Відомий ряд методів побудування криптографічних систем направленого шифрування. Основними з них є такі:

1) Метод складання рюкзака. Необхідно вкласти в рюкзак предмети з різною вагою, але щоб вага рюкзака залишалася постійною. Це не стійка система.

2) У 1978р. була опублікована стаття, у якій був запропонований алгоритм RSA направленого шифрування. Він закріплений в міжнародному стандарті ISO 11166-1,2. Крім того в США він закріплений в стандарті ANSI X10.31.

3) У 1985р. Єль-Гамаль запропонував нову схему НШ Є-2. Всі ці алгоритми були запатентовані. На сьогодні рекомендовано до застосування стандарти X10.30 та у міжнародних стандартах ISO/IEC 1170-3 ISO/IEC 15946-10.

1.2.2 Криптоперетворення НШ в кільцях (RSA)

Алгоритм направленого шифрування RSA є блоковим, у ньому повідомлення M розбивається на блоки M_i, з довжиною блоку $l_i \geq l_\partial$ (на сьогодні 2048 біт мінімум), реально 2048, 3072 і більше бітів. Блок криптограма C_i обчислюється за правилом [11]

$$C_i = M_i^{E_K} (\mathrm{mod}\, N),$$

де E_k – є відкритий ключ прямого перетворення, N – модуль перетворення є добутком виду

$$N = P * Q,$$

де в свою чергу P, Q – великі прості, скоріше сильні, числа.

Якщо l_p є довжина простого числа P, наприклад в бітах, а l_q – довжина простого числа Q, то довжина модуля N

$$l_N = l_p + l_q.$$

Розшифрування блока криптограми здійснюється за правилом:

$$M_i = C_i^{D_K} (\mathrm{mod}\, N),$$

де D_K – є ключ зворотного перетворення, тобто розшифрування $D^K = K^P$. Однозначність розшифрування можна підтвердити. В результаті отримаємо:

$$M_i = M_i^{E_K D_K} (\mathrm{mod}\, N).$$

Оскільки ключова пара (E_K, D_K) пов'язана між собою порівнянням:

$$E_K D_K = 1 (\mathrm{mod}\, \phi(N)),$$

де $\phi(N)$ є функцією Ойлера від модуля N

$$\phi(N) = \phi(P \cdot Q) = \phi(P) \cdot \phi(Q) = (P-1) \cdot (Q-1).$$

Якщо має єдине рішення, тобто існує єдина пара E_K, D_K, то такий шифр є однозначним і при таких умовах RSA криптосистема забезпечує однозначне направлене шифрування.

Зазначимо, що з точки зору забезпечення максимально можливої крипто-стійкості прості числа *P* і *Q* мають бути сильними в широкому або вузькому значенні. Так просте число *P* вважатимемо сильним в широкому значенні, якщо $P = 2R + 1$, де *R* – також велике просте число.

Аналогічно визначається і сильне в широкому значенні просте число *Q*.

Просте число *P* вважається сильним у вузькому значенні, якщо $P - 1$ містить в своєму канонічному розкладі велике просте число *R*, *P*+1 містить в своєму розкладі велике просте число *S*, а крім того *R*-1 містить в своєму розкладі велике число *T*.

Генерування асиметричної ключової пари. Система RSA відноситься до криптосистем з відкритими ключами. В цій системі ключі $E_k \neq D_k$, причому один з них має бути особистим, а другий – відкритим. Наприклад, E_k – особистий, а D_k – відкритий, якщо вони використовуються для ЕЦП і навпаки, якщо використовуються для направленого шифрування.

Усі параметри (*N*,*P*,*Q*) також поділяються на 2 класи: *N* – відкритий, *P*,*Q* – конфіденційні (секретні).

Сутність забезпечення моделі взаємної недовіри – кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Користувач також забезпечує цілісність і дійсність відкритих ключів.

E_k, D_k – мають вибиратися з повної множини випадково, порівняно ймовірно і незалежно, мають забезпечувати однозначну оборотність прямого та зворотного перетворення. Відповідним чином засвідчений відкритий ключ є сертифікатом/

Значення E_k, D_k для практичних використань мають задовольняти умову

$$1 \le E_K, D_K < \phi(N),$$

де $\phi(N) = \phi(P * Q) = \phi(P) * \phi(Q) = (P - 1)(Q - 1)$.

Порівняння можна звести до Діафантового рівняння: ax+by=1.

Це діафантове рівняння – нормоване, тому що справа коефіцієнт дорівнює 1; *a*, *b* – цілочисельні коефіцієнти, *x*, *y* – невідомі. Порівняння можна подати у вигляді:

$$E_K D_K = k * \phi(N) + 1,$$

k – деяке невідоме число.

Діафантове рівняння має цілочисельне розв'язання, якщо *a* і *b* цілочисленні, і $a \geq b$, *a* і *b* взаємно прості. Подавши у вигляді

$$\phi(N) * (-k) + E_K D_K = 1 \ ,$$

отримаємо $a=\varphi(N)$, $x=(-k)$, $b=E_k$, $y=D_k$.

Якщо E_k сформувати випадково, то *a* та *b* – відомі числа, а *x* та *y* – невідомі, що підлягають визначенню.

Найбільш швидке розв'язання дає застосування ланцюгових дробів, які дозволяють визначити *x* та *y* як

$$\begin{cases} y = (-1)^{\mu} a_{\mu-1} \\ x = (-1)^{\mu+1} b_{\mu-1} \end{cases},$$

де μ – порядок ланцюгового дробу, *a* і *b* – параметри ланцюгового дробу.

Знаходимо параметри:

a/*b* подається у вигляді ланцюгового дробу

$$\frac{a}{b} = r_0 + \cfrac{1}{r_1 + \cfrac{1}{r_2 + \cfrac{1}{r_3 + \cdots \cfrac{1}{\mathrm{r}_{\mu} + 0}}}},$$

μ - порядок ланцюгового дробу, перший коефіцієнт, у якого залишок дорівнює 0. Значення (a_0,b_0) та (a_1,b_1) визначаються як

$$\frac{a_0}{b_0} = r_0 = \frac{r_0}{1} \qquad \left.\begin{matrix} a_0 = r_0 \\ b_0 = 1 \end{matrix}\right\},$$

$$\frac{a_1}{b_1} = r_0 + \frac{1}{r_1} = \frac{r_0 r_1 + 1}{r_1} \qquad \left.\begin{matrix} a_1 = r_0 r_1 + 1 \\ b_1 = r_1 \end{matrix}\right\}.$$

Значення (a_2,b_2), (a_3,b_3) і т.д. визначаються рекурентно відповідно до правил

$$\begin{cases} a_\mu = r_\mu * a_{\mu-1} + a_{\mu-2} \\ b_\mu = r_\mu * b_{\mu-1} + b_{\mu-2} \end{cases}.$$

Середнє число ітерацій в (1.60), тобто $\overline{\mu}$, можна визначити як [36]

$$\overline{\mu} = \frac{12 \ln 2}{\pi^2} \ln E_k .$$

Попередня оцінка стійкості[12]. В системі RSA крипто аналіз, метою якого є визначення особистого (таємного) ключа, наприклад $E_к$ ключа ключової пари (E_K, D_K), де $D_к$ є відкритий ключ, може бути здійснений таким чином:

1. Зловмисник отримує системні параметри (однакові для обох користувачів) N_j та відкритий ключ Ек.
2. Використовуючи спеціальну крипто аналітичну систему здійснюється факторизація модуля N_j, в результаті чого він визначає прості числа P_j та Q_j.
3. Розраховується значення функції Ойлера

$$\phi(N) = \phi(P * Q) = \ = \phi(P) * \phi(Q) = (P-1)(Q-1).$$

4. Використовуючи методику, наведену в (1.49), здійснюється розв’язок порівняння $E_K D_K = 1 (\mathrm{mod}\, \phi(N))$.

Взагалі, найбільш простим методом крипто аналізу є підбір ключової пари (E_K, D_K), тобто при відомих $(\mathrm{N_j}, \mathrm{E_K})$ визначається *Dк*.

Нехай N_j має довжину l_{N_j} тоді, якщо $N_j = P_j Q_j$, то

$$\mathrm{l_P} + l_Q = l_N \ \text{ і } \ l_P \approx l_Q = \frac{l_N}{2}.$$

[12] Bakhtiari M., Maarof M. A. Serious Security Weakness in RSA Cryptosystem (англ.) // IJCSI — 2012. — Vol. 9, Iss. 1, No 3. — P. 175—178.

Область існування для ключа D_K можна визначити, як всі цілі числа, що не перевищують $\phi(N)$ та є взаємно простими, тобто $(D_K, \phi(N)) = 1$. Підбір D_K із повної множини є задачею, що набагато складніша, ніж алгоритм, заданий вище пп. 1-4.

Проведені дослідження підтвердили, що необхідний рівень стійкості в RSA забезпечується в тому випадку, якщо прості числа є сильними.

Покладемо, що як D_K використовуються прості числа, тоді справедливе таке: $(D_K, \phi(N)) = 1$, $\alpha \le D_K \le \phi(N_j) - 1$, $\phi(N_j) = (P_j - 1)(Q_j - 1)$.

Використовуючи теорему Чебишева, визначимо кількість особистих ключів, як

$$n_{D_K} = \frac{\phi(N_j)}{\ln \phi(N_j)} = \frac{(P_j - 1)(Q_j - 1)}{\ln (P_j - 1)(Q_j - 1)} \approx \frac{N_j}{\ln N_j}.$$

1.2.3 Проблемні питання крипто перетворень типу RSA.

Існує ряд проблемних питань теорії та практики RSA. В першу чергу до них необхідно віднести такі.

1) Є публікації в яких стверджується існування та запропоновано один із варіантів якби «поліноміального» методу факторизації модуля.

2) Отримані теоретичні та практичні результати факторизації , перше за все у вигляді спеціального решета числового поля та загального решета числового поля, якими підтверджено субекспоненціальний характер складності факторизації. Так для двійкового та загального решіт числового поля складність крипто аналізу може бути оцінена як:

$$I = \exp(\delta (\log N)^{\nu} (\log \log N)^{1-\nu}),$$

δ, ν – параметри методу. Наприклад, для квадратичного решета δ=1,96; ν=1/3, спеціального решета числового поля δ=1,92; ν=1/10.

3) Необхідність постійного збільшення з метою забезпечення допустимого рівня стійкості довжини модулі N криптографічного перетворення , так нині

рекомендується довжина модуля не менше 2048 бітів, що створює проблеми форматів, стандартизації, апаратної реалізації тощо.

4) Збільшення довжини ключів практично до довжини модуля, що викликає підвищення складності прямих та зворотних криптографічних перетворень, а також проблемні питання з форматами та уніфікацією.

5) Числа P і Q мають бути не просто простими, а «сильно» простими числами, наприклад, мати вигляд P=2R+1, де R – у свою чергу також просте число.

6) Для забезпечення стійкості при побудові параметрів та ключів необхідно також :

– відбраковувати ключі-близнята, тобто відмовлятися від ключової пари у якої $E_k = D_k$;

– відмовлятися від простих чисел P та Q, які близькі за значенням, тобто P≈Q;

– відслідковувати можливу появу блоків повідомлень, що не зашифровуються, та приймати відповідні зміни в повідомленні тощо [12].

1.2.4 Направлене шифрування у кільці зрізаних поліномів. Алгоритм NTRU.

Представником направленого шифрування у кільці зрізаних поліномів є алгоритм NTRU. Базовими об’єктами у NTRU є поліноми порядку $N-1$ з цілими коефіцієнтами виду

$$a = a_0 + a_1 X^1 + \ldots + a_{N-1} X^{N-1}$$

Операція додавання в кільці поліномів визначена просто як додавання коефіцієнтів при відповідних ступенях, тобто

$$a + b = (a_0 + b_0) + (a_1 + b_1) X + \ldots + (a_{N-1} + b_{N-1}) X^{N-1}.$$

Операція множення визначена так само, за допомогою множення коефіцієнтів при відповідних ступенях поліномів, тільки з однією особливістю - при множені поліномів необхідно:

- X^N необхідно замінити на 1;
- X^{N+1} замінити на X ;
- X замінити на X^2 і т.д.

Результат множення можна подати у вигляді

$$a*b = c_0 + c_1 X + \ldots + c_{N-1} X^{N-1} \ ,$$

де

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots a_k b_0 + a_{k+1} b_{N-1} + a_{k+2} b_{N-2} + \ldots + a_{N-1} b_{k+1}.$$

Також необхідно відмітити, що операції додавання та множення в кільці зрізаних поліномів володіють властивістю дистрибутивності, тобто

$$a*(b + c) = (a*b) + (a*c)$$

Кільце з визначними таким чином операціями додавання та множення називається кільцем зрізаних поліномів .

Особливістю NTRU є те, що в кільці зрізаних поліномів коефіцієнти також приводяться за модулями p та q. Тобто коефіцієнти ai та bi додаються та множаться за модулями p та q в необхідних випадках.

Алгоритм шифрування NTRUEncrypt

Корпорацією NTRU Cryptosystem[13] опубліковано декілька версій алгоритму NTRU, два з них були реалізовані в цьому проекті. Розглянемо сутність алгоритму.

Генерування асиметричної пари ключів. Нехай генерування асиметричної пари розпочинає абонент B. Для цього він вибирає(генерує) два випадкових поліномів *f* і *g*, що визначені в кільці *R*. Причому поліноми *f* і *g* повинні мати мультиплікативно зворотні поліноми в кільці по модулю загальних параметрів *p* і *q*. Позначимо такі мультиплікативно зворотні значення для поліному *f* як $f_p^{(-1)}(Fp)$ та $f_q^{(-1)}(Fp)$ відповідно. Вони повинні бути розраховані тільки точно для обраного *f*.

[13] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. NTRU: A Ring Based Public Key Cryptosystem. In Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267—288

Необхідно відмітити, що в стандарті NTRU X9.98-2010 особистий ключ f повинен обчислюватись згідно рекомендації в кільці поліномів $(Z/q\,Z)[X]/(X^{N-1})$:

$$f = (1 + p\,F)\ mod\ q,$$

де p = 3 – загальний (доменний параметр), а F випадковий поліном, алгоритм генерування якого визначено в стандарті.

Далі абонент В обчислює свій відкритий ключ у вигляді многочлену h у кільці поліномів $(Z/q\,Z)[X]/\left(X^{N-1}\right)$ згідно правилу

$$h = p(f_q^{(-1)} * g) mod q\ ,$$

де g, як уже вказувалось, є також випадково обраний поліном у кільці . Поліноми f і g крім того що повинні бути "випадково" обраними в R_q , але також повинні мати конкретну кількість коефіцієнтів, 0, +1 і -1, тобто обрані випадково із множини поліномів з фіксованим числом символів коефіцієнтів 0, +1 і -1. Особистий (таємний) ключ у вигляді многочлену f разом із зворотними $f_p^{(-1)}(Fp)$ та $f_q^{(-1)}(Fq)$ є таємними ключовими даними, h – відкритим ключем. Значення N, p і q є параметрами алгоритму шифрування NTRU. В цілому, таким чином, асиметричною парою ключів є (f, h) пара особистого та відкритого ключів, що являються поліномами степені N-1[14].

Алгоритм зашифрування. Нехай абонент А хоче направлено зашифрувати для абонента В двійкове повідомлення m. Для цього А повинен знати справжні загальні параметри N, p і q та відкритий ключ абонента $B\ -h_b$. Далі абонент А генерує «випадково» у кільці R_q многочлен r_a (по суті ключ сеансу). Безпосередньо абонент А зашифрування виконує шляхом обчислення значення

$$c = (\ r_a * h_b + m) mod q$$

[14] Hoffstein J., Pipher J., Schanck J.M., Silverman J.H., Whyte W., Zhang Z.Choosing parameters for NTRUEncrypt. –Режим досту-пу: http://eprint.iacr.org/2015/708.

У рівнянні множення r_a на h_b виконується у рамках розміру кільця, як зазначено вище, тобто у вигляді згортки за модулем q, а повідомлення m додається за модулем q.

Алгоритм розшифрування. Для розшифрування криптограми *c* абонент B повинен мати справжні загальні параметри *N*, *p* і *q*. Розшифрування здійснюється засобом згортки поліномів N-1 степені в кільці $(Z/qZ)[X]/(X^{N-1})$: особистого ключа f_b та криптограми *c* як

$$a = f_b * c mod q.$$

Надалі коефіцієнти полінома *a* для отримання повідомлення *m* приводяться по модулю в інтервалі $[A, A+q-1]$, а також по модулю *p* для отримання кандидата в розшифроване повідомлення m'.

Необхідно відмітити, що при розшифруванні випадково можемо отримати повідомлення, яке буде відрізнятися від вихідного. Це може відбутися за рахунок виконанні операції спочатку за модулем *q*, а потім за модулем *p*. На практиці, якщо правильно обрати загальні параметри імовірність появи такої помилки не перевищує $2^{-100}\left(10^{-30}\right)$ [15].

Отриманий поліном a приводиться за модулем, але таким чином, щоби коефіцієнти приймали значення $-q/2$ та $q/2$. В результаті обчислюється відновлений поліном –

$$m = a * F_p ,$$

де $Fp = (f_p^{(-1)})$ є частиною вказаної вище особистого ключа(він є і мультиплікативно зворотним до $f\ a mod\ p$.

Покажемо, що алгоритми зашифрування та розшифрування є оборотними. В результаті отримаємо, що

$$a = f_b * c\ mod\ q = f_b * (r_a * h_b + m)\ mod\ q = f_b * ((p\ _f - q_1)\ r * g + m)\ mod\ q =$$
$$= p_r * g + f_b * m\ mod\ q.$$

[15] Hoffstein, J. Silverman. Optimizations for NTRU. Public-Key Cryptography and Computational Number Theory (Warsaw, September 11-15, 2000), DeGruyter, to appear.

Вище враховано, що f_b та f_{q-1} є мультиплікативно зворотними за модулем q. На останок, при приведенні поліному a за модулем p, отримаємо що (при $f_p^{(-1)} = Fp$)

$$F_p * a \bmod p = F_p * p_r * g + F_p * f * m \bmod p = m$$

Основні види атак. Основними атаками, що можуть бути реалізовані на алгоритм NTRU, на наш погляд, є такі[16]:

– атака з адаптивно підібраним текстом;

– атаки, що пов’язані з некоректним вибором загальних параметрів :

– атаки, що пов’язані з помилками при генеруванні ключів та параметрів;

– атаки, що пов’язані з використанням при крипто аналізі алгоритмі, що реалізуються на квантових комп’ютерах.

Для вирішення задачі пошуку найближчого вектору (найкоротшого) в теорії зведення решіток використовується метод LLL (Lenstra, Lenstra and Lovasz). Цей алгоритм знаходить достатньо невеликий вектор за поліноміальний час, але у загальному випадку алгоритм не дозволяє знайти найкоротший вектор. Існує багато вдосконалень цього методу, що зроблені вченими Schnorr, Euchner. Ці вдосконалення відомі як «глибока вставка», «блочне зведення», «зрізання». Але складність цих методів для вирішення задачі пошуку найменшого вектора в загальних решітках є експоненційною.

Також складною задачею відносно криптосистеми NTRUEncrypt Public Key є пошук найкоротшого вектора в решітці великого розміру. Сьогодні найкращим з методів крипто аналізу цієї крипто системи вважається метод зведення в решітках LLL. Для того щоб перевірити перевірки на практиці захищеність системи NTRUEncrypt, за допомогою метода LLL було вирішено багато задач знаходження найкоротшого вектора для решіток різних розмірностей. За результатами цих експериментів було отримано графічне представлення часу, необхідного для знаходження необхідного вектору для

[16] Howgrave-Graham N. A meet-in-the-midle attack on an NTRU private key / N.Howgrave-Graham, J.H.Silverman, W.Whyte //Technical report, NTRUCryptosystems, June 2003. Report, 2003.

заданої решітки. З цього графіку було екстрапольовано час здійснення крипто аналізу для решіток більшої розмірності, які використовуються на практиці, та за отриманими результатами було отримано відповідні параметри для NTRUEncrypt.

Таблиця 1.4 – Оцінки оцінку часу крипто аналізу відносно NTRUEncrypt, RSA та EC-DSA

Рівень безпеки (довжина симетричного шифру, біт)	Оцінка часу крипто аналізу, MIPS-years	Криптосистема		
		RSA	NTRU X9.98-2010	EC-DSA
80(2TDEA)	10^9	1024	N=263	f =160 – 223
112(3TDEA)	10^{17}	2048	N=401	f = 224 – 255
128(AES-128)	10^{23}	3072	N=613	f = 256 – 383
192(AES-192)	10^{41}	7680	N=500	f = 384 – 511
256(AES-256)	10^{63}	15360	N=1171	f = 512 +

В таблиці 1.4 для порівняння, наведені оцінки часу крипто аналізу відносно NTRUEncrypt, RSA та EC-DSA криптосистем для різних рівнів безпеки. В якості основного критерію рівня безпеки використовується довжина ключа блокового симетричного шифру.

1.3 Протоколи взаємодії, що можуть бути використані при реалізації систем моніторингу контактів.

1.3.1 Термінологічна база застосування протоколів

Перш за все визначимо, що представляє собою поняття «протокол». Протокол – це розподілений алгоритм сумісного розв’язку об’єктами та суб’єктами деякої задачі, кожен з яких досягає мети (розв’язує задачу) з використанням деяких алгоритмів, при цьому усі об’єкти та суб’єкти

використовують однакову специфікацію даних, синхронізацій дій, організацію відновлення роботи після збоїв тощо[17].

Особливістю криптопротоколів є те, що вони виконуються на основі застосування однієї або декількох криптосистем (криптоалгоритмів), відповідних ключових даних, параметрів і т. ін. В моделі взаємної недовіри взаємодіючі об’єкти та суб’єкти, які мають між собою інформаційні співвідношення мають бути захищені від обману, в тому числі, і юридично. Джерелом погроз в цьому випадку можуть бути внутрішні об’єкти та суб’єкти (порушники), тобто авторизовані користувачі, а також зовнішні об’єкти та суб’єкти (зловмисники, криптоаналітики [13].

Криптографічні протоколи можна поділити на два великі класи:

– протоколи – примітиви або елементарні протоколи;
– прикладні або складові протоколи.

Протоколи-примітиви являють собою елементарні протоколи, з яких будуються більш складні, наприклад, прикладні протоколи. При цьому прикладні протоколи забезпечують розв’язання деякої кінцевої задачі на основі використання протоколів-примітивів.

Усі застосовувані криптографічні протоколи мають бути слушними. Протокол називається слушним, якщо він забезпечує об’єктам та суб’єктам інформаційних технологій гарантовані послуги цілісності, конфіденційності, доступності та спостережності. Більшість криптографічних протоколів можна поділити на інтерактивні протоколи та протоколи з нульовими знаннями.

Перші ознаки інтерактивних протоколів з’явились у 1985 році. Інтерактивний протокол є багатораундовим, в процесі його виконання об’єкти та суб’єкти обмінюються між собою інформацією декілька разів. Внаслідок таких дій виробляються ключі або паролі, установлюють або розподіляють секрети і т. ін.

---

[17] Ричард Э. Смит. Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. — М.: Вильямс, 2002. — С. 432. — ISBN 0-201-61599-1.

Формалізовано криптографічний протокол можна задати у вигляді *PVS* протоколу. По суті, *PVS* протокол описує логіку взаємодій двох об'єктів *P* і *V*, де *P* – об'єкт, який формулює логічне твердження *S* та доводить істинність твердження *S*. *V* – перевіряючий об'єкт, *S* – деяка логіка.

Якщо зловмисником може бути тільки *P*, то такий протокол називається інтерактивним, і має володіти двома властивостями:

– повнота протоколу;

– коректність протоколу.

Вважається, що протокол володіє властивістю повноти у випадку, якщо *S* – істинно, то *P* завжди доведе перевіряючому *V* з великою ймовірністю, що *S* – істинно.

Коректність протоколу, якщо *S* – хибне, то перевіряючий *V* з великою ймовірністю доведе *P*, що *S* – хибне. Слушність протоколу, який володіє властивостями повноти та коректності, забезпечується за рахунок багатораундового обміну інформацією між об'єктами та суб'єктами.

У випадку, якщо *V* може бути зловмисником, для забезпечення слушності протокол має володіти «нульовими знаннями».

Сутність протоколу з «нульовими знаннями»: перевіряючий *V*, отримуючи послідовність тверджень *S*, не має отримати ніяких знань про те, чому твердження *S* істинні[18].

1.3.2 Протоколи автентифікації

У найбільш узагальненому вигляді під криптографічним протоколом автентифікації будемо розуміти криптографічний протокол встановлення достовірності твердження, що об'єкт (суб'єкт) має очікувані властивості. Як правило, достовірність твердження встановлюється з деякою ймовірністю. Тому має сенс застосування такого визначення протоколу автентифікації:

---

[18] А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. Аутентификация. Теория и практика обеспечения доступа к информационным ресурсам. = Authentication. Theory and practice of ensuring access to information resources.. — М.: Горячая линия – Телеком, 2009. — С. 552

автентифікація об’єкта (суб’єкта) – це підтвердження із заданою ймовірністю того, що об’єкт (суб’єкт) є тим, за кого він себе видає [14].

Відносно механізмів автентифікації переважно можуть здійснюватись атаки, що обмежують їх ефективність. Вони можуть здійснюватись у фазі передавання. Їх можна застосовувати відносно загроз(и), проти яких ці механізми є невразливими. Механізми базуються на принципі автентифікації, який можна назвати «дещо відомо». Усі такі механізми можна застосовувати до об’єктів автентифікації, а механізми з цифровим підписом або геш-значенням можна застосовувати й для автентифікації джерела даних.

Міжнародний стандарт рекомендує використовувати для оцінки захищеності такі класи механізмів автентифікації:

Клас 0 – незахищений;

Клас 1 – захищений від розкриття заявленої ІА;

Клас 2 – захищений від розкриття заявленої ІА й атаки типу «повтор» для різних перевірників;

Клас 3 – захищений від розкриття заявленої інформації автентифікації й атаки типу «повтор» на одного перевірника;

Клас 4 – захищений від розкриття заявленої інформації автентифікації й атаки типу «повтор» на одного перевірника або різних перевірників.

Під час розгляду механізмів автентифікації й аналізу криптографічних протоколів усе вищезазначене робиться з точки зору пред’явника, і тому пред’явник завжди є ініціатором. На основі цього застосовують усі класи механізмів направленої автентифікації, а потім проводиться уточнення, де ініціатором є перевірник, оскільки вони застосовуються для однонаправленої та взаємної автентифікації [15].

Для забезпечення захисту у разі автентифікації джерела даних необхідно використовувати ЕЦП, або її деякий аналог засобом застосування асиметричного направленого шифрування. Може також застосовуватись симетричне шифрування, наприклад, у вигляді коду автентифікації повідомлення

(імітовставки), або криптографічного контрольного значення від даних, що виготовлені з використанням особистого ключа ЕЦП.

1.3.3 Фази автентифікації

Сутність фаз автентифікації. Процес автентифікації складається з таких фаз (рис. 1.6).

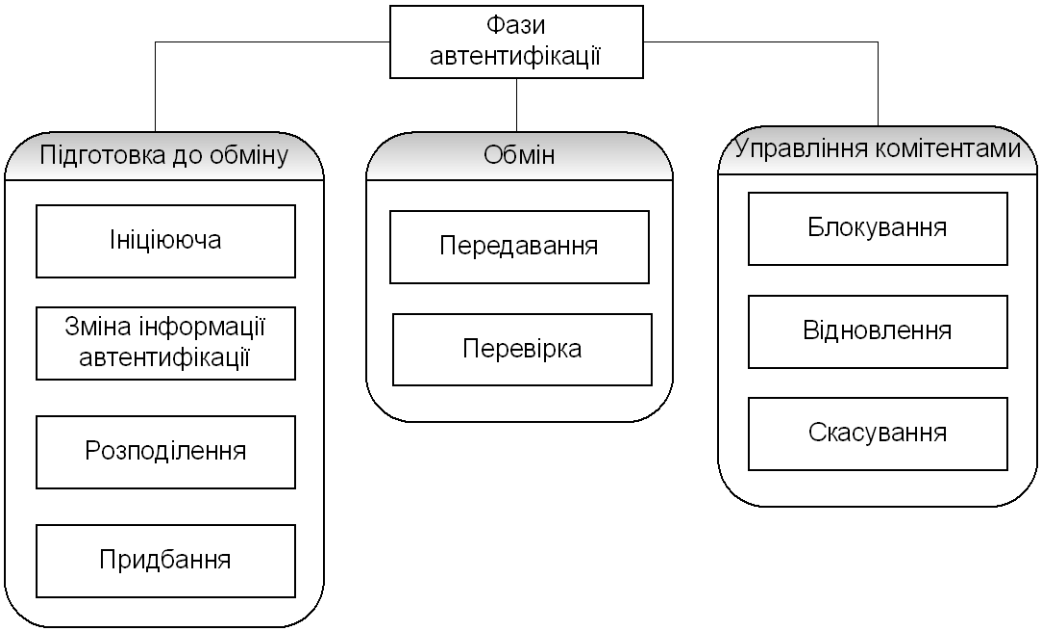


Рисунок 1.6 – Фази автентифікації

При цьому використання всіх фаз автентифікації окремо в часі є необов’язковим, воно може перекриватися (наприклад, виконуватися одночасно, а черговість фаз може залежати від механізму, що реалізується). На рис. 1.6 визначення фаз подано в такому розумінні.

1. Ініціююча фаза. На цій фазі має бути заявлена та перевірочна інформація автентифікації.

2. Змінна інформації автентифікації. Являє собою заявлену й перевірочну інформація автентифікації, яку комітент або менеджер подає для її зміни [16].

3. Розподілення. На цій фазі перевірочна інформація автентифікації об’єкта (наприклад, пред’явника або перевірника) розподіляється для використання при перевірці обмінної інформації автентифікації, наприклад, в автономному режимі

роботи об’єкти-користувачі ІВК можуть одержувати сертифікати автентифікації, списки відкликаних сертифікатів.

4. Перевірка. На цій фазі пред’явник або перевірник можуть одержувати інформацію, що необхідна для генерування обмінної інформації автентифікації для потреби автентифікації. Причому можуть реалізовуватись різні процедури перевірки обмінної інформації автентифікації, перш за все за рахунок взаємодії з третьою довірчою стороною або за рахунок обміну повідомленнями між сторонами, що здійснюють автентифікацію. Наприклад, при використанні центру розподілення ключів в інтерактивному режимі пред’явник або перевірник можуть одержувати від центру розподілення ключів для автентифікації з іншим об’єктом таку інформацію, як сертифікат автентифікації.

5. Передавання. Це фаза передавання обмінної інформації автентифікації між пред’явником і перевірником.

6. Перевіряння. На цій фазі обмінна інформація автентифікації перевіряється на відповідність перевірочній інформації автентифікації. На цій фазі об’єкт, який неспроможний перевірити обмінну інформацію автентифікації самостійно, може взаємодіяти з третьою довірчою стороною, що виконує перевірку обмінної інформації автентифікації. У цьому випадку третя довірча сторона буде повертати позитивну чи негативну відповідь.

7. Блокування. Це фаза встановлення тимчасового стану неможливості автентифікації для комітента, який раніше, можливо, був автентифікованим.

8. Відновлення – це припинення стану блокування комітента.

9. Скасування – це видалення комітента з переліку санкціонованих комітентів.

10. Залучення третьої довірчої сторони. Для здійснення автентифікації може залучатися або не залучатися третя довірча сторона. У зв’язку з цим розрізнюють такі типи автентифікації:

– автентифікація без залучення третьої довірчої сторони;
– автентифікація із залученням третьої довірчої сторони;
– автентифікація за допомогою посередника;
– інтерактивна автентифікація;
– автономна автентифікація;

– автентифікація, коли пред’явник довіряє перевірникові.

1.3.4 Основні положення надання послуг автентифікації

Загрози автентифікації. Основною задачею автентифікації є надання гарантій справжності ідентифікаційних даних комітента. Механізми автентифікації (рис. 1.7) повинні виключати можливість реалізації загроз типу «маскарад», «повтор», «підміна» та компрометацію заявленої інформації автентифікації (ІА). Загроза типу «маскарад» полягає в обмані одного об’єкта іншим об’єктом. Це означає, що один об’єкт особливим чином впливає на інший об’єкт, наприклад, використовуючи джерело даних або інші інформаційні взаємовідносини [17].

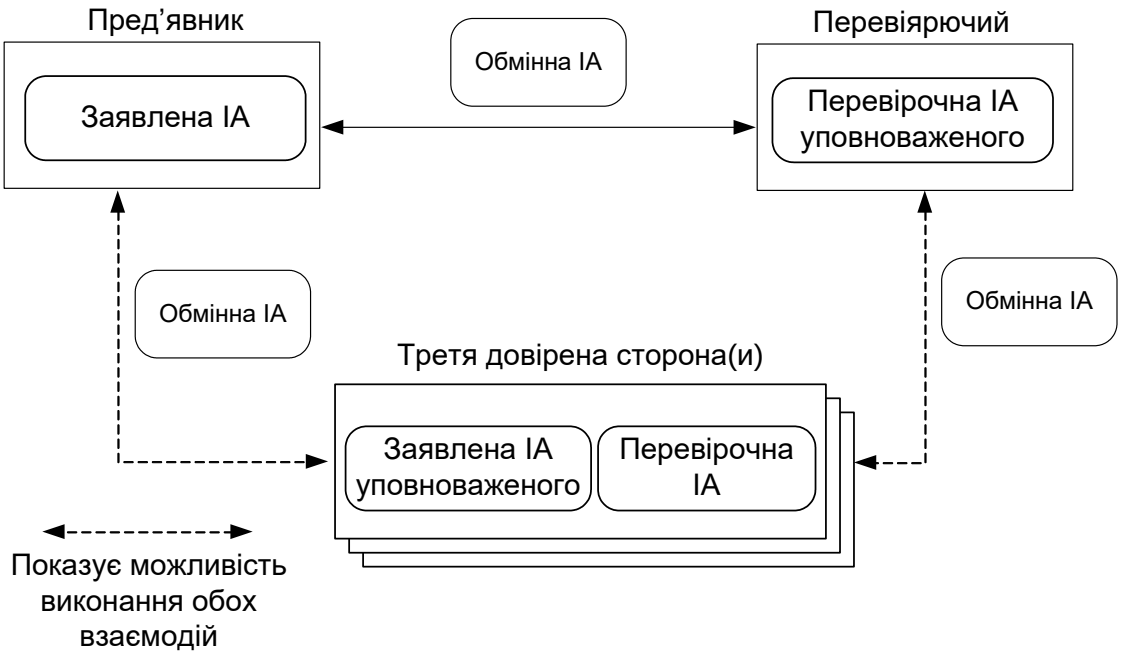


Рисунок 1.7 – Загальна модель використання інформації в процесі автентифікації

Загроза типу «маскарад» реалізується за умови активності джерела даних, комунікаційних взаємозв’язків тощо, що ініціюються або пред’явником, або перевірником. Для захисту проти загроз типу «маскарад» краще використовувати послугу надання цілісності з використанням для обміну при автентифікації відповідних елементів даних. Для протистояння загрозам, що

належать до такого типу, в процесі автентифікації мають використовуватися спеціальні дані, що пов'язані з деяким механізмом реалізації послуги цілісності, наприклад, ЕЦП чи кодом автентифікації, а також при шифруванні.

Загроза типу «повтор» полягає у повторі обмінної інформації автентифікації, що була передана раніше. Зазвичай її використовують у комбінації з іншими атаками, наприклад такими, як атака типу «модифікація». Не всі механізми автентифікації однаково протистоять атакам типу «повтор». Атака типу «повтор» може бути загрозою й для інших послуг безпеки, наприклад неспростовності й автентичності. Механізми автентифікації на основі ЕЦП можна використовувати для протистояння атакам типу «повтор», оскільки ЕЦП забезпечує послугу неспростовності пред'явника.

Загроза типу «підміна» також реалізується за умови активності джерела даних, комунікаційних взаємозв'язків тощо, що ініціюються або пред'явником, або перевірником. Вона зводиться або до підміни істинної обмінної інформації на хибну, або до модифікації істинної. Таку загрозу можна розглядати як один із підвидів загрози типу «маскарад». Для захисту проти загроз типу «підміна» краще використовувати послугу цілісності, наприклад з використанням для обміну при автентифікації ЕЦП чи коду автентифікації, а також шифрування

1.3.5 Протокол автентифікації Шнора

Одним із перших криптографічних протоколів автентифікації є протокол Шнора. Він є трьохетапним і може бути названим класичним. Реалізований з використанням криптоперетворень у скінченному полі Галуа. В якості загальних параметрів вибрані такі, що співпадають із загальними параметрами ЦП типу DSA. Протокол Шнора має ряд переваг і недоліків, останнє визначило необхідність його удосконалення під назвою протокол автентифікації на основі ЦП. Основною метою цього підрозділу є викладення сутності протоколів автентифікації Шнора, аналіз його властивостей та умов застосування. Подальше вдосконалення протоколу Шнора, на наш погляд, пов'язане з його

вдосконаленням засобом використання ЦП в групі точок еліптичних кривих тощо[19].

Протокол призначений для здійснення автентифікації одного з абонентів ІТС. Він розроблений на основі використання трьохетапного механізму автентифікації Шнора та окремих підходів механізму ЦП типу DSA, наприклад, генерування й використання загальносистемних параметрів тощо. Механізм призначений для автентифікації абонента – пред'явника відповідним абонентом – перевірником.

Попередньо кожен із абонентів має отримати відповідним чином цілісні й справжні загальні параметри $\{p, q, \Theta\}$.

Механізм і протокол автентифікації Шнора, що реалізується на його основі, складається з етапів налаштування загальних параметрів та генерування асиметричної пари ключів [18].

Генерування та розповсюдження загальних параметрів $\{p, q, \Theta\}$ має здійснюватись із забезпеченням їх цілісності, справжності й доступності, де p – велике просте число, q – просте число, що входить в канонічний розклад числа p–1, а θ – первісний (породжуючий) елемент підгрупи порядку q–1. Також загальні параметри $\{p, q, \theta\}$ мають задовольняти таким вимогам:

$$q/p-1;\ \theta \in Z_p;\ \theta^q \equiv 1(\mathrm{mod}\ p)$$

За вказаних вимог, оскільки q ділить p–1, тобто $q/p-1$, то q є підгрупою.

Генерування асиметричної пари довгострокових ключів (X,Y), зберігання особистого довгострокового ключа X із забезпеченням його конфіденційності, цілісності, справжності й доступності, а також забезпечення доступності відкритого ключа Y усіх абонентів, що з ним взаємодіють, із забезпеченням його

[19] Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.

цілісності й справжності, наприклад, способом виготовлення й використання відповідного йому сертифіката відкритого ключа. При цьому

$$X \in (1, q-1);\ Y \in (1, p-1)$$
$$Y = \Theta^X \pmod p.$$

Нехай суб'єкт А – ініціатор, тобто пред'явник, що хоче отримати доступ до інформації чи ресурсів абонента В та бути визнаним абонентом В як суб'єкт.

Протокол автентифікації Шнора за вказаних умов реалізується через виконання таких кроків[20].

1. Суб'єкт А виробляє особистий ключ сеансу $K_A \in (1, q-1)$ та обчислює відкритий ключ сенсу, скажімо r_A: $r_A = \Theta^{K_A} \pmod p$ та надсилає його абоненту В.

2. Суб'єкт В виробляє випадкове або псевдовипадкове число e – запит: $e = (1, 2^t - 1)$ та надсилає його суб'єкту А, де $t \geq 72$.

3. Суб'єкт А, одержавши e, обчислює, по суті, цифровий підпис, використовуючи для цього свої ключі: довгостроковий ключ X та ключ сеансу $K_A : S = (K_A + e \cdot X_A) \bmod q$ та надсилає його на третьому етапі суб'єкту В.

4. Суб'єкт В, отримавши значення S та вже знаючи Θ, Y та e обчислює значення r, яке за відсутності помилок має співпасти з r_A, що отримано суб'єктом В на першому етапі, тобто обчислюється $r = \Theta^S y^e \pmod p$, та перевіряється, чи $r_A = r$.

Якщо виконується, то з певною ймовірністю суб'єкт В автентифікує суб'єкта А. Таким чином, протокол автентифікації Шнора забезпечує автентифікацію суб'єкта А суб'єктом В. Щодо безпеки протоколу Шнора необхідно відмітити, що пасивна атака порушника (криптоаналітика) має зводитися до знаходження довгострокового ключа кожного із абонентів, наприклад X_A, та ключа сеансу, наприклад K_A. В обох випадках, згідно нинішніх

[20] A. Menezes, P.van Oorschot, S. Vanstone. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 с.

поглядів, необхідно вирішувати задачі дискретного логарифмування в скінченному полі Галуа [19].

Також необхідно відзначити, що протокол Шнора має ряд недоліків, основними з яких є такі:

1. при виконанні протоколу необхідно виконати три обміни інформацією (раунди) по принципу кожен з кожним;

2. достатньо складною є групова автентифікація, коли один суб'єкт здійснює автентифікацію з багатьма, і краще це зробити одночасно;

3. суб'єкту В необхідно формувати випадкове значення е та передавати його з певним забезпеченням цілісності та справжності тощо.

1.3.6 Протокол автентифікації Шнора на основі ЦП

Протокол автентифікації Шнора на основі ЦП є вдосконаленням протоколу Шнора, що розглянутий у попередньому. Вдосконалення спрямоване на те, щоб здійснювати автентифікацію за один прохід (раунд), отримавши можливість здійснення групової автентифікації, а також іншим чином генерувати випадковий запит *e*. Шнор запропонував генерувати запит на основі використання в якості *e* значення функції гешування від певного повідомлення *m*. Вказане дозволило реалізувати криптографічний протокол за один прохід, в тому числі з груповою автентифікацією.

Генерування й розповсюдження загальних параметрів $\{p, q, \Theta\}$ має здійснюватись аналогічно, як і в протоколі Шнора[21].

Генерувавання асиметричної пари довгострокових ключів (X,Y), має також здійснюватись аналогічно, як і в протоколі Шнора.

Протокол автентифікації Шнора на основі ЦП за вказаних вище умов реалізується через виконання таких кроків.

---

[21] Усовершенствование протокола нулевых знаний, основанного на дискретных логарифмах / И.В. Олешко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – с. 363–372.

1. Для забезпечення стійкості суб'єкти А та В повинні генерувати випадкове е, яке має співпадати. Ця задача розв'язана за рахунок використання функції гешування, тобто обчислення $h = H(m, \Pr)$.

2. Суб'єкт А генерує особистий ключ $K_A \in (1, q-1)$ та обчислює відкритий ключ: $r_A = \Theta^{K_A} (\bmod p)$;

3. Суб'єкт А генерує запит $e = h(r_A, m)$ де т – повідомлення (інформація), що підписується.

4. Суб'єкт А генерує значення підпису S у вигляді $S = (K_A + eX_A) \bmod q$

Необхідно підкреслити особливості протоколу:

– значення запиту е змінюється для одного й того самого т;

– сам підпис є сеансовим (залежить від X_A та ключа сеансу K_A).

Суб'єкт В, отримавши значення S та вже знаючи Θ, Y та е, обчислює значення r', яке за відсутності помилок також має співпасти з r_A, що отримане суб'єктом В на першому етапі, тобто обчислюється $r' = \Theta^S Y^e (\bmod p)$та перевіряється, чи r' = r, причому $e \overset{?}{=} h(r', m')$

При оцінці безпеки протоколу Шнора на основі ЕЦП необхідно відзначити, що пасивна атака порушника (криптоаналітика) має зводитися до знаходження довгострокового ключа кожного з абонентів X_A та ключа сеансу K_A. Як у першому, так і в другому випадках необхідно розв'язувати задачі дискретного логарифмування в скінченному полі Галуа [20].

На відміну від трьохетапного протоколу Шнора, протокол Шнора на основі ЦП має такі переваги:

– для виконання протоколу необхідно виконати тільки один обмін (раунд) (S, r) від А до В;

– можлива також групова автентифікація А з групою суб'єктів з одночасною перевіркою цілісності повідомлення *m*.

– Проблемними для протоколу Шнора на основі ЦП є такі питання:

– при помилках в *m* з великою ймовірністю також буде помилковим;

– якщо m' викривлене, h буде відрізнятись та e не обчислюється.

– забезпечення неспростовності тільки суб'єкта А.

Основним же недоліком, з точки зору обох протоколів Шнора, є те, що він побудований на основі криптографічного перетворення в скінченному полі Галуа. Для цього випадку складність атаки типу «повне розкриття» має субекспоненційний характер. У той же час його можна вдосконалити, скориставшись перетворенням у групі точок еліптичної кривої, в такому разі складність атаки «повне розкриття» вже буде носити субекспоненційний характер.

1.3.7 Криптографічні протоколи автентифікації на основі симетричних криптографічних перетворень

У цьому підрозділі вводиться модель автентифікації, що ґрунтується на симетричних криптографічних перетвореннях, розглядаються обмеження щодо неї, викладається сутність і даються оцінки протоколам, що ґрунтуються на однобічній та взаємній автентифікації, включаючи протоколи автентифікації, що потребують залучення третьої довірчої сторони. Викладення матеріалу та оцінки здійснюються з орієнтацією на міжнародні стандарти ДСТУ ISO/IEC 9798-1, 2[22].

1.3.8 Модель автентифікації

Загальну модель для механізмів автентифікації наведено на рис. 8. Згідно цієї моделі не висувається вимога, щоб усі види об'єктів та обмінів були задіяні в кожному механізмі автентифікації. Для механізмів автентифікації для однобічної автентифікації об'єкт A виступає як пред'явник, а об'єкт B як перевірник. Для взаємної автентифікації об'єкти A та B виступають одночасно у ролі як пред'явника, так і перевірника.

---

[22] ДСТУ ISO/IEC 9798-1.[Electronic resource]. - URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66917

З метою автентифікації об’єкти формують та обмінюються стандартизованими повідомленнями, що мають назву маркерів. Для здійснення однобічної автентифікації потрібен обмін щонайменше одним маркером, для здійснення взаємної автентифікації – щонайменше двома маркерами. Якщо автентифікація розпочинається за запитом, то для цього необхідно здійснювати додатковий обмін. Також може виникати потреба у додатковому обміні, якщо автентифікація здійснюється із залученням третьої довірчої сторони (ТДС).

На рис. 1.8, лініями позначено потенційно можливі потоки інформації. Об’єкти *A* та *B* можуть взаємодіяти безпосередньо як один з одним, так і з третьою довірчою стороною. Вони можуть взаємодіяти з третьою довірчою стороною як через *B* так і через *A* відповідно, а також використовувати при автентифікації деяку інформацію, що випущена третьою довірчою стороною.

Загальні вимоги та обмеження. Кожен об’єкт, здійснюючи автентифікацію іншого об’єкта, має використовувати однаковий набір криптографічних перетворень і параметрів.

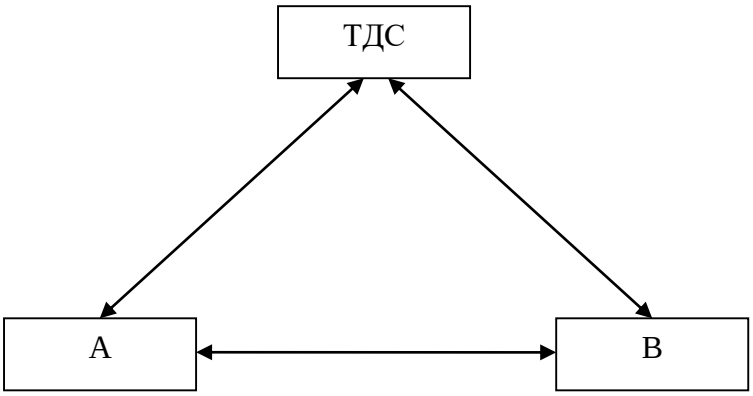


Рисунок 1.8 – Модель автентифікації

Протягом строку дії ключових даних, значення всіх змінних у часі параметрів (відміток часу, порядкових номерів, випадкових чисел тощо) не можуть повторюватися, принаймні ймовірність повтору має бути завідомо дуже малою.

Вважається, що після виконання механізмів автентифікації об’єкти A та B визнають, що інший об’єкт є тим, за кого він себе видає. Це може бути забезпечене включенням в інформаційний обмін між двома об’єктами їхніх ідентифікаторів, або контекстом використання механізму.

Сутність однобічної автентифікації полягає в тому, що автентичність перевіряється з використанням механізму автентифікації тільки для одного з двох об’єктів.

1.3.9 Однобічна автентифікації з одним проходом

У цьому протоколі автентифікації пред’явник A ініціює процес, а суб’єкт B що взаємодіє з А, перевіряючи його автентичність. Маркер зашифровується за допомогою симетричного криптоперетворення на ключі K_{AB}. Унікальність та/або своєчасність забезпечується шляхом генерації та перевіряння позначки часу й порядкового номера. Протокол автентифікації представлено на рис. 1.9.

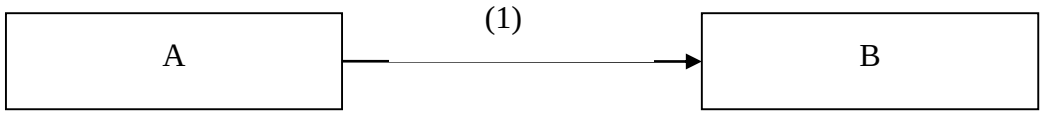


Рисунок 1.9 – Протокол автентифікації

Маркер ($TokenAB$), що відсилається пред’явником A перевірникові B, має таку структуру:

$$TokenAB = Text2 \,||\, eK_{AB}\begin{pmatrix} T_A \\ N_A \end{pmatrix} \,||\, B \,||\, Text1 \Bigg).$$

У маркері пред’явник A в якості змінного в часі параметра використовує або порядковий номер N_A або позначку часу T_A. Вибір параметра залежить від технічних можливостей пред’явника і запитувача, а також від оточення.

Включення розпізнавального ідентифікатора B до маркера $TokenAB$ є необов'язковим[23].

Протокол здійснюється таким чином.

1. Об'єкт A генерує та відсилає $TokenAB$ об'єкту B в зашифрованому вигляді.

2. Об'єкт B розшифровує і потім перевіряє коректність розпізнавального ідентифікатора B, якщо він є, а також позначку часу або порядковий номер.

1.3.10 Однобічна автентифікація з двома проходами

Об'єкт B ініціює протокол автентифікації та перевіряє автентичність пред'явника A. Унікальність та/або своєчасність забезпечуються шляхом генерації та перевірки випадкового числа R_B. Протокол однобічної автентифікації з двома проходами подано на рис. 1.10.

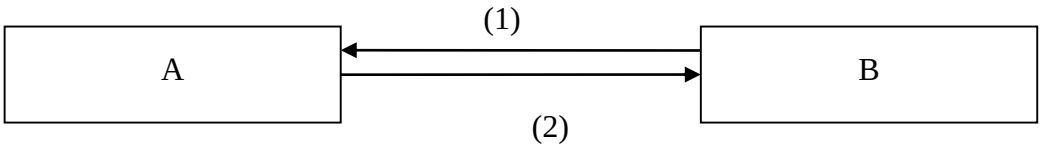


Рисунок 1.10 – Однобічна автентифікація з двома проходами

Маркер ($TokenAB$) зашифровується за допомогою симетричного криптоперетворення на ключі K_{AB}, відсилається пред'явником A об'єкту B і має таку структуру:

$$TokenAB = Text3 \| eK_{AB}\left(R_B \| B \| Text2\right)$$

Включення розпізнавального ідентифікатора B до маркера $TokenAB$ є необов'язковим.

Протокол здійснюється таким чином.

[23] Молдовян А.А., Молдовян Д.Н., Левина А.Б. Протоколы аутентификации с нулевым разглашением секрета.– СПб: Университет ИТМО, 2016. – 55 с

1. Об’єкт B генерує випадкове число R_B та відсилає його об’єкту A (об’єкту A може бути надіслано також текстове поле *Text*1).

2. Об’єкт A формує та відсилає об’єкту B маркер $TokenAB$.

3. Об’єкт B, отримавши повідомлення, що містить маркер $TokenAB$, перевіряє цей маркер шляхом розшифрування його зашифрованої частини і потім перевіряє коректність розпізнавального ідентифікатора B, якщо він є. Перевіряється також відповідність випадкового числа R_B, що було надіслано об’єкту A на кроці (1), випадковому числу, що міститься в одержаному маркері $TokenAB$[24].

З метою запобігання атакам при відомому відкритому тексті, коли криптоаналітик знає відкриті тексти для декількох зашифрованих повідомлень, об’єкт *A* може включати в поле *Text2* випадкове число.

Розпізнавальний ідентифікатор B включається в маркер $TokenAB$ для запобігання атакам типу віддзеркалення. Така атака характеризується тим, що порушник з метою видачі себе за об’єкт A віддзеркалює запит R_B об’єкта *B* [19].

1.3.11 Взаємна автентифікація

Взаємна автентифікація означає, що з використанням протоколу автентифікації обидва об’єкти перевіряють автентичність один одного.

Взаємна автентифікація з двома проходами.

Протокол автентифікації наведено на рис. 1.11. У ньому унікальність та/або своєчасність забезпечуються шляхом генерації та перевіряння позначки часу й порядкового номера. Інформація маркера зашифровується за допомогою симетричного криптоперетворення на ключі K_{AB}.

---

[24] Баришев Ю. В. Моделі псевдонедетермінованованих криптографічних перетворень / Ю. В. Баришев // Матеріали статей П’ятої Міжнародної науково-практичної конференції" Інформаційні технології та комп’ютерна інженерія", м. Івано-Франківськ, 27-29 травня 2015 р.: 189-190

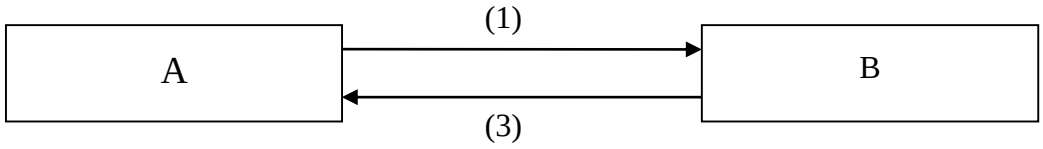


Рисунок 1.11 – Взаємна автентифікація з двома проходами

Структура маркера ($TokenAB$), що відсилається об'єктом A об'єктові B, ідентична структурі маркера, тобто

$$TokenAB = Text2 \,||\, eK_{AB}\begin{pmatrix} T_A \\ N_A \end{pmatrix} \,||\, B \,||\, Text1\Bigg)$$

Структура маркера ($TokenBA$), що відсилається об'єктом B об'єкту A, має таку структуру:

$$TokenBA = Text4 \,||\, eK_{AB}\begin{pmatrix} T_B \\ N_B \end{pmatrix} \,||\, A \,||\, Text3\Bigg)$$

Включення розпізнавального ідентифікатора B до маркера $TokenAB$ та розпізнавального ідентифікатора A до маркера $TokenBA$ є необов'язковим. Розпізнавальний ідентифікатор B включається в маркер $TokenAB$ для запобігання повторного використання маркера $TokenAB$ порушником з метою здійснення «маскараду», видаючи себе за об'єкт B. З аналогічною метою здійснюється включення розпізнавального ідентифікатора A в маркер $TokenBA$. Їх включення не є обов'язковим, тому в оточенні, де такі атаки виключені, один чи обидва розпізнавальні ідентифікатори можна не використовувати.

Використання позначки часу або порядкового номера залежить від технічних можливостей пред'явника та запитувача, а також від стану оточення.

Протокол взаємної автентифікації виконується в такому порядку.

1. Суб'єкт A генерує та відсилає об'єкту B $TokenAB$ у зашифрованому вигляді за допомогою симетричного криптоперетворення на ключі K_{AB}.

2. Суб'єкт B перевіряє $TokenAB$ шляхом розшифрування зашифрованої частини і потім перевіряє коректність розпізнавального ідентифікатора B, якщо він є, а також позначку часу або порядковий номер.

3. Суб'єкт B генерує та відсилає $TokenBA$ суб'єкту A.

4. Суб'єкт A розшифровує $TokenBA$ та перевіряє коректність розпізнавального ідентифікатора A, якщо він є, а також позначку часу або порядковий номер.

Необхідно відмітити, що обидва повідомлення в цьому протоколі пов'язані між собою лише вимогою відносної своєчасності.

Взаємна автентифікація з трьома проходами.

Протокол автентифікації подано на рис. 1.12 У цьому протоколі автентифікації унікальність та/або своєчасність забезпечуються шляхом генерації, передачі в запиті та перевіряння випадкового числа R_B. Інформація маркерів зашифровується за допомогою симетричного криптоперетворення на ключі K_{AB}.

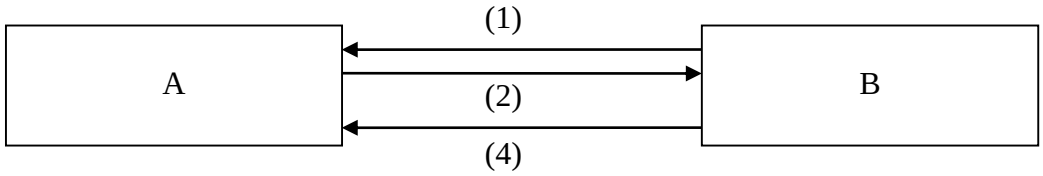


Рисунок 1.12 – Взаємна автентифікація з трьома проходами

Маркери обміну в раундах мають таку структуру:

$$TokenAB = Text3 \| eK_{AB}\left(R_A \| R_B \| B \| Text2\right),$$

$$TokenBA = Text5 \| eK_{AB}\left(R_B \| R_A \| Text4\right)$$

Протокол автентифікації здійснюється таким чином.

1. Об'єкт B генерує випадкове число R_B та відсилає його об'єкту A (а також за необхідності об'єкту A може бути надіслано $Text1$).

2. Об'єкт A генерує випадкове число R_A, формує та відсилає маркер $TokenAB$ об'єкту B.

3. Об'єкт B, отримавши повідомлення, що містить маркер $TokenAB$, перевіряє цей маркер шляхом його розшифрування і потім перевіряє:

– коректність розпізнавального ідентифікатора B, якщо він є;

– відповідність випадкового числа R_B, що було надіслане об'єкту A на першому кроці, та випадкового числа, що міститься в маркері $TokenAB$.

4. Об'єкт B генерує та відсилає маркер $TokenBA$ об'єкту A.

5. Об'єкт A, отримавши повідомлення, що містить маркер $TokenBA$, перевіряє цей маркер шляхом розшифрування його зашифрованої частини і потім перевіряє:

– коректність розпізнавального ідентифікатора A, якщо він є;

– відповідність випадкового числа R_B, що було надіслане об'єктом B на кроці (1), випадковому числу, що міститься в маркері $TokenBA$;

– відповідність випадкового числа R_A, що було відправлено об'єкту B на кроці (2), випадковому числу, що міститься в маркері $TokenBA$.

Розпізнавальний ідентифікатор B включається в маркер $TokenAB$ для запобігання атакам типу віддзеркалення. Така атака характеризується тим, що порушник з метою видачі себе за об'єкт A віддзеркалює запит R_B об'єкту B.

1.3.12 Аналіз криптопротоколів встановлення ключів (узгодження ключів)

Визначимо, що необхідно для встановлення таємниці. Встановлення таємниці може включати такі криптографічні механізми:

– узгодження таємниці (ключа);

– вироблення ключа;

– підтвердження ключа;

– передавання або транспортування ключа.

Узгодження розподіленої таємниці (ключа) – це таке обчислення таємниці (ключа) двома або більше суб'єктами, коли кожен з них не в змозі попередньо обчислити таємний ключ окремо (один) із заданою ймовірністю.

При виконанні криптографічних протоколів у групі точок еліптичних кривих необхідно:

– виконати узгодження спільної інформації та параметрів;

– провести налаштування загальних параметрів;

– встановити параметри кофакторного множення;

– здійснити генерацію асиметричних пар ключів.

Нехай до криптографічного протоколу встановлення ключа висуваються такі вимоги:

– має забезпечуватись взаємна автентифікація об’єктів А та В;

– встановлення ключа має здійснюватись у два етапи – спочатку встановлюється спільна таємниця, а на основі спільної таємниці – спільний ключ;

– у процесі встановлення ключа жодна інформація не повинна передаватись по відкритому каналу;

– в якості третьої довірчої сторони може виступати акредитований центр сертифікації ключів.

Генерування асиметричних пар ключів. Будемо вважати, що застосовується довільне асиметричне криптографічне перетворення. Особистими ключами є випадкові або псевдовипадкові послідовності, наприклад d_A та d_B. Відкритими ключами відповідно є P_A та P_B, тобто асиметричними парами ключів є такі (d_A, P_A) та (d_B, P_B). Далі, з відкритих ключів третя довірча сторона виготовляє сертифікати відкритих ключів P_A та P_B, а особисті ключі мають застосовуватись як конфіденційні з виконанням вимог.

1.3.13 Протокол з нульовим проходом і кофакторним множенням

Спільна інформація. Для всіх механізмів узгодження ключів перед процесом узгодження таємниці, що розділюється, між сторонами необхідно установити та, за необхідності, перевірити таку спільну інформацію.

Параметри еліптичної кривої, з якими мають бути пов’язані ключові пари та які мають бути однаковими для ключових пар обох сторін, наприклад, модулі

p, p^m або 2^m, опис полів $F(p), F(p^m)$ або $F(2^m)$, та зазначення базису, що використовується, кривої E , порядку базової точки n та базової точки G.

У кожному із механізмів, що наведені нижче, результуючий узгоджений ключ не повинен використовуватись безпосередньо як криптографічний. Замість цього, він має використовуватись як вхідні дані для функції вироблення ключа, дозволяючи обом сторонам виробляти з нього однакові криптографічні ключі. Тому, для двох сторін необхідно узгодити ще таку інформацію:

– функцію вироблення ключа, *kdf*;

– будь-які параметри для функції вироблення ключа;

– тип кофакторного множення, яке необхідно виконувати (за необхідності).

Налаштування. Перед процесом узгодження таємниці, що розділюється, додатково до спільної інформації необхідно:

– для кожного об’єкта X установити особистий ключ для узгодження ключів d_X та відкритий ключ для узгодження ключів P_X, який є точкою еліптичної кривої, що задовольняє рівнянню $P_X = d_X G$;

– для кожного об’єкта забезпечити доступ до автентичної копії відкритого ключа для узгодження ключів іншої сторони.

Кожен об’єкт має незалежно перевірити, що відкритий ключ іншого об’єкта дійсно є точкою еліптичної кривої.

Формування спільної таємниці (A).

Об’єкт A обчислює спільну таємницю, використовуючи свій особистий ключ для узгодження ключів d_A та відкритий ключ для узгодження ключів P_B об’єкта B таким чином: $K_{AB} = (d_A \cdot l)(hP_B)$, де l та h – параметри кофакторного множення.

Формування ключа (B).

Об’єкт B обчислює спільну таємницю, використовуючи свій особистий ключ для узгодження ключів d_B та відкритий ключ для узгодження ключів P_A об’єкта A таким чином: $K_{BA} = (d_B \cdot l)(hP_A)$.

Спільний ключ генерується на основі застосування функції *kdf*, тобто K_c = kdf(K_{AB}) = kdf(K_{BA})

Властивості. Цей механізм узгодження спільної таємниці має такі властивості:

– таємниця K_{AB} співпадає з таємницею K_{BA};

– число раундів передачі (проходів) – 0;

– механізм забезпечує взаємну неявну автентифікацію ключа.

Для виконання протоколу кожен суб'єкт повинен мати доступ до сертифіката суб'єкта, з яким узгоджується ключ. Це забезпечується або безпосереднім зберіганням сертифікату у суб'єкта-ініціатора та суб'єкта-відповідача, або має бути забезпечений доступ до сховища сертифікатів.

Кількість проходів. Протокол є неінтерактивним і не вимагає при узгодженні спільної таємниці жодної передачі повідомлення (раунду) від одного суб'єкта до іншого. При цьому зловмисник не має ніякої інформації щодо факту здійснення протоколу [20].

Кількість ключових пар і ключів сертифікатів. Перед виконанням протоколу кожен суб'єкт повинен згенерувати або відповідним чином одержати особистий таємний ключ d_x та відкритий Q_x. Відкритий ключ має бути сертифікований, відносно нього мають бути забезпечені цілісність і справжність на всіх етапах його життєвого циклу. Особистий ключ має зберігатись у його власника, щодо нього мають бути забезпечені конфіденційність, цілісність і справжність. Суб'єкт-ініціатор і суб'єкт-відповідач повинні мати доступ до сертифіката суб'єкта, з яким узгоджується ключ. Таким чином, при виконанні протоколу узгодження ключів використовуються 2 пари ключів, позначимо їх (d_i, Q_i) та (d_j, Q_j).

Додаткова інформація. Аналіз цього протоколу показав, що він забезпечує узгоджене вироблення й узгодження тільки таємниці $K_{AB} = K_{BA}$, що розділюється. Тобто цим протоколом не передбачено вироблення та узгодження спільного таємного ключа симетричного шифрування.

Ступінь захищеності протоколу від атак. З боку зловмисника на протокол можуть бути здійснені пасивні й активні атаки. Під пасивними атаками будемо розуміти атаки, що пов’язані з виконанням криптоаналізу, але при цьому зловмисник не втручається безпосередньо у виконання протоколу (раунди обміну інформацією). Під активною атакою будемо розуміти атаки, під час яких зловмисник втручається в сам протокол узгодження спільної таємниці, порушуючи тією чи іншою мірою конфіденційність, цілісність і справжність спільної таємниці чи ключа.

Захищеність протоколу від пасивних атак. При здійсненні цієї атаки зловмисник (криптоаналітик) робить спробу перехопити повідомлення, що передаються при виконанні протоколу між суб’єктами, що узгоджують спільний ключ. Але в протоколі, що аналізується, ніяка інформація узгодження ключів не передається. Тому атака може здійснюватись на ключові пари (d_i, Q_i) і базу сертифікатів $\{Q\}$. Будемо вважати, що відносно ключа d_i забезпечується конфіденційність, цілісність і справжність. Доступними криптоаналітику є тільки сертифікати Q_i.

1.3.14 Аналіз інтерактивного механізму узгодження спільної таємниці типу Ель-Гамаля

Механізм забезпечує встановлення спільної таємниці між двома суб’єктами і ґрунтується на одноразовій передачі маркера ключа (ключа сеансу) між суб’єктами А та В. Механізм узгодження ключів установлює розділювану таємницю між двома об’єктами А та В, за один прохід.

Налаштування. Перед процесом узгодження таємниці, що розділюється, додатково до спільної інформації необхідно:

– об’єкту В установити особистий ключ для узгодження ключів d_B та відкритий ключ для узгодження ключів P_B, який є точкою еліптичної кривої, що задовольняє рівнянню $P_B = d_B G$;

– об’єкту А забезпечити доступ до автентичної копії відкритого ключа для узгодження ключів об’єкта В.

Також об’єкт А має перевірити, що відкритий ключ об’єкта В дійсно є точкою еліптичної кривої.

Механізм встановлення:

Формування маркера ключа (А)

Об’єкт А випадково генерує таємне значення *r*, що належить діапазону $\{1,...,n-1\}$, обчислює rG, формує маркер ключа (відкритий ключ сеансу) $KT_{A1} = rG$ та надсилає його об’єкту В.

Формування спільної таємниці (А)

Об’єкт А обчислює спільну таємницю: $K_{AB} = (r \cdot l)(hP_B)$.

Формування спільної таємниці (В)

Об’єкт В має перевірити, що КТА1 дійсно є точкою еліптичної кривої, використовуючи свій особистий ключ і маркер КТА1. Спільна таємниця обчислюється таким чином: $K_{AB} = (d_B \cdot l)(h\ KT_{A1})$.

Цей механізм узгодження ключів має такі властивості:

– число проходів – 1;

– механізм забезпечує неявну автентифікацію ключа об’єктом А об’єкта В, оскільки об’єкт В є єдиним об’єктом, що відрізняється від об’єкта А, який може обчислити розділювану таємницю;

– механізм забезпечує криптоживучість ключа об’єкта А.

Об’єм попередньо необхідної інформації. Якщо не враховувати інформацію, якою володіє кожна із сторін протоколу, то цей механізм (протокол на його основі) вимагає зберігання одним із суб’єктів сертифіката (відкритого ключа) іншої сторони. Але навіть цей ключ необов’язково зберігати в тому випадку, коли ключ може бути одержаний як сертифікат із бази сертифікатів.

Кількість проходів. Алгоритм вимагає виконання однієї передачі (раунду) при встановленні спільної таємниці. Тому криптоаналітик може визначити факт

встановлення спільної таємниці та перехопити відкритий ключ сеансу ініціатора протоколу.

Кількість ключів (ключових пар). Для виконання протоколу необхідно, щоб один із суб'єктів володів своїм таємним ключем, тобто заздалегідь генерованою парою особистий/відкритий ключ (d_i, Q_i), інша сторона, що є ініціатором, також повинна володіти парою ключів, але вони мають бути генеровані вже під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму дорівнює двом: одна довгострокова та одна пара сеансу.

Протокол не потребує узгодження додаткової інформації – як таємної, так і відкритої, у зв'язку з тим, що для цього протоколу стандартом не передбачене вироблення спільного ключа симетричного шифрування, а тільки спільної таємниці.

Пасивна атака. При здійсненні атаки криптоаналітик буде намагатися перехопити всі повідомлення, що передаються між суб'єктами, які узгоджують ключ. При використанні інтерактивного протоколу узгодження ключів типу Ель-Гамаля між сторонами здійснюється один раунд передачі даних: суб'єкт-ініціатор передає іншому суб'єкту свій відкритий ключ сеансу. Ще одна передача може здійснюватись під час попередньої підготовки (передача довгострокового відкритого ключа суб'єкта-відповідача суб'єктові-ініціатору). Криптоаналітик теоретично може перехопити обидва відкриті ключі. Для розкриття будь-якої інформації (значення спільної таємниці, значення особистого довгострокового ключа чи значення особистого ключа сеансу) зловмисник має встановити за відомим відкритим ключем і базовою точкою особистий ключ, тобто розв'язати задачу пошуку дискретного логарифма на еліптичній кривій. Ця задача детально розглядається в розділі 4. При цьому визначення особистого ключа з пари ключів суб'єкта-ініціатора не призведе до реалізації атаки типу «повне розкриття», оскільки визначений зловмисником, цей особистий ключ є ключем сеансу і більше не буде використовуватись у системі.

Активна атака. Ця атака вимагає взаємодії між суб’єктами під час узгодження ключів. У протоколі здійснюється єдиний раунд взаємодії між учасниками протоколу – передача відкритого о ключа сеансу суб’єкта-ініціатора суб’єкту-відповідачу. При виконанні атаки зловмисник може використовувати два сценарії. Вибір сценарію залежить від мети, якої прагне досягти зловмисник. Можливі два варіанти:

– завадити суб’єктам, які взаємодіють, виробити ключ. В такому разі зловмисник може перехоплювати й модифікувати повідомлення, ключ сеансу, які ініціатор передає відповідачеві. Суб’єкти не зможуть виробити однакову спільну таємницю;

– сформувати спільну таємницю із суб’єктом-відповідачем. В такому разі зловмисник може видати себе за суб’єкта-ініціатора, оскільки протокол не вимагає попередньої автентифікації суб’єкта-ініціатора і не підтримує її під час виконання протоколу. Зловмисник формує свою пару ключів, використовуючи загальновідомі параметри еліптичної кривої і базову точку, та відсилає свій відкритий ключ відповідачеві. Той перевіряє належність точки еліптичній кривій (точка буде належати еліптичній кривій, тому що зловмисник використовує вірні параметри та алгоритми) і формує з ним спільний ключ.

Методи захисту від цієї атаки – додаткова автентифікація ініціатора та забезпечення цілісності й справжності відкритого маркера ключа. Атака типу «об´єкт посередині» в такому протоколі неможлива, оскільки зловмисник не в змозі підмінити відкритий ключ відповідача.

Загальний рівень безпеки щодо визначення спільної таємниці. Безпека спільної таємниці повністю базується на складності розв’язання дискретного логарифмічного рівняння в групі точок еліптичної кривої. При цьому вважається, що зловмисник не може видати себе за ініціатора протоколу. У разі активної атаки, коли зловмисник може видати себе за ініціатора протоколу, він може сформувати спільну таємницю і нав’язати її суб’єкту-відповідачу.

Інтерактивний протокол узгодження спільної таємниці типу Ель-Гамаля може бути використаний за умови, що суб’єкт-ініціатор не може бути

зловмисником. В іншому разі він, володіючи загальними параметрами, може видати себе за ініціатора протоколу і нав'язати суб'єкту-відповідачу спільну таємницю. Це пов'язане з тим, що протокол не забезпечує автентифікацію суб'єкта-ініціатора. При використанні протоколу необхідно враховувати, що він не забезпечує криптоживучість суб'єкта-відповідача. Таким чином, протокол забезпечує тільки неявну автентифікацію суб'єкта-відповідача та криптоживучість суб'єкта-ініціатора.

1.3.15 Аналіз інтерактивного двопрохідного протоколу узгодження спільної таємниці типу Діффі-Геллмана

Протокол призначений для вироблення спільної таємниці на основі формування й обміну відкритими ключами. Механізм забезпечує узгодження таємниці між об'єктами А та В за два проходи.

Налаштування. Цей механізм узгодження ключів не потребує встановлення будь-якої вхідної інформації, яка відрізняється від спільної інформації.

Формування маркера ключа (А)

Об'єкт А випадково генерує таємне значення r_A, що перебуває в діапазоні $\{1,..., n-1\}$, обчислює $r_A G$, формує маркер ключа: $KT_{A1} = r_A G$ та надсилає його об'єкту В.

Формування маркера ключа (В)

Об'єкт В випадково генерує таємне значення r_B, що перебуває в діапазоні $\{1,..., n-1\}$, обчислює $r_B G$, формує маркер ключа: $KT_{B1} = r_B G$ та надсилає його об'єкту А.

Формування спільної таємниці (А)

Об'єкт А має перевірити, що маркер KT_{B1} дійсно є точкою еліптичної кривої. Об'єкт А обчислює спільну таємницю як $K_{AB} = (r_A \cdot l)(hKT_{B1})$

Формування спільної таємниці (В)

Об’єкт В має перевірити, що маркер KT_{A1} дійсно є точкою еліптичної кривої. Об’єкт В обчислює спільну таємницю як $K_{AB} = (r_B \cdot l)(hKT_{A1})$

Цей механізм узгодження ключів має такі властивості:

– число проходів – 2;

– механізм забезпечує взаємну криптоживучість ключів.

Обсяг та вид попередньо одержаної інформації. Попередньо необхідно одержати загальні параметри криптографічних перетворень у групі точок ЕК.

Кількість проходів. При встановленні спільного ключа алгоритм вимагає виконання двох проходів. Тому криптоаналітик може визначити факт встановлення спільного ключа і перехопити відкриті ключі сеансу ініціатора та відповідача протоколу.

Кількість ключів (ключових пар). Для виконання протоколу необхідно, щоб обидва суб’єкти мали по одній парі особистий/відкритий сеансів ключ, що мають бути генеровані під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму, дорівнює двом.

Пасивна атака. Під час цієї атаки криптоаналітик намагається перехопити всі повідомлення, що передаються між суб’єктами, які узгоджують спільну таємницю. При використанні інтерактивного протоколу узгодження ключів типу Диффі-Гелмана між сторонами відбуваються два раунди передачі даних – суб’єкт-ініціатор і суб’єкт-відповідач передають один одному свої відкриті ключі. Криптоаналітик теоретично може перехопити обидві пари ключів. Для розкриття будь-якої інформації (значення спільної таємниці, значення особистих ключів сеансу) зловмисник має встановити за відомими відкритими ключами й базовою точкою особистий ключ, тобто розв’язати задачу пошуку дискретного логарифма в групі точок ЕК. Але визначення особистих ключів сеансових пар суб’єктів не призведе до реалізації атаки типу «повне розкриття», оскільки визначений зловмисником особистий ключ більше не буде використовуватись у системі і на основі отриманого ключа можна встановити тільки ключ сеансу,

який вже відбувся, і виконати розкриття тільки тієї інформації, що передана на цьому ключі.

Активна атака. Ця атака вимагає взаємодії між суб'єктами під час узгодження ключів. У протоколі виконується два раунди взаємодії між учасниками протоколу – передача відкритого ключа сеансу суб'єктом-ініціатором суб'єкту-відповідачу та навпаки. Для виконання атаки зловмисник може використовувати три сценарії. Вибір сценарію залежить від мети, якої прагне досягти зловмисник. Можливі три варіанти:

– завадити суб'єктам, які взаємодіють, виробити ключ. У такому випадку зловмисник може перехоплювати та модифікувати повідомлення. Суб'єкти не зможуть виробити однакову спільну таємницю;

– сформувати спільну таємницю з одним з суб'єктів. У такому випадку зловмисник може видати себе за суб'єкт-ініціатор чи суб'єкт-відповідач, тому що протокол не вимагає попередньої автентифікації суб'єктів та не підтримує її під час виконання протоколу;

– зловмисник формує свою пару ключів, використовуючи загальновідомі параметри еліптичної кривої та базову точку. Зловмисник відсилає свій відкритий ключ, друга сторона перевіряє належність точки до еліптичної кривої (точка буде належати еліптичній кривій, тому що зловмисник використовує вірні параметри й алгоритми) та формує з ним спільний ключ.

Методи захисту від цієї атаки – додаткова автентифікація ініціатора та забезпечення цілісності та справжності відкритого маркера ключа;

Атака типу «об'єкт посередині» також можлива в цьому протоколі. Атака може бути здійснена таким чином. Зловмисник перехоплює повідомлення, які передаються між ініціатором і відповідачем. На початку виконання протоколу зловмисник перехоплює відкритий ключ, що йде від ініціатора до відповідача, залишає його у себе, а відповідачу відсилає свій відкритий ключ (тільки-но сформований). Відповідач формує свою пару ключів і відсилає ініціатору свій відкритий ключ. У той же час відповідач формує спільну таємницю на основі ключа, який він отримав, тобто формує спільний із зловмисником ключ.

Зловмисник отримує відкритий ключ відповідача і формує з ним спільну таємницю, а ініціатору відправляє свій відкритий ключ. Ініціатор отримує відкритий ключ зловмисника і, використовуючи його, формує спільну таємницю. Таким чином, тепер зловмисник має спільні таємниці з ініціатором та відповідачем. Ініціатор чи відповідач, відсилаючи інформацію на цьому ключі іншому суб'єктові, вважає, що тільки той суб'єкт може відновити її. Насправді інформація перехоплюється зловмисником, розшифровується та зашифровується для іншого суб'єкта. Таким чином, зловмисник завжди зможе з'ясувати, яку інформацію передають між собою суб'єкти, більше того, без зловмисника взагалі буде неможливо передати інформацію.

Загальний рівень безпеки щодо викриття спільного ключа. У протоколі безпека спільного ключа повністю базується на складності розв'язання дискретного логарифмічного рівняння в групі точок еліптичної кривої. При застосуванні протоколу необхідно вважати, що зловмисник не може видати себе за ініціатора та відповідача протоколу. У разі коли зловмисник може видати себе за ініціатора або відповідача протоколу, він може нав'язати спільні таємниці і повністю скомпрометувати захищений обмін інформацією.

Рекомендації з використання протоколу. Протокол узгодження спільної таємниці може бути використаний тільки за умови, що зловмисник не може бути ініціатором або відповідачем у протоколі узгодження спільної таємниці. Для захисту від активної атаки типу «об'єкт посередині» необхідна додаткова взаємна автентифікація ініціатора та відповідача. Для захисту від атаки нав'язування спільної таємниці суб'єктом-ініціатором або суб'єктом-відповідачем, необхідна додаткова однонаправлена або взаємна автентифікація. Протокол забезпечує криптоживучість особистих ключів ініціатора та відповідача, тому що ключі змінюються кожного сеансу. При застосуванні протоколу необхідно виконати заходи щодо забезпечення працездатності каналу обміну інформацією.

1.3.16 Аналіз механізму узгодження ключів типу Діффі-Геллмана з 2-х ключовими парами

Цей механізм узгодження ключів установлює розділювану таємницю між об’єктами А та В за два проходи.

Налаштування. Перед процесом узгодження спільної таємниці додатково до спільної інформації необхідно:

– для кожного об’єкта X установити особистий ключ для узгодження ключів d_X та відкритий ключ – для узгодження ключів P_X, який є точкою еліптичної кривої, що задовольняє рівнянню $P_X = d_X G$;

– для кожного об’єкта забезпечити доступ до автентичної копії відкритого ключа з метою узгодження ключів іншої сторони для кожного об’єкта;

– кожен об’єкт повинен незалежно перевірити, що відкритий ключ іншого об’єкта дійсно є точкою еліптичної кривої.

Формування маркера ключа (А)

Об’єкт А випадково генерує таємне значення r_A, що перебуває в діапазоні $\{1,..., n-1\}$, обчислює $r_A G$, формує маркер ключа $KT_{A1} = r_A G$ та надсилає його об’єкту В.

Формування маркера ключа (В)

Об’єкт В випадково генерує таємне значення r_B, що перебуває в діапазоні $\{1,..., n-1\}$, обчислює $r_B G$, формує маркер ключа $KT_{B1} = r_B G$ та надсилає його об’єкту А.

Формування спільної таємниці (А)

Об’єкт А має перевірити, що маркер KT_{B1} дійсно є точкою еліптичної кривої. Об’єкт А обчислює спільну таємницю: $K_{AB} = (d_A \cdot l)(hKT_{B1}) \| (r_A \cdot l)(hP_B)$

Формування спільної таємниці (В)

Об’єкт В має перевірити, що маркер KT_{A1} дійсно є точкою еліптичної кривої. Об’єкт В обчислює спільну таємницю: $K_{AB} = (r_B \cdot l)(hP_A) \| (d_B \cdot l)(hKT_{A1})$.

Цей механізм узгодження ключів має такі властивості:

– число проходів – 2;

– механізм забезпечує криптоживучість ключів суб’єктів А і В окремо;

– механізм забезпечує взаємну неявну автентифікацію ключа;

– протокол призначений для встановлення спільної таємниці між двома суб’єктами за два проходи (раунди).

Обсяг попередньо необхідної інформації. Попередньо має бути встановлена загальна інформація, сформовані пари особистий/відкритий ключ d_a, Q_a та d_b, Q_b користувачів А та В відповідно, а також сертифіковані відкриті ключі P_a, P_b, які мають бути доступними із забезпеченням їх цілісності й справжності.

Кількість проходів. Алгоритм вимагає виконання двох проходів при встановленні спільного ключа. Криптоаналітик може визначити факт встановлення спільного ключа та перехопити відкриті ключі сеансу ініціатора та відповідача протоколу.

Кількість ключів (ключових пар). Для виконання протоколу необхідно, щоб обидва суб’єкти мали по одній парі особистий/відкритий ключ, які генеровані на етапі попередньої підготовки та доставлені суб’єктам з додержанням цілісності й справжності чи розміщені в якості доступного сертифікату, а також по одній парі особистий/відкритий ключ, що мають бути генеровані під час виконання протоколу. Загальна кількість ключових пар, що використовуються під час виконання алгоритму, дорівнює чотирьом.

Пасивна атака. Під час цієї атаки криптоаналітик намагається перехопити всі повідомлення, якими обмінюються суб’єкти, що узгоджують ключ. При використанні інтерактивного протоколу узгодження ключів типу Діффі-Геллмана між сторонами відбувається два раунди передачі даних – суб’єкт-ініціатор та суб’єкт-відповідач передають один одному свої відкриті ключі. Криптоаналітик теоретично може перехопити обидві пари ключів. Крім того, зловмисник може отримати статичні відкриті ключі (сертифікати). Для розкриття будь-якої інформації, що буде передаватися з використанням спільної

таємниці, отриманої за допомогою усіх пар ключів, зловмисник має встановити за відомими ключами щонайменше по одному особистому ключу зі статичних і сеансових пар ключів, тобто двічі вирішити завдання типу “ повне розкриття ”. У разі коли результати роботи протоколу (спільна таємниця) ніяк не обробляються і використовуються як ключ у чистому вигляді, криптоаналітику може бути вигіднішим з’ясувати тільки половину ключа, тобто розв’язати одне дискретне логарифмічне рівняння. Але визначення особистих ключів сеансових пар суб’єктів не призведе до реалізації атаки типу «повне розкриття», оскільки визначений зловмисником особистий ключ більше не буде використовуватись у системі і на основі отриманого ключа можна встановити тільки ключ сеансу, який вже відбувся, і виконати розкриття тільки тієї інформації, що передана на цьому ключі.

Активна атака. Ця атака вимагає взаємодії між суб’єктами під час узгодження ключів. У протоколі здійснюється два раунди взаємодії між учасниками протоколу – передача відкритого ключа сеансу суб’єкта-ініціатора суб’єктові-відповідачу і навпаки. Для виконання атаки зловмисник може здійснити тільки одну атаку: завадити суб’єктам, які взаємодіють, виробити ключ. В такому разі зловмисник може перехоплювати та модифікувати повідомлення. У результаті цього суб’єкти не зможуть виробити однакову спільну таємницю. Виконання атак типу «об’єкт посередині» чи формування спільної таємниці неможливо, бо ініціатор і відповідач володіють сертифікатами (чи просто цілісними й справжніми копіями) статичних відкритих ключів один одного.

Загальний рівень безпеки щодо визначення спільної таємниці (ключа). Безпека спільної таємниці (ключа) повністю базується на складності розв’язання дискретного логарифмічного рівняння в групі точок еліптичної кривої. Вона детально розглядається в розділі 4 цієї монографії. Аналіз протоколу показав, що зловмисник не може видати себе як за ініціатора, так і за відповідача протоколу.

Рекомендації та пропозиції. Протокол може бути використаний, коли необхідно забезпечити взаємну явну автентифікацію ключів P_A та P_B, взаємну

криптографічну живучість. Протокол забезпечує практичну захищеність від пасивних атак типу «повне розкриття». Для її здійснення необхідно кожен сеанс розв'язувати задачу типу «повне розкриття» для визначення особистого ключа сеансу, а також розв'язувати завдання «повне розкриття» для довгострокового особистого ключа, пов'язаного з сертифікатами. Для захисту від активних атак типу модифікування ключів сеансу необхідно використовувати завадостійкі канали обміну інформацією. При використанні протоколу забезпечується взаємна криптоживучість і неявна автентифікація суб'єктів, які взаємодіють.

1.4 Висновки до першого розділу

У даному розділі було розглянуто криптографічні механізми, що можуть бути застосовані при реалізації систем моніторингу поширення інфекційних захворювань.

1. Перш за все розглянуто основи функціонування симетричних криптосистем, базові перетворення, переваги та недоліки та способи реалізації у потокових та блочних перетвореннях. Можна зробити висновок, що блокові симетричні шифри знайшли широке застосування на практиці для вирішення задач забезпечення конфіденційності, цілісності, доступності, захисту від НСД тощо. Разом з тим, БСШ мають ряд недоліків, серед яких необхідно відмітити: достатньо велика складність перетворень при шифруванні, недостатня швидкодія прямих і зворотних криптоперетворень, можна говорити, що забезпечується середня швидкодія, складність, а в ряді випадків і неможливість розпараллелювання процесів крипто перетворень, всі блоки зашифровуються з використанням одного і того самого ключа тощо. Вирішення цього протиріччя покладається на потокові симетричні перетворення – потокові симетричні шифри (ПСШ). Необхідно відмітити, що зважаючи на вказані переваги ПСШ, на міжнародному рівні проведено та виконано ряд науково-практичних результативних проектів – Nessie, eSTREAM. І за результатами цього конкурсу

визначено ряд алгоритмів, які можуть бути застосовані у практичних системах, у тому числі вони є ефективними при реалізації систем моніторингу контактів.

2. У той же час задля забезпечення конфіденційності, безпечності та інших функцій для користувачів систем моніторингу можуть бути застосовані асиметричні криптосистеми. Найбільшою особливістю асиметричних перетворень є використання асиметричної пари ключів, які містить відкритий ключ, що відомий всім, та особистий ключ, що пов’язаний з відкритим ключем за допомогою певного математичного перетворення. При цьому вважається що обчислення особистого ключа, при знанні загальносистемних параметрів та відкритого ключа, повинно мати в гіршому випадку субекспоненційну складність, за умови коли обчислення відкритого ключа при формуванні асиметричної ключової пари – поліноміальну. Вказана особливість несе в собі як переваги так і недоліки, що стала предметом розгляду в цьому розділі. Здійснено порівняння асиметричних та симетричних криптосистем з точки зору об’єму даних та безпечності, що вони забезпечують.

3. Третім вектором досліджень у даному розділі стали криптографічні протоколи взаємодії, які можуть бути застосовані при взаємодії користувачів систем моніторингу. Особливістю криптопротоколів є те, що вони виконуються на основі застосування однієї або декількох криптосистем (криптоалгоритмів), відповідних ключових даних, параметрів і т. ін. В моделі взаємної недовіри взаємодіючі об’єкти та суб’єкти, які мають між собою інформаційні співвідношення мають бути захищені від обману, в тому числі, і юридично. У розділі наведено рекомендації для реалізації різних протоколів автентифікації та розподілення таємниці з точки зору програмної імплементації та побудови систем моніторингу та інформування населення щодо епідеміологічної ситуації.

2 ФОРМУЛЮВАННЯ КОНЦЕПТУАЛЬНИХ ПОЛОЖЕНЬ З РОЗРОБКИ, АНАЛІЗУ ТА ЗАСТОСУВАННЯ РІЗНИХ РІШЕНЬ ЩОДО ПРОТОКОЛІВ ВЗАЄМОДІЇ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ У СИСТЕМ МОНІТОРИНГУ ЗАПОБІГАННЯ ПОШИРЕННЯ ІНФЕКЦІЙНИХ ЗАХВОРЮВАНЬ

Останні епідеміологічні події у світі перевірили на міцність класичні підходи запобігання надзвичайним ситуаціям та виявили, що сучасні методи не завжди є ефективними. Поява нових форм і методів інформаційного впливу на різні пласти інформаційно-керуючих систем зумовлює підвищення вимог до їх надійності та безпеки. Особливої уваги у цьому розумінні потребують не тільки питання інформаційної та кібербезпеки критично важливих інформаційних, як зазвичай, але й питання персональних та медичних даних учасника цієї мережі.

Згідно до Закону про персональні дані [20], персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, та його дія поширюється на відносини щодо обробки персональних даних на території України. Якщо розглядати міжнародному практику, то відповідність до General Data Protection Regulation (GDPR/Регламент) [21] в Україні це фактично визначить умови входу українських компаній та європейських компаній з українськими фаундерами до ринку ЄС. На відміну Закону GDPR чітко визначає межі своєї територіальної юрисдикції, вказуючи, що його дія поширюється на:

– опрацювання персональних даних контролером або оператором, що зареєстрований на території ЄС;

– опрацювання персональних даних контролером або оператором, які зареєстровані поза територією ЄС, проте які обробляють дані осіб, що перебувають в ЄС.

Відповідно до Закону, персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. В цілому, таке визначення персональних даних запозичене з

тексту GDPR та дещо трансформоване. Як наслідок, персональні дані за GDPR є більш широкою та деталізованою категорією, тому що:

– використовує поняття «будь-яка інформація, що стосується особи», а не відомості про особи (наприклад, назва фірми, у якій використовується ПІБ особи буде інформацією, що стосується особи, проте не буде відомостями про особу);

– додатково роз'яснює, коли особа може вважатися такою, яку можна ідентифікувати.

GDPR встановлює шість підстав, на основі яких можна законно здійснювати обробку персональних даних суб'єкта. Основною підставою є згода суб'єкта даних на обробку його персональних даних. До інших підстав відносяться необхідність виконання договору з суб'єктом, необхідність захисту життєво важливих інтересів суб'єкта, необхідність виконання контролером покладених на нього обов'язків і т.п. По аналогії з питанням визначення суб'єкта даних, Закон повністю рецепіює положення GDPR та в зміненому формулюванні встановлює ті ж самі шість підстав, на основі яких можна здійснювати обробку даних.

Можна сформувати певні критерії, які повинні бути каменем спотикання під час вибору, обґрунтування та встановлення вимог до системи національного рівня, якою є система моніторингу запобігання поширення інфекційних захворювань мають ряд. Це передусім захист персональних й медичних даних учасників системи; деанонімізація обробляємих даних; втручання в збір статичних даних, тим самим викривляючи реальні дані епідеміологічного стану в країні; одержання неправомірної вигоди, тобто це стосується загрози конфіденційності та дотримання прав людини.

Вирішати складну задачу моніторингу можна двома різними моделями – централізована база даних з довіреною стороною і обробкою даних та децентралізована база даних виключно у зашифрованому вигляді з гарантією приватності й доступності даних виключно стороні, що володіє відповідними фрагментами даних та не має довіри до решти учасників.

Метою даного розділу буде формування концептуальних положень з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань.

Об’єктом дослідження це процеси забезпечення послуг безпеки, моделі та методи та механізми моніторингу в умовах надзвичайних ситуацій.

Предметом є технології інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

Коли людина отримує позитивний результат тесту на COVID-19 від органу охорони здоров’я, вона завантажує їх відкриті контактні дані на серверний сервер. Прикладами таких систем є ROBERT, PEPP-PT та OpenTrace/BlueTrace/TraceTogether. Різниця між двома групами стає все більш розмитою. Різниця між централізованими та децентралізованими протоколами полягає не в існуванні серверу додатку, оскільки у централізованих і децентралізованих реалізаціях протоколів він є. Різниця насправді полягає в місці виконання певних ключових функцій, таких як генерація унікальних ідентифікаторів та розрахунок епідеміологічно ефективних показників ризику на основі даних ризику контактів.

2.1 Міжнародна практика та рекомендації щодо впровадження систем моніторингу запобігання поширення інфекційних захворювань

Централізація контактних даних, яка вбудована в централізований підхід, може бути відтворена в децентралізованому протоколі шляхом добровільної передачі контактних даних на серверний сервер після їх збору. З іншого боку, децентралізований протокол покладається на сервери для зберігання та обробки певної добровільно наданої інформації відстеження контактів.

Організація відстеження безпосередності збереження конфіденційності (PEPP-PT) [22], яка з’являється на її головній веб-сторінці, робить відмінність

між двома підходами ще більш розмитою: «PEPP-PT наразі розглядає два підходи для збереження конфіденційності: «централізований» і «децентралізований», і продовжує бути відкритим для подальших ідей щодо вдосконалення, які підтримують цілі PEPP-PT».

Таким чином, основні занепокоєння щодо централізованих і децентралізованих протоколів зв'язку пов'язані з поєднанням проблем безпеки та конфіденційності, технічних обмежень та ринкових позицій Google і Apple, як основних гравців на ринку операційних систем для смартфонів [23]. Початкова реалізація функції BLE на Apple [24] показала, що мобільні телефони зробили

Схоже, не дозволяє централізованим програмам, які працюють у фоновому режимі, отримувати та завантажувати історію всіх спостережуваних контактів. Для виконання такої функції операційна система Apple до 13.5 версії 5 вимагала б розблокованих мобільних пристроїв для запуску програми COVID-19 на передньому плані, або вимагають уникання використання режиму BLE, що сильно впливає на тривалість роботи акумулятора. Як результат цих технічних обмежень деякі держави-учасники та організації централізованого протоколу (PEPP-PT) нещодавно перейшли від централізованого до децентралізованого підходу.

Основна проблема з багатьма різними національними додатками для відстеження контактів COVID-19 полягає в тому, що ви не знаєте, чи працюватимуть вони, коли громадяни однієї країни їдуть в іншу. Використання кількох програм під час подорожей може ще більше ускладнити недоведену технологію та означатиме спробу змінити стандарт. компоненти смартфона для оцінки впливу вірусів, завдання, для якого мобільні пристрої ніколи не були призначені. Тому взаємосумісність програм відстеження контактів між державами-членами та додатками є ключовою: усі програми соціального відстеження повинні мати можливість обмінюватися мінімальний обсяг інформації, необхідний для попередження окремих користувачів програми, де б вони не знаходилися в ЄС, епідеміологічно значущого впливу на користувача, який має COVID-19.

13 травня 2020 року добровільна мережа e-Healthp [25], яка надає платформу для органів держав-членів, що займаються цифровим здоров’ям, запропонувала рекомендації щодо транскордонної взаємодії схвалених мобільних програм для відстеження контактів та пов’язаних процедур. Деякі питання залишаються відкритими, щодо, наприклад, сумісності централізованих і децентралізованих систем відстеження контактів, визначення передової практики та механізмів обміну інформацією щодо функціонування програм, різних проблем конфіденційності та обміну даними з відповідними органами охорони здоров’я та дослідницькими установами, включаючи обмін інформацією агрегованих даних з Європейським центром профілактики та контролю захворювань. Органи влади держав-членів, представлені в мережі e-Health, повинні створити процес обміну інформацією, що забезпечує сумісність програм, коли очікуються транскордонні сценарії.

Незалежно від підходу держав-членів до схвалених програм, усі держави-члени та Комісія вважають сумісність програм і серверних серверів важливою для ефективного відстеження транскордонних ланцюжків зараження, особливо для транскордонних працівників і сусідніх країн. Зрештою, ці зусилля підтримають поступове скасування прикордонного контролю в ЄС та відновлення свободи руху та цілісності Bluetooth сигналу. Однак успіх додатків також залежить від низки інших параметрів, таких як загальна прихильність населення до таких систем, критична маса користувачів і технічна стабільність і надійність сигналів Bluetooth.

Основні позиції ЕС щодо централізованих та децентралізованих підходів це спільний підхід до кризи COVID-19, який також став необхідним, оскільки в деяких країнах вживаються заходи, такі як відстеження осіб на основі геолокації, використання технологія оцінки рівня ризику для здоров'я людини та централізація конфіденційних даних викликає питання з точки зору кількох основних права і свободи, які гарантовані правовим порядком ЄС, включаючи право на приватність і право на захист персональних даних.

Відповідно до принципу мінімізації даних органи охорони здоров'я та науково-дослідні установи повинні обробляти персональні дані лише в тих випадках, коли вони достатні, релевантні та обмежені тим, що необхідно, і повинні застосовувати відповідні запобіжні заходи, такі як псевдонімізація, агрегація, шифрування та децентралізація.

Рекомендація Європейської комісії від 8 квітня 2020 року [26] щодо спільного інструментарію Союзу мовить про використання технологій та даних для боротьби та вихід із кризи COVID-19, зокрема щодо мобільних додатків та використання анонімних даних мобільності.

Розпорядження ЕС комісії від 16 квітня 2020 року[27] – Функціональність відстеження контактів та попередження це дані інфікованої особи. Програми генерують псевдовипадкові ефемерні та періодично змінювані ідентифікатори телефонів, які знаходяться в контакт з користувачем. Одним з варіантів є те, що ідентифікатори зберігаються на пристрої користувача (так звана децентралізована модель обробки). Інший варіант може передбачити, що ці довільні ідентифікатори зберігаються на сервері, до якого органи охорони здоров'я мають доступ (так зване рішення центрального керуючого сервера). Децентралізоване рішення більше відповідає принципу мінімізації. Органи охорони здоров'я повинні мати доступ лише до даних про близькість із пристрою інфікованої людини, щоб вони могли контактувати з людьми, які ризикують зараження.

Резолюція Європейського парламенту від 17 квітня 2020 року [28] бере до уваги появу додатків для відстеження контактів на мобільних пристроях, щоб попередити людей, якщо вони були близькі до інфікованої людини, і рекомендація Комісії розробити загальний підхід ЄС до використання таких програм; зазначає, що будь-яке використання програм, розроблених національними органами та органами ЄС, не може бути обов'язковим і що створені дані не повинні зберігатися в централізованих базах даних, які схильні до потенційного ризику зловживання та втрати довіри та може поставити під загрозу поширення в усьому Союзі; вимагає децентралізації всього зберігання

даних, забезпечення повної прозорості комерційних інтересів розробників цих додатків (не в ЄС), а також продемонструвати чіткі прогнози щодо використання програм відстеження контактів частиною населення, у поєднання з конкретними іншими заходами призведе до значно меншої кількості інфікованих; вимагає, щоб Комісія та держави-члени були повністю прозорими щодо функціонування програм для відстеження контактів, щоб люди могли перевірити як базовий протокол для безпеки та конфіденційності, так і перевірити сам код, щоб перевірити, чи програма функціонує так, як стверджують органи влади; рекомендує встановити положення про припинення дії та повністю дотримуватись принципів захисту даних шляхом проектування та мінімізації даних.

Рекомендації Європейського наглядового органу з питань захисту даних від 21 квітня 2020 р. [29] - реалізація відстеження контактів може здійснюватися за централізованим або децентралізованим підходом (примітка: загалом, децентралізоване рішення більше відповідає принципу мінімізації). Обидва слід вважати життєздатними варіанти, за умови застосування відповідних заходів безпеки, кожен із яких супроводжується набором переваг і недоліки.

Таким чином, концептуальна фаза розробки програми завжди повинна включати ретельний розгляд обох концепцій, ретельно зважуючи відповідний вплив на захист/конфіденційність даних та можливий вплив на права окремих осіб.

2.2 Концептуальні принципі застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу

Втручання в приватне життя та право на захист персональних даних може бути особливо значним, враховуючи те, що деякі функціональні можливості засновані на моделі з інтенсивним використанням даних. Наведені нижче принципи мають на меті надати вказівки щодо того, як обмежити нав’язливість

функцій програми, щоб забезпечити відповідність законодавству про захист персональних даних та конфіденційність.

2.2.1 Принцип контролю

Вирішальним фактором для того, щоб люди довіряли додаткам, є демонстрація того, що вони зберігають контроль над своїми особистими даними. Для забезпечення цього, повинно бути виконані такі умови:

– встановлення додатка на їхній пристрій має бути добровільним і без будь-яких негативних наслідків для особи хто вирішить не завантажувати/використовувати програму;

– різні функції програми (наприклад, інформація, перевірка симптомів, функції відстеження контактів і попередження) не включати в пакет, щоб особа могла надати свою згоду спеціально для кожної функції. Цього не слід заборонити користувачеві комбінувати різні функції програми, якщо це пропонується як опція постачальником;

– якщо використовуються безпосередні дані (дані, отримані в результаті обміну сигналами Bluetooth Low Energy (BLE) між пристроями на епідеміологічно відповідній відстані та протягом епідеміологічно важливого часу), їх слід зберігати пристрій особи. Якщо ці дані мають бути надані органам охорони здоров’я, їх слід повідомити лише після цього підтвердження того, що відповідна особа інфікована COVID-19 і за умови, що вона/він вирішить це зробити тому;

– органи охорони здоров’я повинні надавати особам всю необхідну інформацію, пов’язану з обробкою її чи його персональні дані (відповідно до статей GDPR та Закону про персональну інформацію);

– особа повинна мати можливість реалізувати свої права відповідно до Закону про персональну інформацію (зокрема, доступ, виправлення, видалення). Будь-які обмеження прав відповідно до нормативних норм має відповідати цим актам і необхідним, пропорційна та передбачена законодавством;

– програми слід деактивувати не пізніше, коли пандемія оголошена контрольованою; деактивація повинна не залежить від деінсталяції користувачем.

2.2.2 Правова основа для обробки

Встановлення програм та збереження інформації на пристрої користувача, як зазначено вище, зберігання інформації на пристрої користувача або отримання доступу до вже збереженої інформації дозволено лише в тому випадку, коли користувач дав згоду або зберігання та/або доступ суворо необхідно для послуги інформаційного суспільства (наприклад, програми), яку явно запитує (тобто встановлюється та активується) користувачем.

Зберігання інформації на пристрої особи та отримання доступу до інформації, що вже зберігається на цьому пристрої зазвичай необхідні для роботи програм. Крім того, функція відстеження контактів і попередження вимагає збереження певної іншої інформації (наприклад, тимчасової, періодично змінюваної псевдоніми користувачів цієї функції в безпосередній близькості). Таке завантаження не є необхідним для функціонування програми як такої. Згода має бути «наданою вільно», «конкретною», «явною» та «інформованою». Воно має виражатися через чітку стверджувальну дію особистості; це виключає мовчазні форми згоди.

Національні органи охорони здоров’я, як правило, обробляють персональні дані, коли є юридичні зобов’язання, встановлені в ЄС або законодавством, що передбачає таку обробку та коли така обробка необхідна для виконання завдання, яке виконується для визначеної підтримки суспільних інтересів.

Законодавство має передбачати конкретні та відповідні заходи для захисту прав і свобод суб’єктів даних. Як загальне правило: чим сильніше впливають на свободи індивідів, тим сильнішими мають бути відповідні гарантії передбачені відповідним законом.

З огляду на характер відповідних персональних даних (зокрема дані про здоров’я як спеціальні категорії персональних даних), а також обставини поточної пандемії COVID-19, спираючись на закон як на правову основу, сприятиме правовому визначеності, оскільки це детально прописує обробку конкретних даних про стан здоров’я та чітко визначає цілі для обробка; й чітко вказати, хто є контролером, тобто суб'єктом, який обробляє дані, і хто, крім контролера, може мати доступ до таких даних; виключити можливість обробки таких даних для цілей, відмінних від перерахованих у законодавство та передбачають конкретні гарантії. Щоб не підірвати суспільну корисність і сприйняття додатків національний законодавець має звернути особливу увагу на те, щоб вибране рішення було настільки ж інклюзивним по відношенню до громадян, як можливо.

Обробка органами охорони здоров’я на підставі законодавства не змінює того факту, що особи залишаються вільними встановити програму чи ні, а також поділитися своїми даними з органами охорони здоров’я. Ніяких негативних наслідків для користувачів не повинно тому відбувається щоразу, коли програму видаляють.

Програми для відстеження контактів і попереджень забезпечують попередження осіб. Коли це попередження надається безпосередньо додатком, Комісія звертає увагу на заборону піддавати окремих осіб рішенням, заснованим виключно на автоматизованих обробках, яка має юридичну силу або подібним чином істотно впливає на нього.

2.2.3 Принцип мінімізації даних

Дані, створені за допомогою пристроїв і вже збережені на цих пристроях, захищені таким чином:

– як «персональні дані», тобто будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи, він захищений відповідно до GDPR. Дані про здоров’я отримують додатковий захист (стаття 9 GDPR).

– як «дані про місцезнаходження», тобто дані, що обробляються в мережі електронних комунікацій або за допомогою електронного зв'язку сервіс із зазначенням географічного положення кінцевого обладнання користувача.

– Будь-яка інформація, що зберігається на кінцевому обладнанні користувача та до якої здійснюється доступ із нього.

– Неособисті дані (наприклад, безповоротно анонімізовані дані) не захищені відповідно до законодавства.

Принцип мінімізації даних вимагає, щоб персональні дані були адекватними, релевантними і обмежено тим, що необхідно для мети, може бути оброблено. Оцінка необхідності обробки персональних даних та релевантність таких персональних даних повинні здійснюватися у світлі мети (цілей). Наприклад, що якщо метою функціональності є перевірка симптомів або телемедицина, ці цілі не вимагають доступу до списку контактів особи, яка володіє пристроєм.

Генерування та обробка менше даних обмежує ризики безпеки. Тому дотримання заходів мінімізації даних також передбачає гарантії безпеки.

Інформаційна функціональність. Додатку лише з цією функціональністю не потрібно буде обробляти будь-які дані про здоров'я людей. Це лише забезпечить їх інформацією. Для досягнення цієї мети не можна зберігати інформацію, яка зберігається в термінальному обладнанні та до якої можна отримати доступ обробляється інакше, ніж необхідне для надання інформації.

Функції перевірки симптомів і телемедицини. Якщо додаток містить одну або дві з цих функцій, він оброблятиме персональні дані про здоров'я. Тому список даних які можуть бути оброблені, мають бути визначені в базовому законодавстві, що застосовується до органів охорони здоров'я.

Крім того, органам охорони здоров'я можуть знадобитися номери телефонів осіб, які використовували перевірку симптомів та завантажив результати. Інформація, що зберігається в термінальному обладнанні та доступна з нього, може оброблятися лише в тій мірі, в якій вона є необхідна, щоб програма могла виконувати своє призначення та функціонувати.

Функція відстеження контактів і попередження. Більшість заражень COVID-19 відбувається через крапельки, які переміщуються лише на обмежену відстань. Ідентифікація так само швидко, як Можливі особи, які перебували поблизу інфікованої людини, є ключовим фактором для переривання ланцюга зараження. Визначення близькості є функцією відстані та тривалості контакту та має здійснюватися з епідеміологічного точка зору. Переривання ланцюга зараження є особливо важливим, щоб уникнути повторного виникнення інфекцій під час кризи фаза виходу.

Для цього можуть знадобитися дані про близькість. Для вимірювання наближених і близьких контактів Bluetooth Low Energy (BLE) зв'язок між пристроями виглядає точнішою, а отже, більш доцільною, ніж використання даних геолокації (GNSS/GPS або дані про місцезнаходження стільникового зв’язку). BLE уникає можливості відстеження (на відміну від геолокаційних даних). Тому рекомендується використовувати комунікаційні дані BLE (або дані, згенеровані за допомогою еквівалентної технології).

Дані про місцезнаходження не потрібні для функціональних можливостей відстеження контактів, оскільки їх мета — не слідувати переміщення окремих осіб або виконання приписів. Крім того, обробка даних про місцезнаходження в контексті контакту відстеження було б важко виправдати у світлі принципу мінімізації даних і може створити проблеми з безпекою та конфіденційністю.

З цієї причини порадити не використовувати дані про місцезнаходження в цьому контексті.

Незалежно від технічних засобів, що використовуються для визначення близькості, не видається необхідним зберігати точний час контакт або місце (за наявності). Однак може бути корисно зберегти день контакту, щоб знати, чи є контакт відбулося, коли у людини з’явилися симптоми (або за 48 годин) і щоб направляти подальше повідомлення з порадою, наприклад, про те, як довго проводити самокарантин.

Дані близькості слід створювати та обробляти лише за наявності реального ризику зараження (залежно від близькості та тривалість контакту). Слід

зазначити, що необхідність та пропорційність збору даних, таким чином, залежатиме від таких факторів, як ступінь доступності засобів для тестування, зокрема, коли такі заходи, як тримання під вартою, вже були призначені.

Попередження осіб, які перебували в тісному контакті з інфікованою людиною, можна зробити двома способами:

– Згідно з першим підходом, сповіщення автоматично доставляється через додаток близьким контактам, коли користувач сповіщає програму – зі схваленням або підтвердженням органу охорони здоров’я, наприклад, за допомогою QR-коду або TAN-коду – що він чи вона пройшли тестування позитивний (децентралізована обробка). Зміст попереджувального повідомлення бажано визначатися за станом здоров’я авторитет.

– Згідно з другим підходом довільні тимчасові ідентифікатори зберігаються на серверному сервері, який утримується працездатністю повноваження (рішення серверного сервера). Користувачів неможливо ідентифікувати безпосередньо за допомогою цих даних. Через ідентифікатори, користувачі які перебували в тісному контакті з користувачем із позитивним тестом, отримають сповіщення на своєму пристрої. За бажанням органів охорони здоров’я щоб зв'язатися з користувачами, які були в тісному контакті з інфікованою людиною, також по телефону або SMS, їм потрібна згода цих користувачів надати свої номери телефонів.

2.2.4 Принцип обмеження розкриття/доступу даних

Інформаційна функціональність. Жодна інформація, що зберігається в термінальному обладнанні та доступна з неї, не може бути передана органам охорони здоров’я, крім необхідної мати інформаційний функціонал. Оскільки ця функціональність передбачає лише засоби зв'язку, здоров'я органи влади не отримають доступу до інших даних.

Функції перевірки симптомів і телемедицини. Функція перевірки симптомів може бути корисною для держав-членів, щоб керувати громадянами

щодо того, чи варто їм проходити тестування, надати інформацію про ізоляцію, а також про те, коли і як отримати медичну допомогу, зокрема для груп ризику. Ця функціональність може також доповнювати нагляд за первинною медичною допомогою та допомогти зрозуміти рівень зараження COVID-19 у країні населення. Тому може бути прийнято рішення, що відповідальні органи охорони здоров'я та національні епідеміологічні органи має отримати доступ до інформації, наданої пацієнтом. Пристрій міг отримувати зведені дані від національних органи епідеміологічного нагляду.

Якщо вирішено дозволити контакт з чиновниками охорони здоров’я, а не лише через саму програму, тоді розкривайте інформацію національним органам охорони здоров’я також необхідний номер телефону користувачів програми.

Функція відстеження контактів і попередження:

Дані зараженої людини. Програми генерують псевдовипадкові ефемерні та періодично змінювані ідентифікатори телефонів, які контактують з користувачем. Одним з варіантів є те, що ідентифікатори зберігаються на пристрої користувача (так звана децентралізована обробка). Інший опція може передбачати, що ці довільні ідентифікатори зберігаються на сервері, до якого мають доступ органи охорони здоров’я (так називається рішенням backend серверу). Децентралізоване рішення більше відповідає принципу мінімізації. Міністерство здоров’я повинно мати доступ лише до даних про близькість з пристрою інфікованої людини, щоб вони могли контактувати з людьми з ризиком зараження.

Ці дані будуть доступні органам охорони здоров’я лише після того, як інфікована людина (після проходження тесту) проактивно ділиться з ними цими даними.

Зараженій людині не слід повідомляти про особу, з якою вона потенційно перебувала епідеміологічно відповідний контакт і хто буде попереджений.

Дані осіб, які були в (епідеміологічному) контакті з інфікованою людиною. Особу інфікованої особи не слід розголошувати особам, з якими вона перебувала в епідеміологічному контакт. Їм достатньо повідомити про те, що вони

перебували в епідеміологічному контакті з інфікованим особи протягом останніх 14 днів. Як зазначалося вище, дані про час і місце таких контактів не повинні зберігатися. це є тому передавати ці дані ані необхідно, ані можливо.

Щоб відстежити епідеміологічні контакти користувача електронної програми, у якого виявлено, що він інфікований, національні органи охорони здоров’я повинні повідомляти лише про ідентифікатор особи, з якою інфікована особа перебуває в епідеміологічному контакті з того часу від 48 годин до появи симптомів до 14 днів після появи симптомів, залежно від близькості та тривалості контакт. Пристрій може отримувати зведені дані відстеження контактів від національних органів для епідеміологічного нагляду індикатори, визначені у співпраці з державами.

2.2.5 Принцип забезпечення точних цілей обробки

Рекомендується не використовувати дані, зібрані за вищевказаних умов, для інших цілей, крім боротьби проти COVID-19. Якщо необхідні такі цілі, як наукові дослідження та статистика, їх слід включити до оригінальний перелік цілей і чітко доведений до користувачів.

Інформаційна функціональність. Метою цієї функції є надання інформації, яка є актуальною з точки зору здоров'я влади в умовах кризи.

Функції перевірки симптомів і телемедицини. Функціональність перевірки симптомів може дати вказівку на те, яка частка осіб повідомила про симптоми сумісний з COVID-19, фактично інфікований (наприклад, шляхом взяття мазка та тестування всіх або випадкової кількості людей на такі симптоми, якщо для цього є можливість). Таке визначення мети має чітко вказати, що персональні дані про здоров’я будуть оброблятися для того, щоб:

– надати особі можливість самостійно оцінити на основі набору запитань, якщо він або у неї з’явилися симптоми COVID-19, або

– отримати медичну консультацію, якщо у неї з’явилися симптоми COVID-19.

Функції відстеження контактів та попередження. Проста вказівка на мету «запобігання подальшому зараженню COVID-19» недостатньо конкретна. У цьому випадку, рекомендується додатково уточнити ціль (цілі) у вигляді: «збереження контактів осіб хто користується додатком і хто міг бути зараженим COVID-19, щоб попередити тих осіб, які могли були потенційно заражені.

2.2.6 Принцип встановлення жорстких обмежень на зберігання даних

Принцип обмеження зберігання вимагає, щоб персональні дані не могли зберігатися довше, ніж це необхідно. Терміни повинні ґрунтуватися на медичній відповідності (залежно від мети програми: інкубаційний період тощо), а також на реалістичній тривалість адміністративних заходів, які може знадобитися вжити.

Інформаційна функціональність. Якщо під час встановлення цієї функції будуть зібрані будь-які дані, їх слід негайно видалити. Немає жодного виправдання збереження таких даних.

Функції перевірки симптомів і телемедицини. Такі дані повинні бути видалені органами охорони здоров’я через не більше одного місяця (інкубаційний період плюс запас) або пізніше людина пройшла тестування і результат негативний. Органи охорони здоров’я можуть зберігати дані протягом більш тривалого періоду для спостереження звітність та дослідження за умови, що вони в анонімній формі.

Функції відстеження контактів та попередження. Дані близькості слід видаляти, як тільки вони більше не потрібні для оповіщення людей. Це повинно максимум через місяць (інкубаційний період плюс запас) або після того, як людина була перевірена і результат є негативний. Органи охорони здоров’я можуть зберігати дані про близькість протягом більш тривалих періодів часу для звітності та досліджень за умови, що це в анонімній формі.

Дані повинні зберігатися на пристрої користувача, і лише дані, які були передані користувачами та необхідні для виконання мети слід завантажити на

сервер, доступний для органів охорони здоров’я, де вибрано цей параметр (тобто лише завантажити дані на сервер «близьких контактів» особи, у якої був позитивний тест на зараження COVID-19).

2.2.7 Принцип забезпечення даних

Рекомендується зберігати дані на кінцевому пристрої особи в зашифрованому вигляді з використанням найсучасніших криптографічних методів. У разі, якщо дані зберігаються на центральному сервері, доступ, в т.ч адміністративний доступ, слід зареєструвати.

Дані близькості повинні створюватися та зберігатися на кінцевому пристрої особи лише в зашифрованому та псевдонімізований формат. Щоб переконатися, що відстеження третіми сторонами виключено, слід активувати Bluetooth можливо без активації інших служб локації.

Під час збору даних про близькість через BLE бажано створювати та зберігати тимчасові ідентифікатори користувачів, які регулярно змінюються замість збереження фактичного ідентифікатора пристрою. Цей захід забезпечує додатковий захист від прослуховування та відстеження хакерів і, отже, ускладнює ідентифікацію осіб.

Комісія рекомендує, щоб вихідний код програми був оприлюдненим і доступним для перегляду. Можна передбачити додаткові заходи для захисту оброблюваних даних, зокрема за допомогою автоматичного видалення або анонімізації дані через певний момент часу. Загалом, ступінь захищеності має відповідати кількості та чутливості оброблених персональних даних.

Усі передачі від персонального пристрою до національних органів охорони здоров’я мають бути зашифрованими. Якщо національна легалізація передбачає, що зібрані персональні дані також можуть бути оброблені для наукових досліджень для цілей, в принципі слід використовувати псевдонімізацію

2.2.8 Принцип забезпечення точності даних

Забезпечення точності оброблених персональних даних є не лише необхідною умовою ефективності програми, але й вимоги законодавства про захист персональних даних.

У цьому контексті забезпечення достовірності інформації про те, чи був контакт із інфікованою людиною (епідеміологічний відстань і тривалість) має важливе значення, щоб звести до мінімуму ризик помилкових результатів. Це має вирішити сценарії, коли два користувачі програми контактують на вулиці, у громадському транспорті чи в будівлі. Малоймовірно, що використання даних про місцезнаходження на основі мобільних телефонних мереж є достатньо точним для цього. Тому доцільно покладатися на технології, які дозволяють більш точно оцінити контакт (наприклад, Bluetooth).

2.2.9 Принцип залучення органів із захисту даних

Органи захисту даних мають бути повністю залучені та консультовані в контексті розробки програми та вони повинні контролювати його розгортання. Враховуючи, що обробка даних у контексті програми буде кваліфікуватися як обробляючи у великому масштабі спеціальні категорії даних (дані про стан здоров’я). Органи повинні враховувати усі передбачення у Закону про персональні дані.

2.3 Формування концепцій розробки протоколів взаємодії та криптографічних перетворень для додатку на основі блокчейн технологій

Уявімо блокчейн рішення у вигляді 4-шарової архітектурі (рис. 2.1) [30], яке працює на цих 4 рівнях. На рівні додатку, клієнти блокчейну використовують функціонал backend серверу, які пов’язані з обліковими записами блокчейну та зовнішніми обліковими записами. Рівень даних містить структури даних

блокчейну. Рівень консенсусу забезпечує послідовний стан блокчейну. Потрібно увагу, що блокчейн може використовувати протоколи консенсусу Proof-of-Work (PoW) [31] та Proof-of-Stake (PoS) [32] та інші. Мережевий рівень формулює однорангову мережу блокчейну (P2P) [33] з вузлами (нодами) або клієнтами, наприклад, нода завжди може отримати оновлений стан блокчейну з деяких активних нод. Навколишнє служить їм 4 шари через відповідний компонент: веб-інтерфейс користувача взаємодіяти з додатками; бази даних для зберігання блокчейн даних; криптографічні механізми підтримки консенсусу протоколи; й інтернет-сервіс для мережевого рівня.

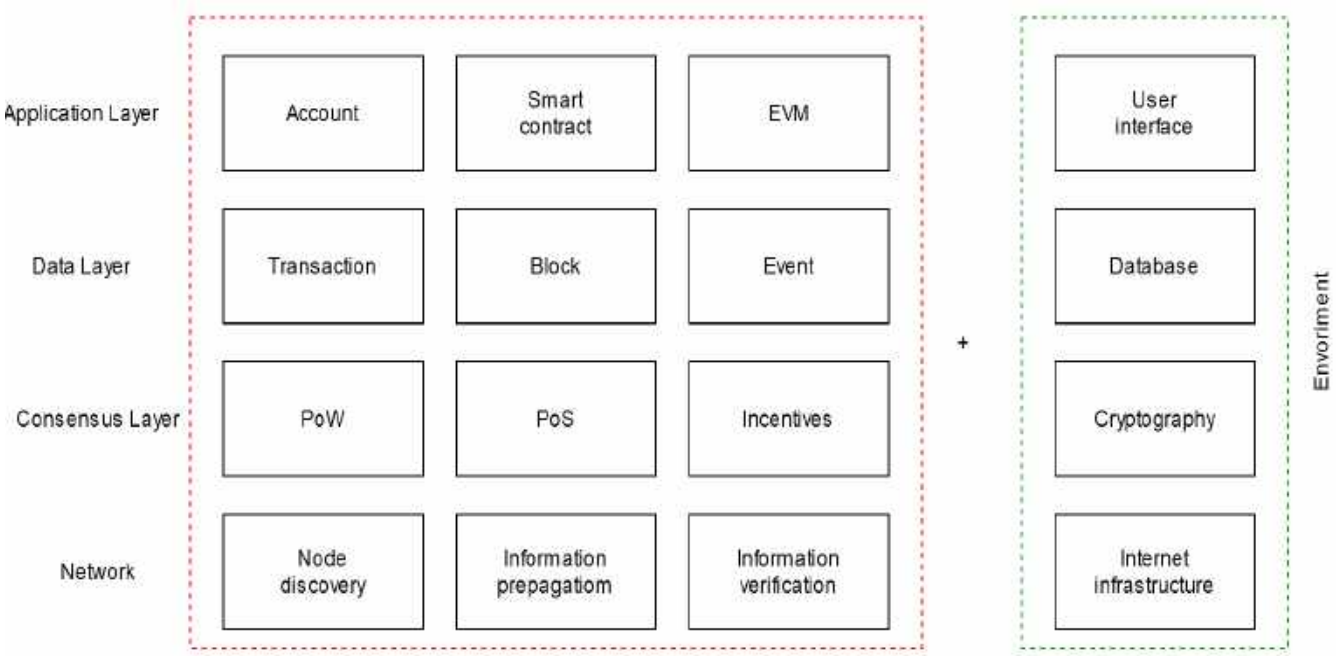


Рисунок 2.1 – Приклад архітектура децентралізованого рішення на основі Ethereum

Шар додатка. Децентралізоване рішення підтримує два типа акаунтів: зовнішні та внутрішні. Особливість зовнішніх акаунтів полягає у тому, що адрес акаунту зв’язуються з відкритим ключем зовнішнього акаунту, адрес внутрішнього акаунту вираховується з секретного ключа внутрішнього учасника децентралізованого додатку.

Шар даних. Транзакції відбуваються у мережі блокчейн та між акаутами з зовні. Транзакція складається з nonce (кількість транзакцій доданих до блоку ланцюга), адрес відправника, адрес отримувача, дані, специфічні дані додатка (наприклад, ліміт Gas та ціна Gas), а також цифровий підпис (рис. 2.2 та 2.3).

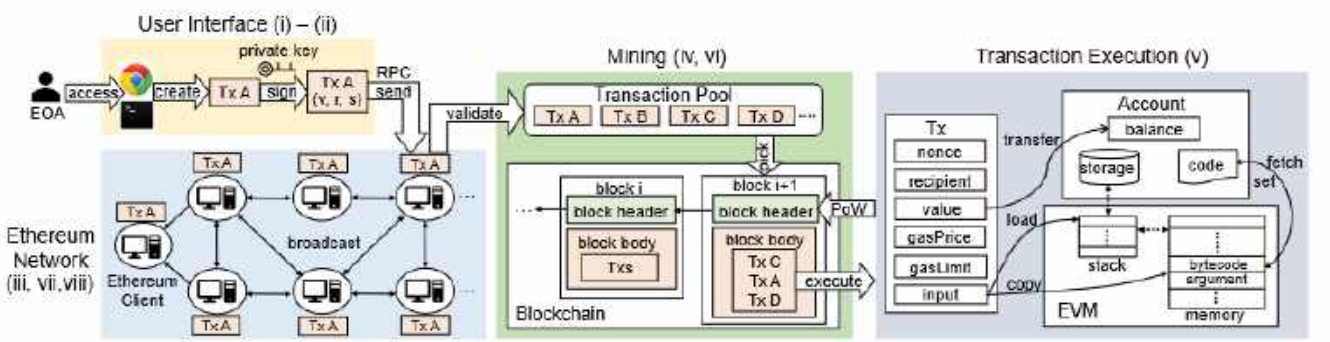


Рисунок 2.2 – Приклад життєвого циклу транзакції децентралізованого рішення

Шар мережі. Мережа – це структурована мережа P2P, де кожен вузол (тобто клієнт) зберігає копію всього блокчейну. Для виявлення та маршрутизації вузлів кожен вузол підтримує динамічну таблицю маршрутизації з 160 сегментів, і кожен сегмент містить до 16 записів ідентифікаторів інших вузлів, IP-адреси, UDP/TCP порти. Блокчейн використовує протокол RLPx для виявлення цільових клієнтів для полегшення обміну інформацією про блокчейн (наприклад, транзакції, блоки) між клієнтами

Шар середовища. Блокчейн працює в середовищі, яке, природно, працює на чотирьох рівнях для надання відповідних послуг, а саме: веб-інтерфейс для взаємодії користувачів із блокчейном; база даних для клієнтів додатку для зберігання даних блокчейну; криптографічні механізми для цілей безпеки; та Інтернет-інфраструктура для підтримки блокчейн-мереж і зв'язку між вузлами. Відокремимо архітектуру блокчейну від середовища, оскільки атаки на блокчейн можуть надходити з середовища, і ці атаки можуть бути краще врегульовані в середовищі, а не блокчейном, що призводить до чистої та модульної абстракції.

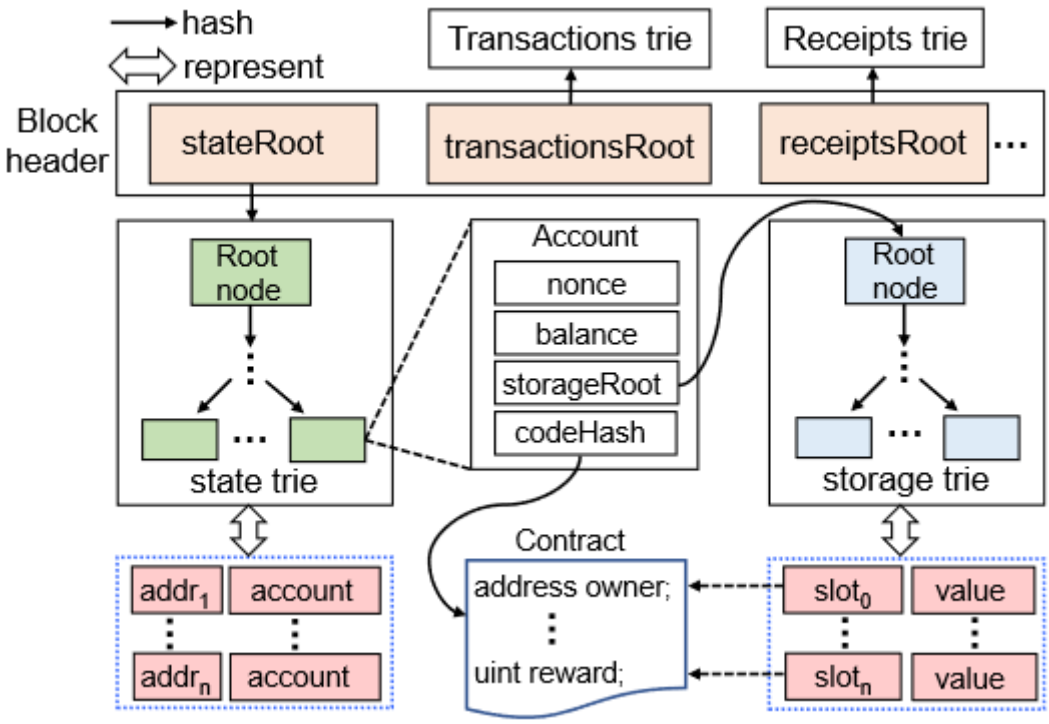


Рисунок 2.3 – Блок-схема блок даних транзакцій, які зберігаються у базі даних

2.3.1 Аналіз вразливостей децентралізованих рішень

Розглянемо основні причин вразливостей: вразливості викликані некомпетентністю або недоліками програмування функціоналу блокчейн рішення, недосконалістю мови та інструментів, дизайном та впровадженням блокчейн рішення, а також людським фактором:

1. На шарі протоколу консенсуса:

– проблема 51%;
– фіксоване припинення протоколу консенсуса;
– DOS-атака.
– Механізм винагороди для майнерів, яку формують блок

2. На шарі мережі:

– відсутність обмеження створення вузлів;
– відсутність ліміту на вхідні з’єднання;
– зовнішня залежність;
– синхронізація єдиного блоку;
– доступ до RPC API.

3. На шарі середовища:

– слабкий пароль;
– XSS;
– неперевірені переадресації URL;
– порушення контролю доступу;
– ненадійний протокол прикордонного шлюзу;
– конфіденційні сервери системних доменних імен (DNS).

4. На шарі додатку:

– повторний вхід;
– ін’єкція в Delegatecall;
– контракт з можливістю оновлення;
– DOS з очікування повернення;
– цілочисельне переповнення;
– маніпулювання з балансом;
– аутентифікація через tx.origin;
– помилкова видимість методів;
– витік даних на довільний адрес;
– збій секретності даних;
– недостатня інформація про підпис;
– DOS з необмеженими операціями;
– неперевірене значення повернення виклику;
– неініціалізований показник зберігання;
– помилкова назва конструктора;
– застаріла версія компілятора;
– коротка адреса;
– обмеження глибини стека викликів;
– заниження коду операцій;
– залежність упорядкування транзакцій;
– залежність від позначки часу;

– генерування випадковості.

5.На шарі даних:

– нерозрізні ланцюжки даних;

– джерело появи даних.

Проаналізувавши ймовірні вразливості, можна виділити наступні причини, які б призвели до виникнення секьюріті проблем:

– некомпетентністю або недоліками розробки функціоналу блокчейн рішення;

– язик програмування та інструменти та сервіси для побудови ланцюгів блоку;

– дизайн та впровадження блокчейн рішення;

– зручність використання блокчейн рішення;

– мережеві фактори.

Для проаналізованих вразливості можна узагальнити наслідки до яких призведе реалізація розглянутих недоліків децентралізованого додатку:

– несанкціоноване виконання коду;

– DoS;

– недобросовісний доходи;

– подвійні витрати;

– витік приватного ключа;

– маніпуляція з веб-сторінкою.

2.3.2 Використання найкращіх практик та принципів під час розробки блокчейну

На відміну від вразливостей і атаки, які природно відповідають деякому шару архітектура децентралізованого додатку, захист ні в якому разі не налаштована у напрямку до шарів. Тому пропонуємо їх класифікувати на два класи: активний захист і реактивний захист. Активний захист спрімований на

вибір спеціальної мови програмування, на вибір актуальною версію програмного забезпечення, використання протоколів консенсусу, крипостійкі криптографічні протоколи. Реактивні засоби захисту мають на меті реагувати на потенційне використання (невідомих) вразливостей під час роботи блокчейну, щоб пом'якшити шкоду. Спостерігає метод перевірки під час виконання сліди виконання для виявлення та, можливо, реагування на підозрілі дії, які можуть порушувати певні властивості.

Підчас розробки децентралізованого рішення необхідно враховувати наступні контролі безпеки:

– *контроль викликів*. Принцип контролю викликів говорить, що розробник повинен забезпечувати взаємодію між внутрішніми акаунтами й зовнішніми. Цей принцип також поділяється на два підпринципи: один – це боротьба з несподіваною поведінкою абонента, а інший – контроль доступу абонента;

– *контроль даних*. Принцип контролю даних говорить, що розробник повинен забезпечувати потік даних контракту. Цей принцип також поділяється на два підпринципи: один стосується захисту конфіденційних даних, а другий — запобігання потраплянню неправильних даних у блок;

– *контроль ресурсів*. Принцип контролю ресурсів говорить, що розробник повинен пом'якшити вичерпання доступного газу в Ethereum;

– *контроль інструментів*. Принцип контролю інструментів говорить про те, що програміст повинен використовувати оновлені інструменти (наприклад, компілятор, налагоджувач) для усунення відомих вразливостей.

А також використовувати сучасні механізми програмної інженерії: для захисту від атак, які можуть використовувати невідомі вразливості, потрібно ввести кілька механізмів розробки програмного забезпечення, орієнтованих на блокчейн, наприклад: механізм обмеження швидкості, який обмежує кількість послідовних дій, які здійснюються зовнішнім учасником, надісланих протягом певного періоду часу; механізм ліміту балансу, який регулює максимальну суму коштів, яка може бути утримана за договором; механізм ліміту швидкості, який відкладає деякі потенційно шкідливі операції.

Для підвищення якості блокчейн рішення необхідно використовувати два методи аналізу програмного коду - статичний аналіз та динамічний аналіз.

У свою чергу статистичний аналіз повинен включати наступні кроки:

– символьне виконання (symbolic execution) – виконання коду за допомогою символів, а не реальні значення змінних. Результати цього аналізу в алгебраїчних термінах оперування цими символами та умовними операторами в програмі призводять до пропозиційних формули, що спрямовують хід виконання. Доцільність шлях потоку визначає, чи є кон'юнкція формул на шляху задоволений;

– CFG (Control Flow Graph) [34] Конструкція – представлення програми в орієнтованому графі. Ребро цього графіка представляє потік виконання із зазначеними умовами на краю як етикетка;

– розпізнавання шаблонів (pattern recognition) [35] – класифікація основ програми одиниці або дані залежно від попередніх знань або статис інформація, отримана з шаблонів;

– аналіз на основі правил (rule-based analysis) [36] – перевірка/аналіз коду специфікація його поведінки на основі правил. На основі правил специфікація описує сценарії під час виконання та накладає обмеження на послідовність операцій і даних входи;

– аналіз декомпіляції (de-compilation analysis) [37-38] – представлення байт-код з вищою абстракцією рівень для покращення аналізу коду та потоку даних.

Динамічний аналіз у свою чергу повинен включати наступні кроки:

– відстеження виконання під час виконання – відстеження послідовності інструкцій, які виконуються під час певного виконання коду;

– Fuzzing Input Generation [39] – Фаззінг – це автоматизований метод аналізу, який перевіряє виконання програми, надаючи структуровані дані як вхідні дані для комп’ютерної програми. Потім аналізується програма відстежується на предмет неочікуваної поведінки, наприклад, незвичайного шляху коду або збоїв.

2.4 Підґрунтя створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини

Після створення системи моніторингу потрібно продумати резервування/дублювання системи, як наступний крок для підвищення рівня зрілості безпеки впровадженої системи. Дублювання буде використовуватись, як метод підвищення надійності ІКС за рахунок використання додаткових елементів та функціональних можливостей понад мінімально необхідних для нормальної роботи/виконання заданих завдань.

Система потрібно представити із ряду ступенів, де кожен виконую свої окремі функції. Завдання резервування наддасть змогу знайти мінімальну/оптимальну кількість дублюючих компонентів для кожної ступені, яке буде забезпечувати заданий рівень надійності системи при найменшої вартості. Для резервування потрібно встановити певні вимоги/рекомендації, щоб цей процес був повний:

– з точки зору структури системи, повинно врахувати використання надлишкових елементів, що входять до фізичної структури системи. Забезпечується підключенням до основної структури резервної так, щоб при відмові основної елементів резервна продовжувала виконувати її функції;

– з точки зору функціональності, повинно враховувати використання здібності елементів виконувати додаткові функції замість основних та поряд з ними;

– з точки зору часу, повинно використовувати надлишкового часу, виділеного на виконання завдань. Інакше кажучи, тимчасове резервування - таке планування роботи системи, у якому створюється резерв робочого дня виконання заданих функцій. Резервний час може бути використаний для повторення операції, або для усунення несправності елемента системи;

– з точки зору інформування, повинно передбачати використання надмірної інформації понад мінімально необхідну виконання завдань;

– з точки зору навантажування, потрібно передбачати використання можливості його елементів приймати додаткові навантаження понад номінальних. З позицій розрахунку та забезпечення надійності технічних систем необхідно розглядати структурне резервування.

Сам факт створення всеукраїнської системи моніторингу на рівні держави дасть змогу заробити репутацію на рівні суспільства, тому її функції у подальшому можна буде використовувати в інших галузях (діяльність у сфері статистики та соціології; медична практика; діяльність центрів з нагляду за дорослими, що страждають фізичними чи розумовими вадами; діяльність щодо безпеки населення в надзвичайних ситуаціях тощо).

2.5 Висновки до другого розділу

У розділі було розглянуто концептуальних положень стосовно застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань.

Було запропоновано низка принципів:

- принцип контролю;
- принцип контролю обробки інформації;
- принцип мінімізації даних;
- принцип обмеження розкриття/доступу даних;
- принцип забезпечення точних цілей обробки;
- принцип встановлення жорстких обмежень на зберігання даних;
- принцип забезпечення даних;
- принцип забезпечення точності даних;
- принцип Залучення органів із захисту даних,

яким потрібно врахувати підчас розробки системи моніторингу інфекційних захворювань.

Було проаналізовані аспекти, які потрібно врахувати під час розробки подібної системи моніторингу, а саме – специфічні вразливості децентралізованого рішення на основі блокчейну, інструменти та методики для аналізу програмного коду; та запропоновані механізми захисту та інструменти/підходи моніторингу функціоналу рішення на основі блокчейну.

Також було розглянуто можливість створення дублюючої системи, як наступний крок після отримання досвіду створення децентралізованої системи на рівні держави дасть змогу виявити критичні місця та підготує базу для створення системи електронного голосування різних рівнів – від місцевих виборів до виборів президента України.

3 ЗБІР, АНАЛІЗ ТА СИСТЕМАТИЗАЦІЯ СТАТИСТИЧНИХ ДАНИХ ЩОДО СТАНУ МЕРЕЖІ, ХАРАКТЕРИСТИК ТРАФІКУ, ПОВЕДІНКИ КОРИСТУВАЧІВ У РІЗНИХ РЕЖИМАХ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

В області мережної безпеки вторгнення визначається як набір зловмисних дій проти цілісності, конфіденційності та доступності інформації в системі або мережі, які роблять її уразливою для майбутніх атак [41, 42]. Для протидії таким загрозам розгортаються системи виявлення вторгнень для виявлення та ідентифікації спроб вторгнення в систему або мережу [43-45]. Використовуючи набір апаратних і програмних ресурсів, системи виявлення вторгнень (СВВ) намагається виявити вторгнення, відстежуючи дані, зібрані з одного хоста або мережі, і генерувати тривогу в разі виявлення спроб вторгнення [46, 47]. Системи виявлення вторгнень можна розділити на різні категорії залежно від джерела інформації і техніки виявлення.

Швидкий розвиток комп'ютерних мереж та інформаційних технологій породжує ряд проблем, пов'язаних з безпекою мережних ресурсів, які вимагають нових підходів. Сьогодні питання побудови систем виявлення атак є актуальною тенденцією в області інформаційних технологій [48, 49]. Є багато робіт, присвячених темі виявлення і класифікації атак з використанням різних методів, які включають традиційні підходи, засновані на відповідність шаблонами сигнатур і адаптивним моделям з використанням методів інтелектуального аналізу даних [42, 50].

3.1 Порівняння наборів даних датасетів та їхня обробка

Основною проблемою в ході тестування можливостей СВВ є потреба в репрезентативному стандартному наборі даних, який дозволяє порівнювати різні методи [41-44]. MIT Lincoln Lab в 90-х роках випустила добре відомі набори даних DARPA'98 і DARPA'99. Багато інших дослідників і проекти з тих пір

намагалися надати поліпшені версії цих наборів даних, наприклад, NSL-KDD, або створення нових наборів даних. Однак всі набори даних мають деякі обмеження, такі як наявність дубльованих записів, незбалансовані зразки атак і нормальних з’єднань, а також властиві обмеження для розгляду синтетичного трафіка, відсутність реального трафіку, оновлених стратегій атак, обмеження, пов’язане з тривалістю запису даних [45].

3.1.1 Набори даних

Розглядатимемо тільки ті набори даних, які містять мітки, що вказують, присутні атаки чи ні. Існують інші немарковані набори даних трафіка, які широко використовуються для інших цілей, наприклад, набори даних CAIDA, але їхнє застосування в області оцінки СВВ обмежено [41-45].

Набори даних DARPA. Як зазначалося раніше, перша спроба створити набір даних для оцінки СВВ була зроблена лабораторією MIT Lincoln Lab. Ці набори даних відомі як набори даних DARPA: DARPA'98 і DARPA'99.

DARPA'98 складається з 4 ГБ стислих необроблених (довічних) даних tcpdump, які охоплюють 7 тижнів синтетичного мережного трафіка з 5 МБ записів з’єднань. Тестові дані включають в себе два тижні трафіку і близько двох мільйонів записів про з’єднання. DARPA'99 містить 5 тижнів файлів мережного трафіка tcpdump, виявлених в двох різних точках синтетичної мережі (одна всередині мережі, а інша зовні). Дані аудиту на основі хоста також збираються з чотирьох систем-жертв.

Набір даних KDDCup'99. Цей набір даних був підготовлений для конкурсу KDD'99. Він побудований на основі набору даних DARPA'98 і складається з 4,9 млн. одиночних векторів підключення, кожен з яких має 41 функціональність, позначену як нормальна або атакуюча з однією з таких категорій: DoS, root-користувач (U2R), віддалений (локальний) (R2L) і зондування атаки. Існує 24 типи тренувальних атак з додатковим набором з 14 різних атак, які відображаються тільки в даних тесту. Особливості, виділені, були отримані як

кілька класів: а) основні характеристики TCP-з’єднань (наприклад, тривалість, # байти, прапорці TCP, номер порту і т. ін.); б) характеристики трафіку, отримані з ковзаючого вікна часу довжиною дві секунди, і враховують з’єднання, спрямовані на один і той самий хост або ту саму послугу (наприклад, # з’єднання до того самого хосту, що і поточне з’єднання в останні дві секунди); в) особливості контенту, витягнуті з інформації корисного навантаження, наприклад, кількість невдалих спроб входу в систему.

Покращення в наборах даних DARPA. McHugh та його колеги провели великий аналіз наборів даних DARPA, зробивши висновок, що дані про трафік не мають статистичних доказів подібності з типовим мережним трафіком ВВС, низькими швидкостями трафіка, відносно рівномірним розподілом чотирьох основних категорій атак, спотворених розподілом хостів-жертв і топологією плоскою мережі.

Автори роботи [43] заявили, що набір даних DARPA'99 становить статистичні проблеми, тобто вони виявили наявність артефактів, які можуть дозволити системі виявлення мережних аномалій виявляти деякі нові вторгнення, засновані на ідіосинкразії базової реалізації моделювання, з штучно низьким хибним рівнем тривоги. На основі цих досліджень створено набір даних NSL-KDD [44]. З вихідного набору даних вони виключили величезну кількість надлишкових записів, присутніх у вихідних даних, і застосували методологію для підвищення рівня складності записів у наборі даних. Інші автори також запропонували додаткові розширення, де набір даних gureKDDCup був побудований як розширення KDDCup '99, в якому інформація про з’єднання, пов’язані з корисним навантаженням, була оброблена з DARPA'98 і включена в набір даних [44].

Хоча багато поточних досліджень в області СВВ все ще використовують ці цитовані набори еталонних даних, через критиків і вже згадані проблеми, багато інших дослідників створили нові оновлені набори даних. Основними мотивами в цих наборах даних є або надання різних типів даних, наприклад, дані, що належать до більш оновлених загроз, таким як бот-мережі, або до збору

трафіка, який більш реалістичний в сучасних мережах, у рамках гіпотези про те, що функції трафіка в поточному Інтернеті еволюціонували з часів збору наборів даних DARPA.

Деякі набори даних створені протягом останніх років, у хронологічному порядку наведено нижче.

Сперотто. Поточний набір даних 2008 року був створений [41, 46]. Набір даних складається з позначеного несинтетичного трафіка. Його основне обмеження в тому, що обсяг зібраного трафіка зменшується, а топологія дуже спрощена, в основному через те, що з причин продуктивності вони контролюють один хост (honeypot), підключений до мережі університету. Автори стверджують, що розміру набору достатньо, але він триває всього шість днів, що не дозволяє тестувати алгоритми, засновані на добових і тижневих схемах зміни трафіка. Маркування в цьому наборі даних виконується на основі журналів з системи honeypot, що робить його залежним від конфігурації системи виявлення та обробки журналів. Набір даних доступний тільки на вимогу поштою авторам.

Набір даних робочої лабораторії MAWI. Цей набір даних [46] було додано з 2010 року як маркована версія архівного зразка MAWI (вимірювання та аналіз в Інтернеті) для вузлів мережі. У архіві містяться щоденні трасування tcpdump протягом 15 хвилин, отримані зі з’єднання між Японією і Сполученими Штатами. Хоча архів містить трафік з 2001 року, позначений тільки трафік з 2007 року. Мітки генеруються з використанням комбінації декількох класифікаторів виявлення аномалій. Цей набір даних дійсно великий і дозволяє проводити аналіз протягом дуже тривалого періоду. Основним обмеженням є те, що трасування виходить тільки протягом 15-хвилинного періоду в день. Крім того, маркування залежить від класифікаторів, які використовувалися в процесі, і від їхньої генерації помилкових спрацьовувань.

UNB ISCX 2012. Цей набір даних був створений Shiravi та його колегами. Найбільш значущим внеском цієї роботи є використання профілів для генерації трафіку. Автори визначають профілі для трафіка атаки і профілі для фонового трафіку. Вони реалізують свою пропозицію в мережі з 17 станціями Windows XP

і одним комп’ютером з Windows 7, збираючи дані протягом 7 днів. Сьогодні основними недоліками цього набору даних є його тривалість, використання якихось старих операційних систем (Windows XP) і використання синтетичного трафіка.

CTU-13. Цей набір даних складається з 13 різних захоплень шкідливих програм у реальному мережному середовищі, включаючи позначений ботнет, звичайний і фоновий трафік, де фон означає, що автори не можуть в дійсності визначити, чи є він шкідливим чи ні. Щодо виду наданої інформації, трасування потоку доступні в декількох форматах. З міркувань конфіденційності файли pcap пропонуються тільки в тому випадку, якщо інформація про мережу відсутня, наприклад, один хост з синтетичним трафіком. Існує багато різних короткочасних захоплень, які охоплюють період з 2013 по 2016 рік, хоча єдиний набір даних, який добре документований, відповідає 2013 року. Основне обмеження полягає в короткій тривалості трафіку, що перешкоджає побудові моделей, які враховують циклостаціонарну еволюцію. Інше обмеження стосується фонового трафіка. Автори кажуть, що він отриманий з університетського роутера, але ніяких подробиць щодо топології або послуги надано не було. Що стосується трафіку атаки, цей набір даних орієнтований на поведінку 13 сценаріїв ботнетів, де шкідливі програми знаходяться на комп’ютерах з Windows XP. Незважаючи на ці проблеми, цей набір даних є дійсно гарним для захоплення реального трафіка, хоча його застосування звужується до визначення поведінки ботнету.

ADFA-LD12 (2013). В цьому наборі даних основна увага приділяється системі виявлення вторгнень хоста (НСВВ). Кілька атак робляться на комп’ютер з ОС Linux (Ubuntu 11.04), наприклад, злом паролів щодо FTP і SSH, атак на стороні клієнта, корисних навантажень на основі Java, атак на php RFI і т. ін. Крім того, використовуються сучасні методики злому, в тому числі використання таких середовищ атак, як Metasploit. Трафік збирається за допомогою інструменту аудиту Unix. Основна проблема з цим набором даних пов’язана з нормальною поведінкою. Тут розглядається тільки один комп’ютер (з ОС Linux),

і взагалі немає опису встановлених служб і програмного забезпечення. Таким чином, неможливо взяти його за основу, щоб узагальнити поведінку інших машин в Інтернеті.

UNSW-NB15. Автори цього набору даних використовували інструмент автоматичної генерації атак під назвою IXIA PerfectStorm для реалізації дев'яти типів реальних і оновлених атак на кілька серверів. Вони зібрали tcpdump дані мережного трафіку, загальною тривалістю 31 годину на початку 2015 року (2M потоків). З цих даних був побудований набір даних з 49 об'єктів для кожного потоку. Основна проблема з цим набором даних – синтетична генерація трафіка, яка пов'язана з теоретичною, а не з реалістичною поведінкою в Інтернеті.

Набори даних для конкретного додатка.

UGR'16 [43]. Для набору даних, з яким працюєш, особливо важливо мати як реалістичний фон, так і трафік атаки. Тривалість набору даних достатня для навчання моделей, що враховують нестаціонарні періоди. Для дотримання вимог конфіденційності дані надаються в анонімному форматі.

3.1.2 Вимоги до наборів даних для оцінки СВВ

Основні набори даних були проаналізовані в роботах [43, 44] і визначені набори бажаних особливостей для ідеального набору даних для оцінки СВВ. Таким чином існують такі вимоги:

1. Ознаки: набори даних можуть включати в себе мережні і / або хост-функції. Мережні функції зазвичай підсумовуються для кожного потоку і включають такі характеристики, як тривалість потоку, часові мітки, кількість байтів і пакетів, прапорці, IP-адреси і номери портів, середній час між пакетами і т.ін. Що стосується функцій хоста, деякі приклади використовуються в попередніх наборах даних: число невдалих спроб входу в систему або прапорців, що вказують на певні умови, наприклад, якщо отримана коренева оболонка або, якщо зловмисник успішно увійшов в систему. Для навчання аномалій мережної СВВ необхідні мережні ознаки, в той час як характеристики хоста зазвичай

використовуються для навчання аномалій хоста. Деякі набори даних включають обидва набору ознак, що дозволяє навчати обидва типи СВВ. Обраний набір даних має містити відповідні ознаки для типу СВВ, що підлягає навчанню та тестуванню. У будь-якому випадку бажано, щоб дані передавалися в необробленому форматі в міру їх отримання з мережі. Таким чином, дослідники можуть використовувати свої власні ознаки за бажанням.

2. Реальний фоновий трафік: набір даних має містити реальний трафік. Це особливо важливо для фонового трафіка, оскільки синтетичне генерування мережного трафіка може призвести до неправильних моделей нормальної поведінки і некоректного поводження.

3. Оновлений трафік атаки: набори даних для оцінки СВВ мають містити реалістичні екземпляри атаки, оновлені за допомогою найсучасніших методів та інструментів атаки.

4. Маркування: в ідеалі різні записи в наборі даних повинні бути правильно позначені як шкідливі чи ні. У разі записів про атаки також необхідний тип атаки. Як вказано далі, процес маркування становить багато труднощів.

5. Тривалість: набори даних мають охоплювати кілька циклів навчання (дні або тижні), щоб можна було враховувати циклостаціонарну еволюцію руху в денний / нічний час, а також у будні / вихідні дні і навіть в різні місяці.

6. Документація: докладний опис набору даних необхідний для розуміння його обмежень і можливостей. Деякі з опублікованих наборів даних не надають досить повної інформації.

7) Формат: набори даних зазвичай включають інформацію у форматі pcap (tcpdump), csv або flow (netflow). Формат pcap дозволяє більш всебічно оцінити СВВ, головним чином завдяки тому, що в інформацію включені корисні дані. У форматі csv, з іншого боку, є попередня обробка інформації pcap і витяг відповідних записів для різних функцій. Включення інформації про корисне навантаження зазвичай має на увазі проблему з точки зору конфіденційності, оскільки складно надійно анонімізувати трасування. З цієї причини інформація про потік, наприклад, формат netflow іноді кращий під час роботи з реальним

трафіком, тоді як формати pcap / csv надаються в наборах даних імітованого / синтетичного трафіка. Нарешті, обсяг даних безпосередньо пов'язаний з форматом. Отже, формат потоку здається більш відповідним для наборів даних з великою тривалістю, оскільки формат pcap генеруватиме величезний обсяг даних у цьому випадку.

3.1.3 Порівняння існуючих наборів даних

Таблиця 3.1 містить порівняння різних наборів даних, розглянутих вище. Тут аналізуються різні вимоги, описані раніше, і оцінюється, чи відповідають їм різні набори даних. По-перше, необхідно постійно оновлювати як фоновий, так і атакуючий трафік, і тому періодично потрібні нові набори даних.

Таблиця 3.1 – Порівняння датасетів для СВВ

	СВВ М:мережна Х:хоста	Засновано на реальному трафіку	Оновлювальні атаки	Маркування	Тривалість
guretKDDCup'08	M	-	-	+	+
NSL-KDD'09	M	-	-	+	+
Darpa'98/99	M	-	-	+	+
KDDcup99	M	-	-	+	+
Sperotto'2008	M	+-	+	+	-
MAWILab'2010	M	+	+	+-	+
UNB ISCX'2012	M	-	+	+	+
ADFA-2013	X	+-	+	+	+
CTU-2013	M	+-	+	+-	+-
UNSW-NB15	M	-	+	+	+
UGR'16	M	+	+	+-	+

Проте, існує рішення засноване на побудові моделей трафіка, і немає ніяких гарантій, що реальний трафік у найближчому майбутньому слідуватиме цими моделями. Це означає, що еталонні набори даних, які були дійсно корисні протягом багатьох років, більше не дійсні. По-друге, видно, що в останніх наборах даних були зроблені великі зусилля для розгортання реалістичних даних про атаки, в основному з використанням потужних хакерських середовищ і

стандартних інструментів. Навпаки, недостатні зусилля були зроблені для забезпечення реалістичного фонового трафіка.

Основним обмеженням тут є проблема конфіденційності. З цієї причини деякі набори даних, які відстежують реальний трафік, наприклад, CTU-13, надає тільки інформацію про потік і приховує корисні дані. Нарешті, основна проблема останніх наборів даних з точки зору тверджень, які ми робимо, пов'язана з тривалістю слідів. Якщо проводити оцінку СВВ, яка будує моделі нормальності з урахуванням еволюції трафіка в нестаціонарні періоди (день / ніч, будні / вихідні або навіть в різні місяці), існуючі набори даних надають тільки дуже обмежену інформацію.

Для набору даних, який описаний в [45], було особливо важливо зібрати реалістичний фон, так і трафік атаки. Для маркування використовується модифікований підхід, щоб зберегти баланс між забезпеченням повного маркування синтетичним трафіком і реалістичним трафіком. Тривалості набору даних достатньо для навчання моделей, що враховують нестаціонарні періоди. Для дотримання вимог конфіденційності дані надаються в анонімізованому форматі.

3.2 Аналіз параметрів безпеки та якості обслуговування мережі

У сучасних умовах одним з основних процесів управління телекомунікаційною мережею (ТКМ) є процес управління її інформаційною безпекою (ІБ). Даний процес має бути як на етапі проектування мережі, так і на етапі її функціонування, і складається із постійного аналізу стану мережі. На реалізацію даного процесу значною мірою впливає можливість зміни структури, топології і режимів роботи ТКМ у процесі її функціонування. Така ситуація може мати місце внаслідок додавання нових пристроїв у мережу або зміни налаштувань вже діючих механізмів, поломок устаткування, неправильних дій адміністраторів мережі, користувачів і т. ін.

Під час аналізу стану мережі основними з оцінюваних параметрів є ймовірність атаки, ступінь (ймовірність) уразливості елементів мережі до інформаційних атак. [51]

Аналітики з безпеки, які перевіряють результати роботи СВВ, хотіли б знати ймовірність того, що за певних видів атак з'являться попередження. Нарешті, дослідникам необхідно розуміти сильні і слабкі сторони існуючих на сьогодні систем, щоб вони могли ефективно сфокусувати дослідницькі зусилля на вдосконаленні систем і вимірювати їхній прогрес.

3.2.1 Кількісно-вимірні характеристики СВВ

Наведемо деякі вимірювання, які можуть бути виконані у СВВ [52]. Особливу увагу ми приділяємо кількісним вимірам, пов'язаних з точністю виявлення.

Охоплення. Це вимірювання визначає, які атаки СВВ може виявити в ідеальних умовах. Для систем, що базуються на підписах, це було б просто підрахувати кількість підписів та зіставити їх за стандартною схемою іменування. Для систем, що не базуються на підписах, потрібно було б визначити, які атаки з набору всіх відомих атак можуть бути виявлені певною методикою.

Імовірність помилкової тривоги. Це вимірювання визначає частоту помилкових спрацьовувань СВВ у даному середовищі протягом певного періоду часу. Хибнопозитивні спрацьовування або помилкова тривога – це сигнал тривоги, викликаний звичайним безпечним фоновим трафіком. Вимірювання помилкових спрацьовувань складне, оскільки СВВ може мати різну частоту помилкових спрацьовувань в кожному мережному середовищі і не існує «стандартної» мережі. Крім того, важко визначити аспекти мережного трафіка або активності хоста, які можуть викликати помилкові тривоги.

Ймовірність виявлення атак. Це вимірювання визначає частку атак, правильно виявлених СВВ у даному середовищі протягом певного періоду часу.

Труднощі вимірювання ступеня виявлення полягають у тому, що успіх СВВ значною мірою залежить від набору атак, які використовуються під час тестування. Крім того, ймовірність виявлення різниться залежно від частоти хибно-позитивних спрацьовувань, і СВВ може бути налаштована на користь можливості виявлення атак або зведення до мінімуму хибнопозитивних спрацьовувань. Під час тестування на наявність помилкових спрацьовувань і частоту попадань слід з обережністю використовувати одну і ту саму конфігурацію [53].

Опір атакам, направлених на СВВ. Це вимірювання демонструє, наскільки стійка СВВ до спроби зловмисника порушити правильну роботу СВВ [54]. Атаки проти СВВ можуть мати такі форми:

1. Надсилання великої кількості легального трафіка, об’єм якого перевищує можливості обробки СВВ. Занадто багато трафіка для обробки, то ж СВВ може скидати пакети і не в змозі виявити атаки.

2. Відправлення легальних пакетів на СВВ, які спеціально створені для запуску багатьох підписів всередині СВВ, тим самим переповнюючи систему сповіщення хибнопозитивними спрацьовуваннями СВВ або збоєм інструментів для обробки або виведення сповіщень.

3. Відправлення на СВВ великої кількості пакетів атак, призначених для відволікання адміністратора мережі від СВВ, в той час як зловмисник проводить справжню атаку, приховану під «димовим екраном», створеним множиною інших атак.

4. Відправлення пакетів у СВВ, що містять дані, які використовують уразливість в алгоритмах обробки СВВ. Такі атаки будуть успішними лише в тому випадку, якщо СВВ містить відому помилку кодування, яку може використовувати нападник.

5. Можливість обробки трафіка з високою інтенсивністю трафіка. Це вимірювання демонструє, наскільки добре СВВ функціонуватиме з великим обсягом трафіка. Більшість мережних СВВ почнуть скидати пакети в міру збільшення обсягу трафіка, тим самим змушуючи СВВ пропустити деякий

відсоток атак. При певному порозі більшість СВВ припинить виявлення будь-яких атак. Це вимірювання майже ідентичне «вимірюванню стійкості до відмови в обслуговуванні», коли зловмисник надсилає велику кількість легітимного трафіка на СВВ. Єдина відмінність у тому, що це вимірювання обчислює здатність СВВ обробляти певні обсяги нормального фонового трафіка.

6. Можливість співвідносити події. Це вимірювання демонструє, наскільки добре СВВ корелює події атаки. Ці події можуть бути зібрані з СВВ, маршрутизаторів, брандмауерів, журналів додатків або з множини інших пристроїв. Однією з головних цілей цього співвідношення є виявлення поетапних атак проникнення. Наразі СВВ мають лише обмежені можливості у цій галузі.

7. Здатність виявляти ніколи раніше не бачені напади, атаки «нульового дня». Це вимірювання демонструє, наскільки добре СВВ може виявляти напади, які раніше не відбувалися. Для комерційних систем, як правило, не корисно проводити це вимірювання, оскільки їхня технологія на основі підпису може виявляти напади, що відбувалися раніше (за кількома винятками). Однак дослідницькі системи, засновані на виявленні аномалії або на основі специфікації, можуть бути придатними для такого типу вимірювань. Зазвичай системи виявлення атак «нульового дня», дають більше хибнопозитивних результатів, ніж ті, у яких немає цієї функції.

8. Можливість ідентифікації атак. Це вимірювання показує, наскільки добре СВВ може ідентифікувати атаку, яку вона виявила, позначаючи кожну атаку загальним іменем або іменем уразливості або присвоюючи атаці категорію.

9. Можливість визначення успіху в атаці. Це вимірювання показує, чи може СВВ визначати успіх атак з віддалених сайтів, які надають зловмиснику привілеї вищого рівня для атакованої системи. У сучасних мережних середовищах багато віддалених атак (або зондів), які отримують привілеї, виходять з ладу і не пошкоджують атаковану систему. Однак багато СВВ не відрізняють невдалі від успішних атак. Для тієї ж атаки деякі СВВ можуть виявити докази пошкоджень (успіх нападу), а деякі СВВ виявляють лише підпис

дій атаки (без вказівки, успішна атака чи ні). Здатність визначати успіх атаки є важливою для аналізу кореляції атаки та сценарію атаки; це також значно спрощує роботу аналітика, розрізняючи більш важливі успішні атаки та, як правило, менш згубні невдалі атаки. Вимірювання цієї можливості вимагає інформації про невдалі атаки, а також про успішні атаки.

10. Перевірка ємності для мережних СВВ. Мережна СВВ вимагає поінформованості протоколів вищого рівня, ніж інші мережні пристрої, такі як комутатори та маршрутизатори; вона має можливість перевірки глибшого рівня мережних пакетів. Тому важливо виміряти здатність мережної СВВ захоплювати, обробляти та виконувати дії на тому ж рівні точності під час заданого навантаження мережі, як це відбувається у спокійній мережі. Наприклад, Холл запропонував методологію тестування та показники трафіка для стандартизованої оцінки потенціалу щодо мережної СВВ. Потім клієнти мережної СВВ можуть використовувати стандартизовані результати тестування потужностей для кожної метрики та профілю їхніх мереж, щоб визначити, чи здатна мережна СВВ навіть підтримувати перевірку трафіка.

11. Продуктивність. Під час розгляду мережних технологій наведемо ключові структури і властивості, пов’язані з продуктивністю мережі.

Топологія: існують фізичні та логічні топології. Фізична топологія – схема розташування кабелів, мережних пристроїв і кінцевих систем. У ній описується, як мережні пристрої з’єднані між собою за допомогою проводів і кабелів. Логічна топологія – це шлях, за яким дані передаються у мережі. У ній описується, як користувачі бачать з’єднання мережних пристроїв.

Швидкість – це кількість переданих даних за будь-якими каналами мережі, яка вимірюється в бітах за секунду (біт/с).

Вартість вказує загальні витрати на придбання компонентів мережі, встановлення та обслуговування мережі.

Безпека вказує на ступінь захищеності мережі, в тому числі захищеності інформації, що передається в мережі. Фактор безпеки відіграє дуже важливу роль, тому технології та методи забезпечення безпеки постійно розвиваються. За

будь-яких дій, які можуть вплинути на роботу мережі, необхідно звертати увагу на забезпечення безпеки.

Доступність вказує на можливість використання мережі в момент звернення користувача.

Масштабованість показує, наскільки легко мережа може вміщати більшу кількість користувачів і відповідати вимогам передачі даних. Якщо проект мережі оптимізований тільки для виконання поточних завдань, то розширення мережі для відповідності зростаючим вимогам тягне за собою великі труднощі і високі витрати.

Надійність вказує на ступінь безвідмовності компонентів, з яких складається мережа: маршрутизаторів, комутаторів, комп’ютерів і серверів. Надійність часто вимірюється як ймовірність збою або як середній час безвідмовної роботи.

3.2.2 Часові та якісні показники роботи мережі

Ці характеристики і властивості забезпечують способи для порівняння різних мережних рішень. В роботі [51, 56] показник мережної безпеки може дати дані, які піддаються кількісній оцінці та які допоможуть фахівцям з безпеки забезпечити безпеку комп’ютерних мереж. Однак дослідження показників безпеки, засновані на графі атак, не застосовні до характеристик внутрішніх атак, тому автори пропонують метод вимірювання безпеки внутрішньої мережі, заснований на ймовірності атаки. Переваги їхнього підходу полягають у тому, що: передбачений метод спрощення графіка атаки з моніторингом вузла подій, який дозволяє вирішити проблему експоненціального зростання графу атаки зі збільшенням розміру мережі, одночасно знижуючи маскування внутрішніх атак і підвищуючи ефективність всього методу; метод розрахунку ймовірності атаки на основі спрощеного графу дозволяє спростити складність внутрішніх атак і підвищити точність підходу.

Результати проведеного аналізу показали, що існує множина показників якості роботи мережі та систем виявлення вторгнень і можна обрати ті показники, які найкраще підходять для кожного методу управління самоподібним трафіком та СВВ [49, 57].

3.3 Оцінка характеристик ефективності виявлення вторгнень

3.3.1 Класи методів інтерпретації даних

Можна виділити такі класи, кожен з яких може включати кілька методів:

– методи виявлення відомих порушень;
– методи виявлення аномалій;
– змішаний метод, що включає обидва вищеназвані.

3.3.2 Методи виявлення відомих порушень

Методи виявлення відомих порушень зводяться до пошуку ознак вже відомих атак. Переваги: методи майже не схильні до помилкових спрацьовувань; методи, реалізовані як зіставлення зі зразком, як правило виконуються досить швидко і не вимагають великих витрат ресурсів. Недоліком цих методів є неможливість виявляти невідомі системі атаки.

У класичному варіанті реалізація передбачає порівняння сигнатур пакетів з сигнатурами в базі. Порівняння може бути, як точне, так і з шаблоном або за регулярним виразом. Більшість відомих СВВ використовують методи даного класу. Сюди ж належать методи нечіткого порівняння: навчений перцептрон; методи порівняння з нечіткою логікою.

3.3.3 Виявлення аномалій

Суть в тому, щоб записати шаблон нормальної активності мережі та реагувати на відхилення від цього шаблону.

Можливий варіант реалізації у вигляді бази сигнатур "нормальних" пакетів у мережі і статистичної системи виявлення відхилень, коли аналізатор шукає якісь рідкісні дії, або активності. Події в системі досліджуються статистично, щоб знайти ті з них, прояв яких виглядає аномальним.

3.3.4 Методи представлення результату

Як показав аналіз існуючих рішень, зазвичай використовуються два типи методів:

– Двокласовий (бінарний). Система відповідає на запитання «Чи є проблеми?», Відповіддю «так / ні». Даний спосіб характерний для академічних статей і досліджень, але він може бути застосовний для написання модулів або датчиків реальних СВВ.

– Багатокласовий. Система відповідає на запитання «Які зараз є проблеми?». Якщо проблем немає, то «ніякі». Результат також може бути поданий з певним рівнем достовірності. І будь-яка нейромережа надає результат, не як «так» або «ні», а як множину ймовірностей результатів. В існуючих підходах ймовірність апроксимується до одиничної або нульової (наприклад, з усіх можливих атак на виході мережі, вибирається перша з найвищою ймовірністю) і ніде далі не враховується.

3.4 Аналіз методів виявлення вторгнень

З урахуванням методів виявлення вторгнень СВВ можна розділити на два основних типи систем: на основі сигнатур і аномалій [49, 58].

3.4.1 Метод аналізу аномалій

СВВ на основі аномалій створюють профіль, відстежуючи нормальну активність в системі [50, 59, 60]. Цей профіль використовується, щоб знайти

відхилення спостережуваних дій від нормальної поведінки системи і повідомити про них як про аномалії. У системах такого типу дуже важливо правильно визначити нормальний профіль системи в автономному режимі або в режимі онлайн [51, 54]. В іншому випадку будь-яка активність, яка відрізняється від створеного профілю, може бути ідентифікована як вторгнення, і, отже, система може страждати від високого рівня помилкових спрацьовувань, який викликаний маркуванням будь-якої неінтрузивної ненормальної поведінки як шкідливої. На відміну від систем на основі сигнатур, системи на основі аномалій здатні виявляти нові типи атак.

Система виявлення вторгнень, яка використовує методи виявлення аномалій для виявлення зловмисних дій, називається системою виявлення аномалій. Системи виявлення аномалій побудовані на основі припущення, що вторгнення є підмножиною аномалій [50]. В ідеальному випадку кожна виявлена аномалія фактично є вторгненням, що означає відсутність в системі помилкових спрацьовувань. Відповідно до цього припущення, системи виявлення аномалій здатні виявляти нав'язливі дії, навіть якщо атаки запускаються з законного облікового запису користувача. Однак основним недоліком систем виявлення аномалій є висока частота помилкових спрацьовувань, що виникають під час спостереження за будь-якою законною ненормальною активністю в контрольованій системі або мережі. У реальних додатках тягар помилкових спрацьовувань може призвести до збою СВВ [47, 52]. З іншого боку, в ході виявлення аномальних дій системний адміністратор повинен витратити багато часу на виявлення першопричини згенерованих аварійних сигналів [57, 60]. Зі збільшенням кількості аварійних сигналів системний адміністратор може не мати можливості відслідковувати всі ініційовані попередження або може просто відключити генератор аварійних сигналів. Отже, ряд дійсних сигналів тривоги може бути втрачений серед великої кількості помилкових сигналів в системному трафіку.

Загальний процес системи виявлення аномалій можна розділити на дві фази: навчання і тестування. На етапі навчання нормальний профіль системи

будується СВВ. Цей профіль становить нормальну поведінку системи в термінах певних характеристик і метрик. На етапі тестування СВВ відстежує поточні дії системи або мережі і намагається знайти відхилення, порівнюючи навчений профіль з новими даними [48, 51, 53]. Системи виявлення аномалій можуть використовувати різні методи щодо доступних функцій даних. До них належать методи на основі статистики і машинного навчання.

3.4.2 Метод заснований на аналізі статистичних даних

У методах, заснованих на статистиці, система підтримує два профілі для нормальної і поточної поведінки системи або мережі. У кожному з цих профілів поведінка системи моделюється шляхом розрахунку деяких статистичних показників, таких як середнє значення, стандартне відхилення, розподіл даних і т. ін. [44, 55, 59]. Коли в системі або мережі запускається новий набір дій, СВВ намагається знайти відхилення між двома профілями відповідно до згаданих мір. Використовуючи деякі статистичні тести, система обчислює показник аномалії для поточного профілю, який показує ступінь відхилення від норми. Якщо оцінка аномалії вище певного порогу, система викликає тривогу як ознаку аномалії [48].

Методи, засновані на статистиці, мають ряд переваг. По-перше, вони не мають потреби в будь-яких попередніх знаннях про систему або мережу, оскільки нормальний профіль може бути створений тільки шляхом спостереження за діями в системі протягом певного періоду часу. Крім того, оскільки ці підходи використовують статистичні моделі, вони особливо ефективні під час виявлення атак, що відбуваються протягом тривалих періодів часу [59]. З іншого боку, засновані на статистиці підходи, мають два основних недоліки. У цих методах зловмисник може навчити систему, щоб можна було припустити, що нав'язлива поведінка є нормальною. Більш того, основним принципом цих підходів є моделювання точок даних як стохастичних розподілів, які передбачають квазістаціонарний процес [46].

3.4.3 Методи машинного навчання

У підходах, заснованих на машинному навчанні, система намагається вивчити шаблони даних і побудувати модель для класифікації аналізованих моделей [47, 55]. Використовуючи цю модель, системи виявлення аномалій, засновані на машинному навчанні, можуть поліпшити свої характеристики відповідно до попередніх результатів. Техніки, засновані на машинному навчанні [53, 56, 57], можуть використовувати навчання під наглядом або без нього. У контрольованому навчанні набір помічених даних використовується системою на етапі навчання. Кожен ярлик є класом дій, таких як шкідливі або звичайні. Після створення моделі на основі характеристик даних і відповідних їм міток система здатна робити прогнози для класифікації нових даних, доступних на етапі тестування.

З іншого боку, під час навчання без учителя доступний набір даних не позначається. У цьому методі система намагається проаналізувати структуру даних й ідентифікувати подібні точки даних, що робить його досить ефективним у вирішенні проблем кластеризації. Переваги і недоліки методів виявлення вторгнень наведено в таблиці 3.2.

Таким чином всі наведені методи управління трафіком і СВВ можна об’єднати в концепцію універсалізації та централізації аналізу трафіка і стану мережі при використанні СВВ шляхом розвитку засобів DPI / DCI. Дана концепція може бути позначена як «DPI як сервіс» – під цією назвою вона була наведена в роботі [56]. Суть концепції в тому, що якщо в мережі використовується велика кількість різних засобів, що реалізують той чи інший аналіз трафіка (міжмережні екрани, системи СВВ, оптимізатори трафіку і ін.), то є сенс винести весь аналіз в окремий пристрій. Цей пристрій виконуватиме повний розбір мережних даних і розсилатиме результати аналізу на всі пристрої залежно від їхніх потреб, а ті, в свою чергу, реалізовуватимуть тільки реакцію на дані, що надходять [58]. Перехід до цієї концепції в чомусь аналогічний переходу до програмно-конфігурованих мереж (Software Defined Networks, SDN) у питаннях управління трафіком, за якого всі рішення щодо використовуваних алгоритмів маршрутизації і рівня їхнього виконання переходять від конкретних маршрутизаторів до виділених пристроїв – SDN-контролерів. Такі підходи спрощують масштабування систем і дозволяють ефективно розширювати функціонал без додаткових робіт з інтеграції і перенастроювання додатків.

Таблиця 3.2 – Переваги і недоліки методів виявлення вторгнень

Засновані на сигнатурах (засновані на знаннях)	Засновані на аномаліях (засновані на поведінці)	Засновані на аналізі стану
Переваги: Найпростіший і ефективний метод виявлення відомих нападів. Докладний контекстний аналіз і виявлення атак шляхом зіставлення захоплених сигнатур із заздалегідь визначеними в базі знань. Висока точність виявлення відомих атак. Низька вартість обчислень. Дуже низька частота помилкових спрацьовувань. ініціюючи процедури обробки інцидентів.	**Переваги:** Здатність виявляти нові атаки або невідомі атаки. Виявляє нові і непередбачені уразливості. Менше залежить від операційної системи і сприяє виявленню випадків зловживання привілеями. Використовує статистичний тест на зібрану поведінку для виявлення вторгнення. Може знизити частоту помилкових спрацьовувань за невідомих атак.	**Переваги:** Знати і відстежувати стан протоколу. Відрізняти несподівані послідовності команд.
Засновані на сигнатурах (засновані на знаннях)	Засновані на аномаліях (засновані на поведінці)	Засновані на аналізі стану
Може відстежувати проблеми безпеки в системах,	Немає необхідності апріорі знати про недоліки в системі. Може повертатися, щоб визначити сигнатури для неправильних детекторів.	
Недоліки: Неможливо виявити нові атаки, невідомі атаки, ухилення від атак, і варіанти відомих атак. Невелике розуміння про стан і протоколи. Складно тримати сигнатури / схеми в актуальному стані. На підтримку знань йде багато часу. Висока частота помилкових спрацьовувань за невідомих атак і т.ін. Виявлення тільки тих атак, для яких вони навчені. Потрібні поновлення з сигнатурними атаками.	**Недоліки:** Слабка точність профілів через постійні зміни подій, за якими йде обчислення. Недоступність під час відновлення профілів поведінки. Потрібно більше часу для виявлення атак. Точність виявлення залежить від кількості зібраної інформації (ознак) щодо поведінки. Добре відомі атаки можуть бути не виявленими, якщо вони відповідають встановленим користувачем. Складно виявляються атаки, які повільно змінюють поведінковий профіль з часом. Висока частота помилкових спрацьовувань через фіксований розподіл профілів користувачів Висока частота хибно-негативних спрацьовувань через широко тренований алгоритм виявлення. Менш ефективний в динамічному середовищі. Потрібні великі "тренувальні комплекти" для опису нормальних моделей поведінки.	**Недоліки:** Ресурсоспоживання на відстеження і експертизу стану протоколу. Неможливо перевірити атаки, що виглядають як доброякісний протокол Поведінки. Може бути несумісний з виділеними операційними системами / точками доступу.

Концепція «DPI як сервіс» може бути ефективно реалізована в рамках систем уніфікованого управління загрозами (Unified threat management, UTM) і уніфікованого управління безпекою (Unified security management, USM). Ці системи також є відображенням тенденції централізації у вигляді об’єднання функціоналу міжмережних екранів, мережних систем СВВ / СПВ, антивірусів, VPN-серверів, фільтрів вмісту, балансування навантаження і запобігання витоків даних у рамках єдиної системи.

Проведено аналіз методів управління трафіком і СВВ, який показав що їх можна об’єднати в концепцію універсалізації та централізації аналізу трафіку і стану мережі при використанні СВВ шляхом розвитку засобів DPI / DCI. В подальшому варто використовувати концепцію DPI.

3.5 Дослідження методів аналізу протоколів з відстеженням стану

3.5.1 Аналіз мережних пакетів з урахуванням стану потоків.

Концепція аналізу протоколу з відстеженням стану проста: додати характеристики з аналізом стану в аналіз звичайного протоколу. Коли виконується аналіз протоколу, перевіряються корисні навантаження TCP і UDP, які містять такі протоколи, як DNS, FTP, HTTP і SMTP. Датчики СВВ, які виконують аналіз протоколу, розуміють, як повинен працювати кожен протокол, ґрунтуючись на RFC і реальних реалізаціях цих протоколів. Таким чином, датчик СВВ може виявити багато підозрілих значень в корисних навантаженнях додатків протоколу. Сигнатури аналізу протоколів також можуть бути розроблені для подолання спроб зловмисників приховати свої дії. Наприклад, шістнадцяткове кодування може бути використано для невеликої зміни URL-адрес, щоб вони виглядали для нас різними, але мали однакове значення для веб-серверів. Веб-сервери Microsoft IIS виконують дві операції шістнадцятирічного декодування URL-адрес перед їхньою обробкою: набір сигнатур для аналізу протоколу HTTP, який шукає спроби IIS, має також виконати дві операції

шістнадцяткового декодування, щоб він перевіряв ту саму URL-адресу, яку побачить веб- сервер IIS.

В рамках SPI підходу, програма або пристрій, який його реалізує, в момент відкриття нового з’єднання перевіряє його на відповідність заданій політиці безпеки і до закриття зберігає параметри цього з’єднання в пам’яті. За допомогою таких рішень, зокрема, здійснюється перевірка коректності з’єднання, наприклад, відсутність пакетів на відкритому мережному порті після завершення з’єднання. Реалізації SPI містяться в більшості сучасних маршрутизаторів у вигляді SPI-брандмауерів. Також ця технологія використовується в програмних міжмережних екранах, які враховують стан (stateful firewalls), компанії CheckPoint і ряді СВВ / СЗВ систем [49].

З цим підходом відслідковуються не тільки вхідні і вихідні пакети, але і стан окремих з’єднань, який зберігається в динамічних таблицях, як це зображено на рисунку 3.1. Завдяки цьому під час аналізу наступного пакета можуть враховуватися не тільки задані правила і політики по відношенню до адрес і вмісту пакетів, а й стан з’єднання, до якого належить пакет і попередніх пакетів, які до нього відносяться, а також і інших, пов’язаних з даними, з’єднань. Класичний приклад переваги брандмауера підтримує стан потоку в порівнянні з міжмережними екранами без такої підтримки - обробка FTP протоколу.

Хоча аналіз протоколу сам по собі є дуже потужним методом, він обмежується розглядом одного запиту або відповіді. Зазвичай, багато атак не можуть бути виявлені при перегляді одного запиту – атака може включати серію запитів. Кращий спосіб виявити такі атаки – додати характеристики стану в аналіз протоколу.

Коли виконується аналіз протоколу з відстеженням стану, відстежуються і аналізуються всі події в з’єднанні або сеансі. Датчик СВВ може «запам’ятовувати» значущі події і дані на час сеансу. Це дозволяє датчику знаходити кореляції між різними подіями протягом сеансу, ідентифікуючи атаки з кількома компонентами, які інакше не можуть бути виявлені. Без можливості

зберігати стан ми можемо тільки перевіряти кожен пакет, запит або відповідь самостійно, повністю незалежно від іншої частини сеансу.

Рисунок 3.1 – Метод аналізу протоколу з урахуванням стану

3.5.2 Приклад аналізу протоколів з відстеженням стану.

Поняття аналізу протоколів з відстеженням стану найкраще пояснити, розглянувши кілька прикладів. Є кілька способів думати про «стан» у зв’язку. Одна з найпростіших форм стану – це можливість зв’язати запит з відповідною відповіддю. Оскільки датчик СВВ, який виконує аналіз протоколу з відстеженням стану, може послідовно відстежувати кожен запит і відповідь в сеансі, він легко може зіставити відповідь із запитом, який його згенерував. У багатьох випадках це надзвичайно цінно, оскільки багато відповідей містять якийсь індикатор стану, який повідомляє нам, який був результат запиту. 1) Наприклад: під час виконання команди FTP відповідь сервера починається з тризначного коду. Код стану, який починається з «2», вказує на те, що команда була успішною, а «5» вказує на збій.

Датчики СВВ можуть використовувати цю інформацію декількома способами.

Найбільш очевидний спосіб – визначити, чи були певні атаки успішними або невдалими. Якщо зловмисник намагається отримати конфіденційний файл, і видно, що код стану у відповіді починається з «2», то спроба була успішною.

Оскільки можна ідентифікувати кожен невдалий запит і відслідковувати, скільки запитів не було виконано в сеансі, можна шукати велику кількість збоїв. Це дуже корисно в ході виявлення атак методом «грубої сили», таких як атаки з використанням паролів.

Більш складне використання в тому, щоб ідентифікувати випадки, коли запит не має відповідної відповіді. Деякі атаки включають швидку відправку однієї і тієї ж команди на сервер сотні або тисячі разів. У цих випадках датчик СВВ може побачити багато запитів від клієнта, перш ніж побачити один у відповідь від сервера.

Таким чином, проста можливість запам'ятати останню команду і зв’язати її з відповіддю дає нам можливість ідентифікувати кілька типів атак. Однак не існує обмежень щодо запам’ятовування попередньої команди; можна пам’ятати попередні команди і відповіді. Набагато більш ймовірно, що можна просто витягнути важливі дані з певних команд і відповідей і зберегти ці дані для майбутнього використання.

2. Приклад збереження даних з сеансу для датчика СВВ, який використовуватиметься в останній частині сеансу. Користувач FTP входить в систему, використовуючи чотири етапи:

Користувач відправляє «USER kkent» на FTP-сервер, де kkent –ім’я користувача.

FTP-сервер відповідає «331 Надіслати пароль».

Користувач відправляє «PASS foobar» на FTP-сервер.

FTP-сервер підтверджує, що пароль правильний, і відповідає «230 Користувач увійшов в систему».

Датчик СВВ виявляє команду USER і зберігає «kkent» в якості попереднього імені користувача для цього сеансу FTP. Потім він очікує команду PASS, яка має відповідь з кодом стану, який починається з 2, що вказує на успішність аутентифікації. Датчик СВВ також відстежує іншу команду USER, яка вказує, що користувач намагається знову аутентифікуватися. Як тільки успішна аутентифікація була виявлена, датчик СВВ знає, що сеанс, який він відстежує, є сеансом імені користувача kkent.

Ця інформація корисна двома основними способами. По-перше, якщо атака відбувається під час цього сеансу, СВВ може повідомити, що ім’я користувача kkent використовувалося для цього сеансу. Ця інформація може бути надзвичайно корисна при розслідуванні інциденту. По-друге, якщо використовувалося ім’я «root» або «administrator». Аналізуючи всі запити і відповіді, пов’язані з аутентифікацією, датчик СВВ може виявляти спроби використовувати такі облікові записи, а також записувати, чи були успішними всі спроби чи ні.

3. Приклад фази сеансу FTP, щоб краще зрозуміти переваги відстеження стану.

З'єднання: FTP-клієнт встановлює TCP-з’єднання з FTP-портом сервера (TCP-порт 21).

Аутентифікація: користувач FTP-клієнта або відправляє ім’я користувача і пароль, або «анонімний» логін на FTP-сервер. Користувач залишається в цьому стані до тих пір, доки аутентифікація не буде успішною або з’єднання не буде розірвано.

Транзакція. Як тільки користувач пройшов аутентифікацію, він може видавати команди на FTP-сервер. Якщо будь-яка з цих команд викликає передачу даних, таких як файли, скопійовані між клієнтом і сервером, або списки каталогів, для кожної передачі встановлюється окреме недовговічне TCP-з’єднання.

На етапі транзакції FTP створюється додаткове TCP-з’єднання кожного разу, коли дані FTP мають передаватися між FTP-клієнтом і сервером. Перед

встановленням з'єднання для передачі даних FTP клієнт і сервер FTP обмінюються даними (за допомогою команд і відповідей) про те, яку IP-адресу і порт слід використовувати. Якщо клієнт FTP хоче ініціювати з’єднання для передачі даних з сервером (пасивний FTP), він відправить команду на сервер FTP та очікуватиме, що відповідь сервера FTP буде містити номер порту. Потім FTP-клієнт спробує встановити нове TCP-з’єднання з цим портом на сервері. Датчик СВВ, який використовує аналіз протоколу з відстеженням стану, може знайти відповіді сервера FTP, які повідомляють клієнтам, які номери портів використовувати для з’єднань даних. Коли він бачить підключення з використанням FTP-сервера, він може потім підтвердити, чи є вони законними FTP-з’єднаннями для передачі даних або зловмисник намагається підключитися до сервера, щоб отримати несанкціонований доступ до даних. Це відмінний приклад того, як відстеження стану може ідентифікувати атаки, які інакше не могли б бути виявлені.

4. Приклад перевірки послідовності команд. Коли перейменовується файл в FTP, використовуються дві команди. По-перше, команда RNFR (перейменувати з) надає старе ім’я файлу; після отримання позитивної відповіді сервера на цю команду має бути виконана команда RNTO (перейменувати в). Є атаки, які включають в себе багато послідовних команд RNTO. Оскільки команді RNTO має передувати RNFR, то є підозрілим, якщо є десять послідовних команд RNTO. Розширені підписи, засновані на аналізі протоколу з відстеженням стану, можуть підраховувати, скільки послідовних команд RNTO помічено, або вони можуть пам’ятати попередню команду, і коли RNTO видається, перевірити попередню команду.

Таким чином з проведеного аналізу видно, що протокол з відстеженням стану є найкращим і в багатьох випадках єдиним способом виявлення різних складних атак.

Реалізовані сьогодні у СВВ методи засновані на загальних уявленнях теорії розпізнавання образів. Відповідно до них для виявлення аномалії на основі експертної оцінки формується образ нормального функціонування

інформаційної системи. Цей образ виступає як сукупність значень параметрів оцінки. Його зміна вважається проявом аномального функціонування системи. Після виявлення аномалії і оцінки її ступеня формується судження про природу змін: чи є вони наслідком вторгнення або допустимим відхиленням. Для виявлення зловживань також використовується образ (сигнатура), однак тут він відображає заздалегідь відомі дії атакуючого.

Наведені методи виявлення вторгнень проваджуються та функціонують в СВВ. Процеси, які проходять в СВВ протягом пошуку вторгнень, наведено на рис.3.2.

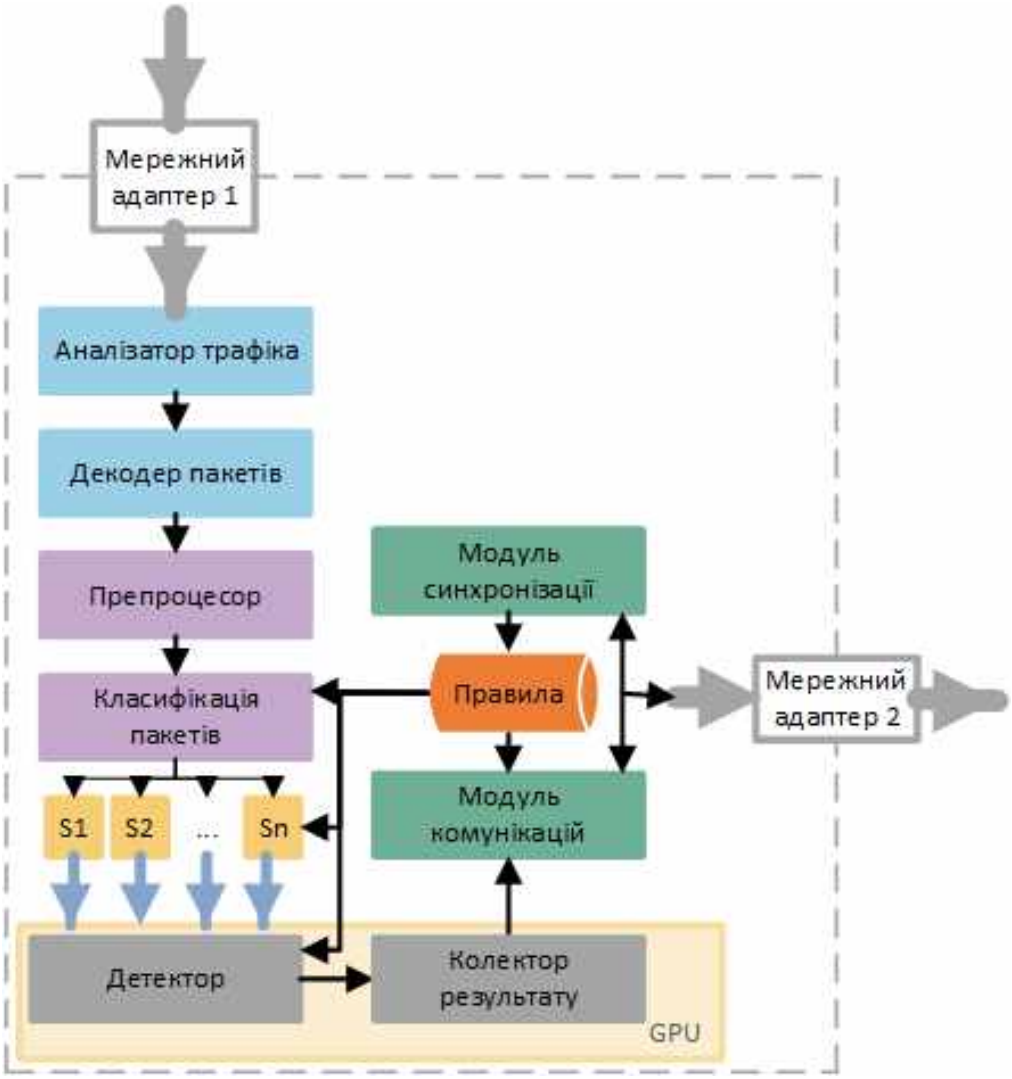


Рисунок 3.2 – Модель процесів у мережній СВВ

3.5.3 Вибір оптимальної сукупності ознак оцінки інформаційної системи

Сьогодні використовується евристичне визначення (вибір) множини параметрів вимірювань системи, що захищається, використання якого має дати найбільш ефективне і точне розпізнавання вторгнень. Складність вибору множини можна пояснити тим, що складові її підмножини залежать від типів вторгнень, що виявляються. Тому одна і та ж сукупність цієї установки не буде адекватною для всіх типів вторгнень.

Будь-яку систему, що складається зі звичних апаратних і програмних засобів, можна розглядати як унікальний комплекс зі своїми особливостями. Це є поясненням можливості пропуску специфічних вторгнень для системи, що захищається СВВ, та які використовують один і той самий набір параметрів оцінки. Найбільш переважне рішення – визначення необхідних параметрів оцінки в процесі роботи. Труднощі ефективного динамічного формування параметрів оцінки в тому, що розмір області пошуку експоненціально залежить від потужності початкової множини. Якщо є початковий список з N параметрів, актуальних для ідентифікації вторгнень, то кількість підмножин цього списку становить 2N. Тому не є можливим використання алгоритмів перебору для знаходження оптимальної множини. Одне з можливих рішень – використання генетичного алгоритму [58].

Отримання єдиної оцінки стану інформаційної системи.

Загальна оцінка аномальності має визначатися з розрахунку множини параметрів оцінки. Якщо ця множина формується так, як було запропоновано в попередньому параграфі, то отримання єдиної оцінки є досить непростим завданням. Один з можливих методів – використання статистики Байєса. Інший спосіб, який застосовується в СВВ, заснований на використанні коваріантних матриць [47, 53].

Дані, що збираються на вузлах та в мережі.

Оскільки існуючі атаки викликають відхилення у використанні ресурсів, на вузлах та в мережі збираються такі параметри, які об’єднуються у вектор:

– завантаження CPU (відсотків);

– дискові IO операції (операцій за секунду);

– споживання пам'яті (у відсотках);

– мережна активність (Мбіт за секунду).

В роботі [44] пропонується збирати такі мережні параметри:

– послідовність TCP пакетів, прапорці, номери портів відправника і одержувача і IP адреси відправника;

– послідовність ICMP пакетів, IP адреси відправника, ICMP_ID;

– IP адреси джерела, довжину пакета і UDP порти джерела і одержувача.

В роботі [45] наведено опис датасету трафіка, який містить атаки та має великий список параметрів, частина з яких надалі буде використана як ознаки. Параметри трафіку та атак наведено нижче:

duration – тривалість з’єднання в секундах;

protocol_type – тип використовуваного протоколу: TCP, UDP та ін.;

service – тип використовуваного обслуговування: HTTP, FTP, TELNET і ін.;

flag – прапорець з’єднання: норма або помилка;

scr_bytes – кількість байт даних від джерела до одержувача;

dst_bytes – кількість байт даних від одержувача до джерела;

land – 1 якщо з’єднання з / на такому самому хості / порті;

wrong_fragments – кількість «невірних» фрагментів;

urgent – кількість термінових (urgent) пакетів;

hot – кількість «гарячих» індикаторів;

num_failed_logins – кількість помилкових спроб входу;

logged_in - 1 – успішний вхід, 0 в іншому випадку;

num_compromised – кількість скомпрометованих умов;

root_shell – 1 – якщо отримана коренева оболонка, 0 – в іншому випадку;

su_attempted – 1 – якщо була спроба виконати «su root», 0 – в ін. випадку;

num_root – число доступів типу «root»;

num_file_creations – кількість операцій створення файлу;

num_shells – кількість «підказок оболонки»;

num_access_files – число отримань доступу до контролю над файлами;

num_outbound_cmds – кількість вихідних команд через ftp сесію;

is_host_login – 1 – якщо логін належить до «host» списку;

is_quest_login – 1 – якщо підключення типу «гість»;

count – кількість підключень до цього хоста за останні 2 секунди;

srv_count – кількість підключень до цього сервісу за останні 2 секунди;

serror_rate – відсоток підключень з syn помилками;

srv_serror_rate – відсоток підключень до сервісу з syn помилками;

rerror_rate – відсоток підключень з rej помилками;

srv_rerror_rate – відсоток підключень до сервісу з rej помилками;

same_srv_rate – відсоток підключень до такого сервісу;

diff_srv_rate – відсоток підключень до різних сервісів;

srv_diff_hast_rate – відсоток підключень до різних хостів;

dst_host_count – кількість з’єднань до локального хосту, встановлених віддаленою стороною;

dst_host_srv_count – кількість з’єднань до локального хоста, встановлених віддаленою стороною та використовують одну і ту саму службу;

dst_host_same_srv_rate – процентна кількість з’єднань до локального хоста, встановлених віддаленою стороною та використовують одну і ту саму службу;

dst_host_diff_srv_rate – процентна кількість з’єднань до локального хоста, встановлених віддаленою стороною та які використовують різні служби;

dst_host_same_src_port_rate – процентна кількість з’єднань до даного хоста при поточному номері порта джерела.

dst_host_srv_diff_host_rate – процентна кількість з’єднань до служби різних хостів;

dst_host_serror_rate – процентна кількість з’єднань з помилкою типу syn для даного хоста-приймача;

dst_host_srv_serror_rate – процентна кількість з’єднань з помилкою типу syn для даної служби приймача;

dst_host_rerror_rate – процентна кількість з’єднань з помилкою типу rej для даного хоста-приймача;

dst_host_srv_rerror_rate – процентна кількість з’єднань з помилкою типу rej для даної служби приймача.

Ознаки можуть обиратися адміністратором мережі. Номер порту відправника, як правило, не має сенсу враховувати, оскільки він генерується автоматично.

Таким чином, є можливість збору, аналізу та систематизації статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи, обирати методи виявлення вторгнень, хмарні чи фізичні сервіси обробки та зберігання інформації в системі.

3.6 Висновки до третього розділу

1. Проведено аналіз множини існуючих параметрів функціонування системи та мережі, який показав, що бажано зменшити кількість вхідних змінних як для зниження обчислювальної вартості моделі, так і для підвищення продуктивності моделі. Методи вибору функцій, засновані на статистиці, припускають оцінку зв’язку між кожною вхідною змінною та цільовою змінною за допомогою статистики і вибір тих вхідних змінних, які мають найтісніший зв’язок з цільовою змінною. Ці методи можуть бути швидкими і ефективними, хоча вибір статистичних заходів залежить від типу даних як вхідних, так і вихідних змінних. Таким чином, при виборі функцій, заснованих на фільтрації, було обрано набір ознак для розробки методів моніторингу та виявлення вторгнень.

2. Оскільки в світі кіберзлочинів з’являються нові шаблони і класи атак, істотною вимогою є оновлення існуючих систем виявлення вторгнень згідно з новими шаблонами даних. Таке оновлення вимагає перепідготовки СВВ з використанням нового набору даних поруч зі старим існуючим, які наведено в цій роботі. Наведено забезпечення своєчасного і економічно ефективного механізму поновлення, який зазначено як критичну вимогу під час розробки систем виявлення вторгнень.

3. Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак, що базується на хмарному підході є складовою дублюючої системи оповіщення населення про надзвичайні події у регіоні. Дані, які зібрано зберігаються та оброблюються в хмарному компоненті системи IDS, що дозволяє розвантажити кінцеві пристрої від необхідності виконувати складні обчислення. Функції пристроїв нижнього рівня обмежуються виділенням ознак мережного трафіку та виявленням аномалій. Пристрої повідомляють хмарному сервісу про виявлені аномалії та передають їх параметри для аналізу.

4 ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ МЕТОДІВ ТА ПРОТОКОЛІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ КОНФІДЕНЦІЙНИХ ПОВІДОМЛЕНЬ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ. ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНИХ РІШЕНЬ ТА ПРОВЕДЕННЯ ПОРІВНЯЛЬНОГО АНАЛІЗУ З ВІДОМИМИ ПРОТОКОЛЬНИМИ АНАЛОГАМИ

4.1 Аналіз місця порогових криптографічних схем в інфокомунікаційних мережах

Ключову роль у забезпеченні мережної безпеки відіграють криптографічні засоби захисту інформації, які широко реалізуються в сучасних інфокомунікаційних мережах. Наприклад, в межах порогової криптографії на стороні відправника конфіденційне повідомлення (секрет) розбивається на декілька частин, які загалом мають доставлятись отримувачу незалежно одна від одної. Зокрема повідомлення може бути дешифровано лише за наявності в отримувача більш ніж заданої порогової кількості його частин. Таким чином, за умови використання порогової криптографії зловмисник має скомпрометувати не менше за порогову кількість частин повідомлення. Слід зазначити, що порогова криптографія вважається однією з найбезпечніших криптосистем та використовується в сучасних рішеннях, наприклад, таких як RSA (алгоритм Рівеста–Шаміра–Алдемана), криптосистема Пейє, криптосистема Дамгорда–Юрика, схема Ель-Гамаля, алгоритм електронного цифрового підпису із застосуванням еліптичних кривих [61-68].

Концепція порогової криптографії знайшла своє широке використання та застосування у сучасних ІКМ і реалізується в технологіях хмарних обчислень, механізмах автентифікації, управлінні ключами, технології Інтернету речей (Internet of Things, IoT), мобільних самоорганізованих мережах (Mobile Ad hoc Network, MANET), сенсорних мережах, електронних цифрових підписах, застосунках електронного голосування, візуальній криптографії тощо (табл. 4.1) [61-68].

Таблиця 4.1 – Напрями застосування різних порогових схем в ІКМ

Напрям застосування	Схема порогового розділення секрету	Переваги використання
Хмарні обчислення	Схема Шаміра	Зменшення кількості ключів; забезпечення конфіденційності приватних даних; безпечне та надійне зберігання даних; безпечна передача даних.
Автентифікація	Схема Шаміра, криптосистема Пейє	Швидка групова автентифікація користувачів; стійкість до масиву атак, масштабованість, гнучкість; легковагова, масштабована групова автентифікація в IoT; анонімна автентифікація в IoT.
Ad-Hoc мережі	Схема Шаміра, порогова криптографія на основі еліптичних кривих (ECC)	Стійкість до сертифікатів фальшивих відкритих ключів, захист від уразливостей, спричинених шкідливими вузлами; високий рівень безпеки, доступний сервіс управління ключами.
Електронний цифровий підпис	Схема Шаміра, схема Шаміра з криптосистемою Ель-Гамаля	Відстежуваність підписів, множина політик підпису; відсутність потреби в довіреній третій стороні.
Електронне голосування	Схема Шаміра, схема Асмута–Блума, криптосистема Пейє	Зменшення порушення цілісності даних, відсутність потреби в довіреній третій стороні; надійність, конфіденційність; підтримка множинного та нульового вибору, ієрархічність; використання властивості гомоморфності.
Цифрове оброблення зображень	Схема Шаміра	Безпечна передача зображення через незахищені мережі.

Взагалі схеми розділення секрету (secret sharing schemes) можна класифікувати таким чином [61-63]:

– проактивне розділення секрету;

– динамічне розділення секрету;

– розділення секрету з можливостями вето;

– робастне розділення секрету;

– поліноміальне розділення секрету;

– схеми, основані на китайській теоремі про остачі (Chinese Remainder Theorem, CRT);

– анонімне розділення секрету;

– розділення секрету на основі систематичних блокових кодів;

– розділення секрету у вигляді «чорної скрині» (black box secret sharing);

– візуальне розділення секрету.

Схема Шаміра належить до схем поліноміального розділення секрету, тоді як схема Асмута–Блума основана на використанні теореми CRT. У схемі візуального розділення секрету візуальне зображення було як конфіденційне повідомлення. До прикладів забезпечення мережної безпеки також може належати концепція безпечної маршрутизації, яка реалізована в ІКМ, наприклад, за допомогою механізму SPREAD [64, 65]. Це рішення основане на багатошляховій передачі частин конфіденційного повідомлення, які сформовані відповідно до схеми Шаміра. Зокрема чим більше шляхів, які не перетинаються, буде використано, тим з меншою ймовірністю компрометації повідомлення буде доставлено отримувачу. Подібні особливості у свою чергу накладають додаткові вимоги на використовувані математичні моделі та методи маршрутизації в ІКМ.

У роботах [64, 65] представлено та досліджено механізми SPREAD (Secure Protocol for Reliable dAta Delivery) та H-SPREAD (Hybrid Secure Protocol for Reliable dAta Delivery) для посилення безпечної передачі повідомлень у MANET (рис. 4.1). Основна ідея полягає в тому, щоб розділити конфіденційне повідомлення на кілька фрагментів – частин, а потім передавати ці частини від відправника до отримувача множиною шляхів, які не перетинаються, так, щоб навіть якщо певну кількість частин повідомлення буде скомпрометовано, секретне повідомлення загалом залишиться нескомпрометованим. Запропоновано загальну архітектуру системи: математичну модель для створення та реконструкції частин повідомлення, оптимальний розподіл його

частин за декількома шляхами з точки зору безпеки, а також підходи щодо розрахунку мультишляху в мережах MANET.

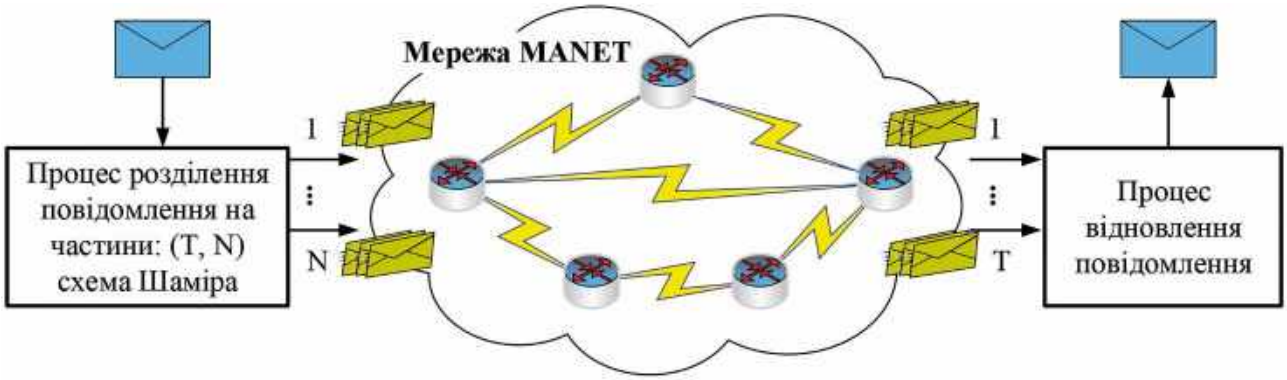


Рисунок 4.1 –Загальна архітектура роботи механізму SPREAD

Порівняно з проводовими мережами забезпечення безпеки в MANET пов’язано з виявленням і запобіганням множини наявних уразливостей та атак. По-перше, радіоканали більш сприйнятливі до атак як пасивного прослуховування, так і активного втручання в сигнали та здійснення завад. По-друге, більшість протоколів маршрутизації в MANET припускають довірчі взаємодії між вузлами для здійснення передачі пакетів. Залежність від такої взаємодії робить передачу даних більш уразливою щодо несанкційного доступу, підміни даних та атак типу «відмова в обслуговуванні». По-третє, відсутність фіксованої інфраструктури та централізованого управління ускладнює застосування більшості традиційних рішень щодо забезпечення мережної безпеки.

Унаслідок використання механізму SPREAD вдається знизити ймовірність компрометації переданого повідомлення, тому що помітно ускладнюється завдання зловмисника: йому необхідно скомпрометувати не один маршрут, яким передається нерозділене повідомлення, а всі шляхи, якими передаються його частини. Зокрема під компрометацією повідомлення розуміється подія, пов’язана з несанкційним доступом до його вмісту.

Варто окремо зазначити, що ймовірність компрометації шляху багато в чому залежить як від кількості складників його вузлів і каналів зв’язку, так і від

параметрів їх безпеки, тобто кожен елемент (вузол, канал) шляху може бути скомпрометований з певною ймовірністю. У загальному випадку шляхи, які використовуються для передачі частин розділеного відповідно до схеми Шаміра повідомлення, можуть мати різні значення ймовірності компрометації. У межах відомих рішень SPREAD вважається, що множина шляхів, які не перетинаються, вже попередньо відома. Однак рішення, орієнтовані на використання лише шляхів, які не перетинаються, негативно впливають на ефективність використання доступного мережного ресурсу.

Тому в даному розділі пропонуються рішення, які, з одного боку, доповнюють механізм SPREAD з точки зору розрахунку множини шляхів, що не перетинаються, а з іншого, адаптують цей механізм під використання шляхів, що можуть перетинатись.

4.2 Метод безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах з використанням шляхів, які не перетинаються

4.2.1 Математична модель розрахунку маршрутів, які не перетинаються, в інфокомунікаційних мережах

Як показав проведений аналіз, проблема забезпечення мережної безпеки на сучасному етапі розвитку інформаційного суспільства є дуже актуальною. Саме різнотипні та взаємодоповнюючі організаційні, соціальні, технічні (апаратні та програмні) заходи та засоби повинні забезпечити належний рівень безпеки інформації, яка передається в сучасних ІКМ. Перелік таких засобів невпинно розширюється, а ефективність їх використання постійно зростає, але й методи та стратегії виявлення та використання вразливостей мережного обладнання також безперервно вдосконалюються.

Досить дієвим засобом забезпечення мережної безпеки в ІКМ є протоколи маршрутизації [68-71]. Саме вони повинні забезпечити проактивний і реактивний захист телекомунікаційної мережі на основі збору та аналізу

інформації про її стан. Водночас протоколи безпечної маршрутизації, крім звичних даних про стан мережі (її топологію, пропускні здатності, завантаженість та надійність каналів зв'язку), мають прогнозувати та оцінювати значення ключових показників безпеки комутаційного та серверного обладнання ІКМ, рівень їх уразливості та ймовірність компрометації. З цією метою математичне та алгоритмічне забезпечення протоколів маршрутизації ІКМ має бути вдосконалене та розширене під нові умови та завдання, пов'язані із забезпеченням заданого рівня мережної безпеки, оскільки більшість існуючих маршрутних протоколів у кращому випадку орієнтовані на покращення показників якості обслуговування (Quality of Service, QoS).

Ґрунтуючись на результатах, отриманих у роботах [64, 65, 68, 72-74], у даному розділі пропонується метод безпечної маршрутизації конфіденційних повідомлень, які для зниження ймовірності їх компрометації мають передаватись за шляхами, що не перетинаються та включають в себе найбільш безпечні канали зв'язку. Фактично метод є подальшим узагальненням рішень, що охоплюють оптимізаційні моделі маршрутизації, які запропоновані у роботах [64, 65, 68, 72-74] та доповнюють одне одну.

Для опису математичної моделі розрахунку шляхів, запропонованої у роботах [72-74], будуть використані наступні позначення:

- $G=(R,E)$ – граф, що описує структуру ІКМ;
- $R=\{R_i; i=\overline{1,m}\}$ – множина вершин графа *G*, що представляють маршрутизатори мережі;
- $E=\{E_{i,j}; i,j=\overline{1,m}; i\neq j\}$ – множина дуг графа *G*, що описують канали зв'язку ІКМ;
- s – вузол-відправник (джерело) КП;
- d – вузол-отримувач конфіденційного повідомлення.

У процесі розв'язання задачі щодо розрахунку маршрутів, що не перетинаються, необхідно розрахувати множину маршрутних змінних $a_{i,j}$,

кожна з яких визначає належність каналу $E_{i,j} \in E$ до множини обчислених шляхів, при передачі фрагментів повідомлення. Позначимо через M цілочисельний параметр, що характеризуватиме кількість використаних фрагментами повідомлення шляхів, що не перетинаються.

Відповідно до фізичної суті поставленої задачі на маршрутні змінні $a_{i,j}$ накладається система обмежень. По-перше, актуальними є такі умови

$$a_{i,j} \in \{0;1\}. \tag{4.1}$$

Для вузлів відправника та отримувача повідомлення мають виконуватися наступні умови [72-74]:

$$\sum_{j:E_{i,j} \in E} a_{i,j} = \mathrm{M}\ ;\ R_i = s; \tag{4.2}$$

$$\sum_{j:E_{j,i} \in E} a_{j,i} = \mathrm{M};\ R_i = d. \tag{4.3}$$

При забезпеченні виконання умов (4.2) та (4.3) гарантується, що кількість шляхів, які виходять з вузла-відправника, співпадає з числом шляхів, які входять у вузол-отримувач повідомлення. У процесі використання транзитних вузлів ІКМ ($R_i \neq s, d$) на маршрутні змінні накладаються такі обмеження [72-74]:

$$\begin{cases} \sum\limits_{j:E_{i,j} \in E} a_{i,j} \leq 1, \\ \sum\limits_{j:E_{j,i} \in E} a_{j,i} \leq 1, \\ \sum\limits_{j:E_{i,j} \in E} a_{i,j} - \sum\limits_{j:E_{j,i} \in E} a_{j,i} = 0. \end{cases} \tag{4.4}$$

Перша і друга умови в (4.4) відповідають за те, щоб через транзитний вузол R_i проходило не більше одного шляху. Виконання третьої умови в (4.4) гарантує, що з транзитного вузла R_i може виходити шлях лише у тому випадку, якщо він

у цей вузол заходить. Виконання умов (4.1)-(4.4) відповідно до результатів дослідження, представлених у роботах [72-74], має забезпечити розрахунок шляхів у ІКМ, що не перетинаються, тобто спільними в них будуть лише вузли відправник (s) та отримувач (d).

На цілочисельний параметр M накладаються обмеження виду

$$\mathrm{M} \geq 1. \tag{4.5}$$

Для врахування параметрів мережної безпеки у процесі розрахунку множини шляхів, що не перетинаються в ІКМ, у роботах [72-74] запропоновано до використання критерій оптимальності, що забезпечує максимум наступної цільової функції:

$$J_1 = v\mathrm{M} - \sum_{E_{i,j} \in E} w_{i,j} a_{i,j}\ , \tag{4.6}$$

де v та $w_{i,j}$ – додатні вагові коефіцієнти, які визначають важливість відповідних доданків у (4.6). Коефіцієнти $w_{i,j}$ визначають маршрутні метрики каналів зв'язку мережі $E_{i,j} \in E$, які будуть пов'язані з імовірністю їх компрометації [72-74]

$$w_{i,j} = -\log_{10}(1 - p_{i,j}), \tag{4.7}$$

де $p_{i,j}$ – імовірність компрометації каналу зв'язку $E_{i,j} \in E$.

Для того, щоб першочергово забезпечувалась максимізація кількості шляхів, які не перетинаються, у цільовій функції (4.6) вибір вагових коефіцієнтів треба здійснювати згідно умови

$$v >> w_{i,j}, \tag{4.8}$$

У цьому разі другий доданок у (4.6) буде впливати на включення в розраховану множину шляхів найбільш безпечних каналів.

Таким чином, задача щодо розрахунку шляхів, що не перетинаються, була сформульована в оптимізаційній формі. Критерієм оптимальності виступає

максимум цільової функції (4.6), а на керуючі змінні $a_{i,j}$ та M накладаються обмеження (4.1)-(4.5). Оптимізаційна задача (4.1)-(4.6) відноситься до класу задач цілочисельного лінійного програмування (Integer Linear Programming, ILP).

4.2.2 Математична модель безпечного балансування фрагментів конфіденційного повідомлення у інфокомунікаційній мережі

У роботах [64, 65] представлено рішення щодо розробки та вдосконалення механізму SPREAD (Secure Protocol for Reliable dAta Delivery), що відноситься до засобів безпечної маршрутизації. Для забезпечення безпечної маршрутизації конфіденційного повідомлення (КП) в мережі відповідно до механізму SPREAD необхідно вирішити такі завдання [64, 65]:

1. Розрахунок множини маршрутів, що не перетинаються, між заданими вузлами «відправник» і «отримувач».

2. Розділення конфіденційного повідомлення, що передається, на множину частин відповідно до обраної схеми Шаміра.

3. Розподіл множини частин повідомлення між множиною маршрутів, визначених у процесі вирішення першого завдання.

Крім того, у роботах [75-79] запропоновано вдосконалену модель механізму SPREAD, в межах якої допускається певний характер перетину шляхів у ІКМ, що супроводжується покращенням показників мережної безпеки при передачі КП. Закон (схема) розділення повідомлення на фрагменти в загальному випадку може бути відомим зловмиснику, але скомпрометувати конфіденційне повідомлення він зможе лише тоді, коли скомпрометує всі використані для доставки шляхи. Тому рівень мережної безпеки у цьому випадку цілком залежить від кількості та безпечності шляхів, що використовуються для доставки фрагментів КП.

З метою пояснення принципу роботи механізму SPREAD будуть використані такі позначення:

– M_i – кількість каналів зв'язку в i-му шляху, що можуть бути скомпрометовані ($i=\overline{1,M}$);

– p_i^j – імовірність компрометації j-го каналу зв'язку i-го шляху ($i=\overline{1,M}$, $j=\overline{1,M_i}$);

– (T,N) – параметри схеми Шаміра, де N – загальна кількість фрагментів, на які розділяється повідомлення, що передається, унаслідок застосування схеми Шаміра; T – мінімальна кількість фрагментів, за якими можливо відновити повідомлення, що передається $(T \le N)$;

– p_i – імовірність компрометації i-го шляху ($i=\overline{1,M}$);

– P_{msg} – імовірність компрометації повідомлення загалом за умови його фрагментованої передачі мережею;

– n_i – цілочисельна змінна, яка характеризує кількість фрагментів КП, що передаються за i-м шляхом $i=\overline{1,M}$.

Тоді ймовірність компрометації i-го шляху, що складається з M_i елементів, можна розрахувати таким чином

$$p_i = 1-\left(1-p_i^1\right)\left(1-p_i^2\right)\ldots\left(1-p_i^{M_i}\right) = 1-\prod_{j=1}^{M_i}\left(1-p_i^j\right). \tag{4.9}$$

Для керуючих змінних n_i ($i=\overline{1,M}$) має виконуватися така умова [64, 65]:

$$\sum_{i=1}^{M} n_i = \mathrm{N}. \tag{4.10}$$

У випадку реалізації схеми Шаміра з параметрами $T<N$ мають виконуватися умови [64, 65]

$$N-T+1 \le n_i \le T-1,\ (i=\overline{1,M}). \tag{4.11}$$

Якщо ж використовується схема без надмірності, тобто $T=N$, мають місце такі умови [64, 65]:

$$1 \le n_i \le \mathrm{T} - 1, \ (i = \overline{1, M}). \tag{4.12}$$

Імовірність компрометації конфіденційного повідомлення, розділеного відповідно до схеми Шаміра на N фрагментів з подальшим використанням M шляхів, визначається згідно з виразом [64, 65]

$$P_{msg} = \prod_{i=1}^{M} p_i \ . \tag{4.13}$$

Фактично вираз (4.13) визначає ймовірність компрометації всіх M шляхів, що не перетинаються та використовуються для передачі фрагментів конфіденційного повідомлення.

Задачу безпечного балансування фрагментів конфіденційного повідомлення за множиною попередньо розрахованих, наприклад, за допомогою моделі (4.1)-(4.8), шляхів можна також представити в оптимізаційній формі. Критерієм оптимальності може виступати мінімум цільової функції [75, 76]

$$J = \sum_{i=1}^{M} p_i n_i \ . \tag{4.14}$$

Таким чином, в основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв’язання двох задач:

- розрахунку маршрутів, що не перетинаються, в інфокомунікаційній мережі за допомогою моделі (4.1)-(4.8);
- безпечного балансування фрагментів конфіденційного повідомлення (4.9)-(4.14) за множиною попередньо розрахованих шляхів (4.1)-(4.8).

4.2.3 Результати дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються

Дослідження процесу безпечної маршрутизації конфіденційних повідомлень, організованого за допомогою запропонованого методу, буде продемонстровано на прикладі ІКМ, структура якої представлена на рис. 4.2.

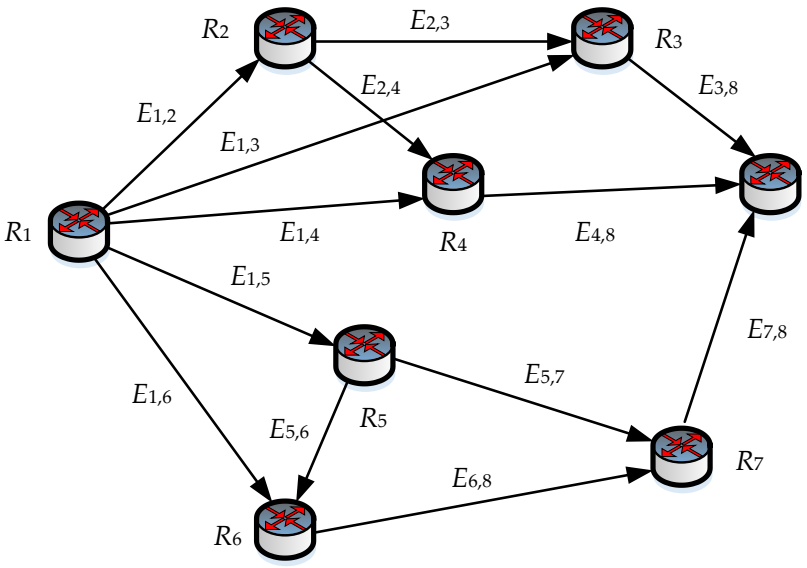


Рисунок 4.2 – Структура інфокомунікаційної мережі

До складу мережі входить вісім маршрутизаторів і тринадцять каналів зв’язку. Нехай конфіденційне повідомлення треба передати між маршрутизаторами R_1 і R_8. В процесі дослідження розглядалось три варіанти ймовірностей компрометації каналів зв’язку ІКМ (табл. 4.2).

Таблиця 4.2 – Варіанти ймовірностей компрометації каналів зв’язку ІКМ

Номер варіанту компрометації каналів ІКМ	$E_{1,2}$	$E_{1,3}$	$E_{1,4}$	$E_{1,5}$	$E_{1,6}$	$E_{2,3}$	$E_{2,4}$	$E_{3,8}$	$E_{4,8}$	$E_{5,6}$	$E_{5,7}$	$E_{6,7}$	$E_{7,8}$
1	0,1	0,8	0,3	0,4	0,8	0,2	0,5	0,6	0,5	0,4	0,3	0,9	0,2
2	0,9	0,6	0,1	0,2	0,8	0,3	0,1	0,3	0,7	0,4	0,9	0,2	0,1
3	0,1	0,1	0,9	0,9	0,6	0,1	0,3	0,8	0,4	0,6	0,2	0,1	0,1

Тоді в табл. 4.3 зазначені всі можливі маршрути ($L_1 \div L_7$) між маршрутизаторами R_1 та R_8, які виступали відправником та отримувачем КП. В цій же таблиці вказані ймовірності компрометації шляхів $L_1 \div L_7$, які розраховані відповідно до виразу (4.9).

Таблиця 4.3 – Імовірності компрометації шляхів у ІКМ для різних варіантів компрометації каналів мережі

Шлях		Номер варіанту компрометації каналів ІКМ		
		1	2	3
L_1	$R_1 \to R_2 \to R_3 \to R_8$	0,712	0,951	0,838
L_2	$R_1 \to R_3 \to R_8$	0,92	0,72	0,82
L_3	$R_1 \to R_2 \to R_4 \to R_8$	0,775	0,973	0,622
L_4	$R_1 \to R_4 \to R_8$	0,65	0,73	0,94
L_5	$R_1 \to R_5 \to R_7 \to R_8$	0,664	0,928	0,928
L_6	$R_1 \to R_5 \to R_6 \to R_7 \to R_8$	0,9712	0,6544	0,9676
L_7	$R_1 \to R_6 \to R_7 \to R_8$	0,984	0,856	0,676

В табл. 4.4 наведено ймовірності компрометації мультишляхів $LL_1 \div LL_7$, що складались з множини шляхів, які не перетинались. Фактично в табл. 4.4 вказані ймовірності компрометації, які розраховані відповідно до формули (4.13).

Таблиця 4.4 – Імовірності компрометації мультишляхів у ІКМ, що складаються зі шляхів, що не перетинаються, для різних варіантів компрометації каналів

Мультишлях	Шляхи, що входять до мультишляху	Номер варіанту компрометації каналів ІКМ		
		1	2	3
LL_1	L_1, L_4, L_5	0,3073	0,6442	0,731
LL_2	L_1, L_4, L_6	0,4495	0,4543	0,7622
LL_3	L_1, L_4, L_7	0,4554	0,5943	0,5325
LL_4	L_2, L_4, L_5	0,3971	0,4878	0,7153
LL_5	L_2, L_4, L_6	0,5808	0,344	0,7458
LL_6	L_2, L_4, L_7	0,5884	0,4499	0,5211
LL_7	L_2, L_3, L_5	0,4734	0,6501	0,4733
LL_8	L_2, L_3, L_6	0,6925	0,4584	0,4935
LL_9	L_2, L_3, L_7	0,7016	0,5997	0,3448

Використання математичної моделі (4.1)-(4.6) дозволило визначити таку множину використаних шляхів, що відповідає мінімальному значенню ймовірності компрометації повідомлення (4.13), яке буде передаватись ними

окремими фрагментами. Ці шляхи в табл. 4.4 для кожного варіанту компрометації каналів зв'язку виділено сірим кольором. Таким чином, результати дослідження, наведені в табл. 4.3 та 4.4, підтвердили адекватність моделі розрахунку маршрутів, що не перетинаються, в інфокомунікаційній мережі (4.1)-(4.6). Використання запропонованого методу безпечної маршрутизації, заснованого на маршрутних метриках (4.7), дозволило у порівнянні з іншими доступними рішеннями знизити ймовірність компрометації конфіденційних повідомлень (табл. 4.4):

– від 23% до 56% для першого сценарію компрометації каналів ІКМ;
– від 27% до 47% для другого сценарію компрометації каналів ІКМ;
– від 27% до 55% для третього сценарію компрометації каналів ІКМ.

Для наочної демонстрації отриманих результатів на рис. 4.3 – 4.5 показано множини шляхів у ІКМ, що не перетинаються, тобто мають спільними лише вузли відправника (R_1) та отримувача (R_8).

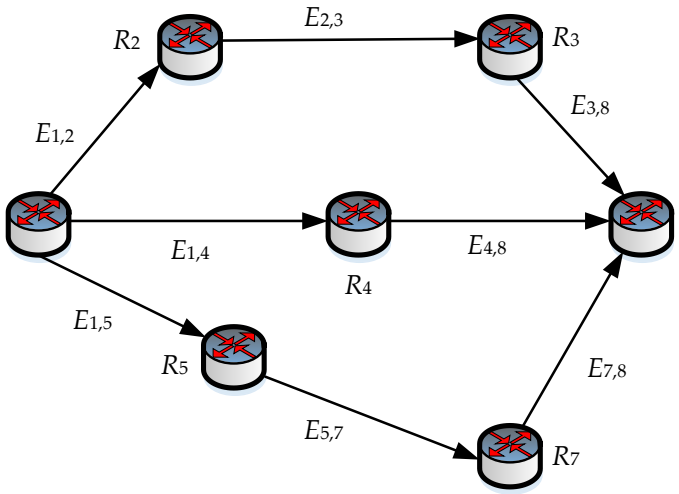


Рисунок 4.3 – Множина оптимальних шляхів L_1, L_4, L_5 для першого варіанту компрометації каналів зв'язку ІКМ ($P_{msg} = 0{,}3073$)

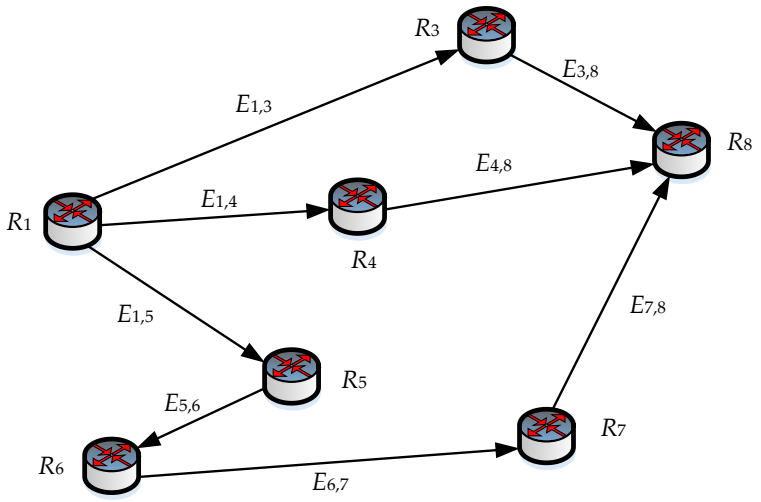


Рисунок 4.4 – Множина оптимальних шляхів L_2, L_4, L_6 для другого варіанту компрометації каналів зв'язку ІКМ ($P_{msg} = 0{,}344$)

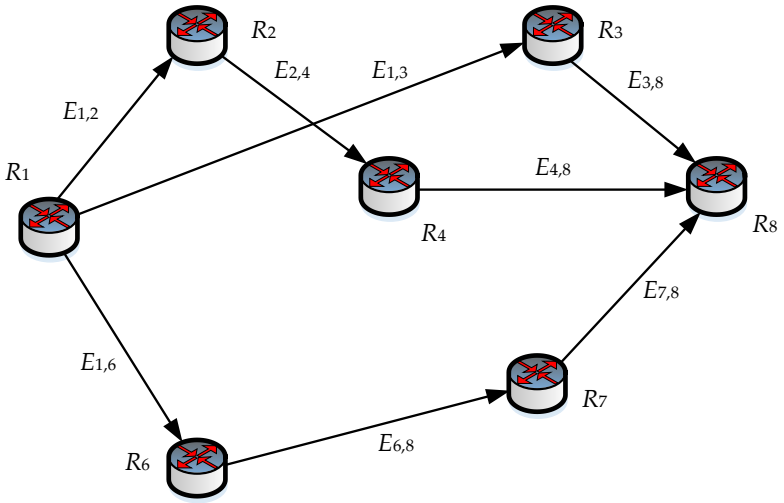


Рисунок 4.5 – Множина оптимальних шляхів L_2, L_3, L_7 для третього варіанту компрометації каналів зв'язку ІКМ ($P_{msg} = 0{,}3448$)

У табл. 4.5 представлено порядок фрагментованої передачі *k*-го повідомлення в ІКМ за допомогою множини розрахованих шляхів (табл. 4.4), що не перетинаються, для різних варіантів компрометації каналів мережі.

У процесі розділення конфіденційного повідомлення на фрагменти використовувалась схема Шаміра (8, 10). Як показано в табл. 4.5, кількість фрагментів, які передавались тим чи іншим шляхом, відповідала ймовірності

його компрометації (4.14) та умовам (4.11). Чим вищою була ймовірність компрометації шляху, тим менше фрагментів повідомлення ним передавалось, але завжди для компрометації повідомлення зловмиснику необхідно скомпрометувати всі три використані для передачі маршрути, що не перетинались.

Таблиця 4.5 – Порядок фрагментованої передачі повідомлення в ІКМ за допомогою множини розрахованих шляхів, що не перетинаються, для різних варіантів компрометації каналів мережі

Номер варіанту компрометації каналів ІКМ	Мультишлях	Шлях	Кількість фрагментів повідомлення, n_i	Ймовірність компрометації шляху
1	LL_1	L_1	3	0,712
		L_4	4	0,65
		L_5	3	0,664
2	LL_5	L_2	3	0,72
		L_4	3	0,73
		L_6	4	0,6544
3	LL_9	L_2	3	0,82
		L_3	4	0,622
		L_7	3	0,676

4.3 Метод безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах з використанням шляхів, які перетинаються

В умовах використання шляхів, які не перетинаються, значно спрощується розрахунок та аналіз ймовірності компрометації конфіденційних повідомлень (4.13), однак необхідно попередньо розрахувати множину подібних шляхів. Запропоноване у попередньому підрозділі маршрутне рішення оптимізоване під використання максимальної кількості шляхів, які не перетинаються, з

включенням до їх складу каналів (вузлів) з найкращими показниками мережної безпеки, тобто мінімальними ймовірностями компрометації. Як показали результати проведеного дослідження, це суттєво впливає на результуючі значення ймовірності компрометації конфіденційних повідомлень (табл. 4.4).

При забезпеченні високого рівня мережної безпеки та якості обслуговування варто враховувати, що сучасні інфокомунікаційні мережі є гетерогенними системами з досить складною та неоднорідної (нерегулярною) топологією. Тому між заданою парою маршрутизаторів ІКМ, як правило, існує досить потужна множина шляхів, які мають досить різні характеристики як з точки зору пропускної здатності, затримок та втрат пакетів, так і ймовірності компрометації. Проте використання при безпечній маршрутизації лише маршрутів, які не перетинаються, залишає поза увагою деякі вузли та канали, які мають певний мережний та кіберресурс. Нехтувати такими ресурсами, особливо в умовах складних та інтенсивних кіберзагроз, недоцільно.

У роботах [72-74] розроблено моделі та метод безпечної маршрутизації конфіденційних повідомлень шляхом їх фрагментованої передачі за композитними шляхами, які допускають певний тип перетинання та засновані на паралельно-послідовній структурі каналів зв’язку ІКМ. Проведений аналіз у роботах [72-74] показав, що використання запропонованого рішення в межах наведених розрахункових прикладів дозволив у порівнянні з механізмом SPREAD знизити ймовірність компрометації переданих повідомлень в залежності від розміру ІКМ у середньому від 5–10 % до 25–50 %. У даному підрозділі буде запропоновано подальший розвиток описаних рішень, представлений у вигляді методу безпечної маршрутизації конфіденційних повідомлень за маршрутами з довільним характером перетинання в ІКМ та проведено його порівняльний аналіз з класичним рішенням SPREAD.

4.3.1 Математична модель розрахунку ймовірності компрометації конфіденційних повідомлень, які фрагментовано передаються за шляхами, які перетинаються

У зв'язку з подальшим використанням у розрахунках шляхів, які перетинаються, в ІКМ позначення, які уведені у пункті 4.2.2, будуть дещо змінені та доповнені:

- V – кількість каналів зв'язку в ІКМ взагалі;
- $\tilde{M}$ – кількість шляхів, які перетинаються та можуть бути використаними для фрагментованої передачі конфіденційного повідомлення;
- p^j – імовірність компрометації j-го каналу ІКМ ($j=\overline{1,V}$);
- q^j – імовірність події, що j-й канал ІКМ не буде скомпрометовано ($j=\overline{1,V}$).

Тоді для кожного каналу зв'язку ІКМ буде справедливою наступна формула

$$p^j + q^j = 1,\ j=\overline{1,V}. \tag{4.15}$$

У випадку використання при безпечній маршрутизації шляхів, які перетинаються, події, що пов'язані з компрометацією цих шляхів, стають сумісними, тобто формула (4.13) для розрахунку ймовірності компрометації повідомлення використовуватись не може. Тоді, в межах логіко-ймовірнісного підходу [80] елементи мережі, за якими перетинаються маршрути, можна представити у вигляді т.з. «містків» або «перемичок». Наприклад, для структури ІКМ, представленої на рис. 4.6, при передачі КП між R_1 і R_4 «містком» виступає канал між маршрутизаторами R_2 і R_3. Цей «місток» з'єднує два маршрути, які не перетинаються: $R_1 \to R_2 \to R_4$ та $R_1 \to R_3 \to R_4$. Структура ІКМ з «містком» між R_2 і R_3 в залежності від крайніх значень імовірності компрометації каналу $E_{2,3}$ може набувати варіанти з'єднань, які наведені на рис. 4.7.

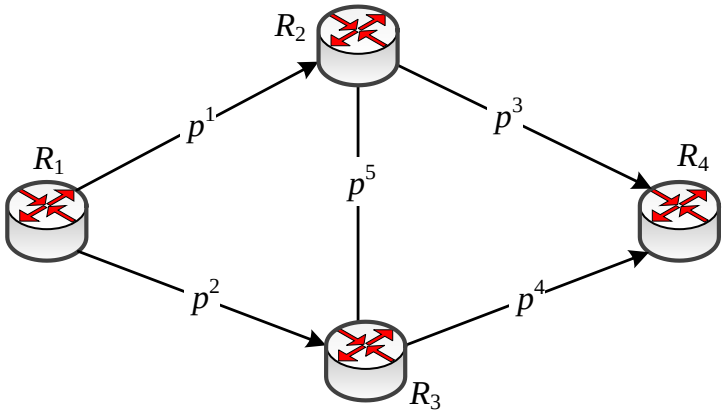
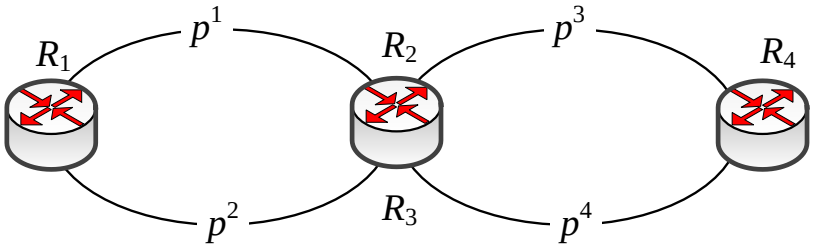
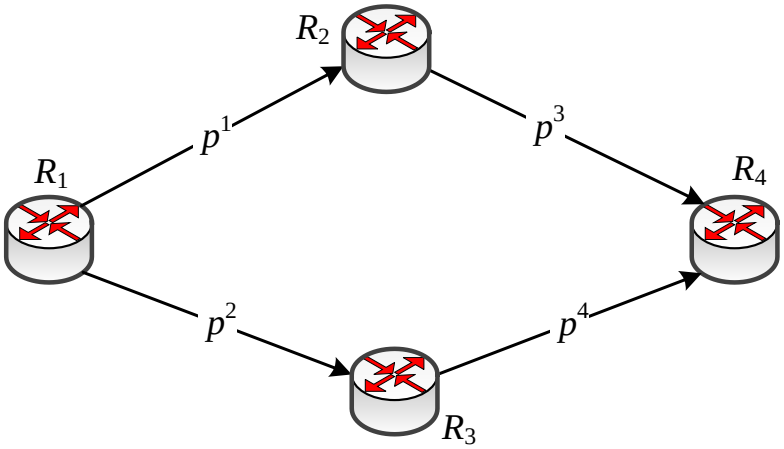


Рисунок 4.6 – Перший досліджуваний фрагмент структури ІКМ



а) $p^5 = 0$



а) $p^5 = 1$

Рисунок 4.7 – Варіанти з’єднань маршрутизаторів ІКМ в залежності від крайніх значень імовірності компрометації каналу $E_{2,3}$

Тобто, якщо канал $E_{2,3}$ абсолютно безпечний ($p^5 = 0$), то структура ІКМ може бути представленою варіантом, представленим на рис. 4.7 а. У випадку компрометації цього ж каналу структура ІКМ може бути описана топологією, наведеною на рис. 4.7 б. Тоді вираз для ймовірності компрометації повідомлення, яке передається між R_1 і R_4, буде записано на основі формули для обчислення повної ймовірності компрометації мережі, наведеної на рис. 4.6:

$$P_{msg} = q_5(1-(1-p_1p_2)(1-p_3p_4)) + p_5(1-q_1q_3)(1-q_2q_4)\,. \qquad (4.16)$$

З метою проведення подальшого порівняльного аналізу визначимо ймовірність компрометації повідомлення, яке передається за двома шляхами, що не перетинаються (рис. 4.7 б):

$$P_{msg} = (1-q_1q_3)(1-q_2q_4)\,. \qquad (4.17)$$

Тоді на рис. 4.8 показано залежність ймовірності компрометації повідомлення (4.16) та (4.17) від імовірностей компрометації каналів зв’язку ІКМ, які в межах даного прикладу вважались однаковими. Тоді на рис. 4.9 наведено числові значення виграшу від використання шляхів, які перетинаються, для структури мережі, наведеної на рис. 4.6. При малих значеннях ймовірності компрометації каналів використання «містка» дозволяло найбільше знизити ймовірність P_{msg}.

На рис. 4.10 показана залежність виграшу щодо значень ймовірності компрометації повідомлення від ймовірності компрометації каналу $E_{2,3}$ (p^5) для різних значень ймовірностей компрометації інших каналів.

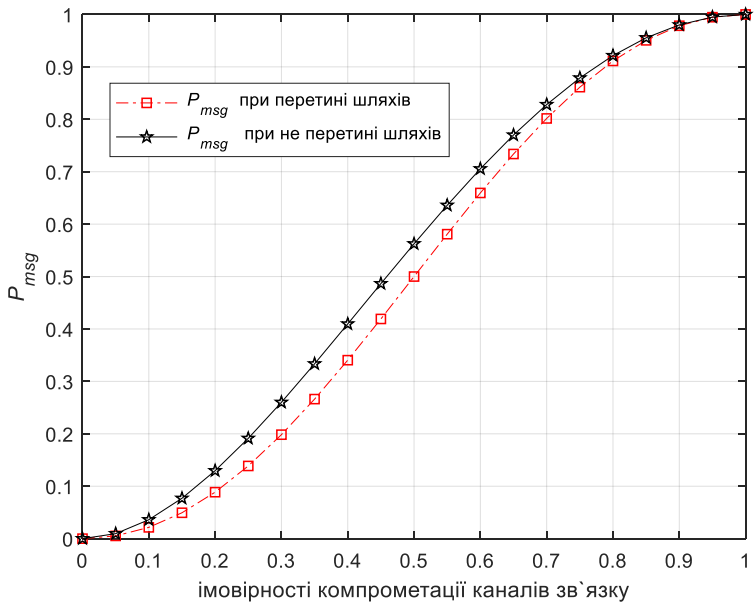


Рисунок 4.8 – Залежність ймовірності компрометації повідомлення (4.16) та (4.17) від імовірностей компрометації каналів зв’язку ІКМ

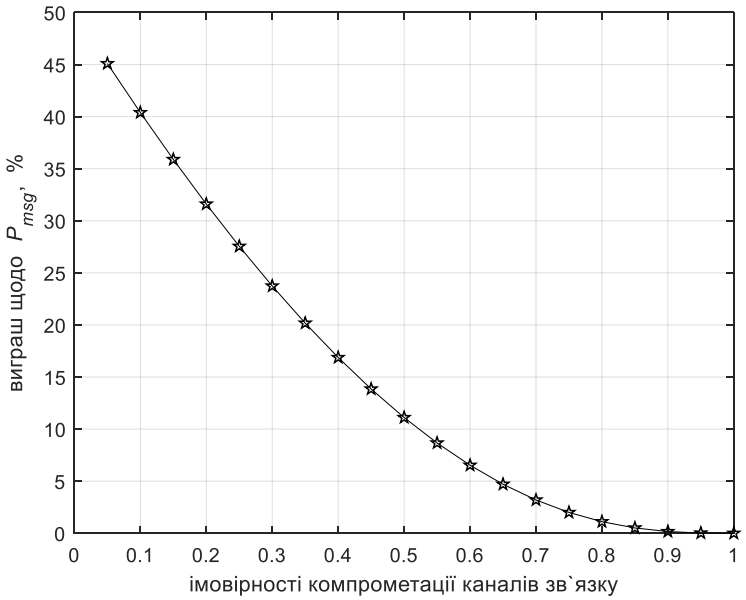


Рисунок 4.9 – Виграш від використання шляхів, які перетинаються, для структури мережі, наведеної на рис. 4.6

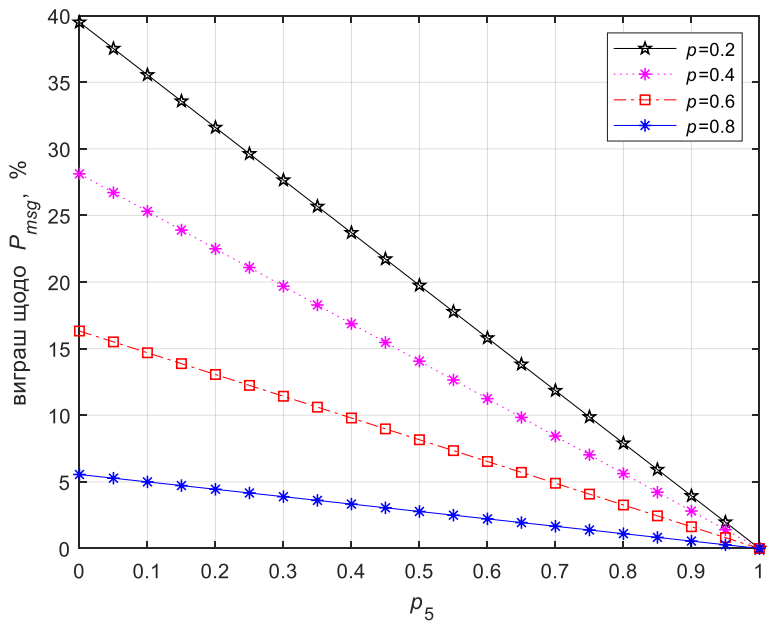


Рисунок 4.10 – Залежність виграшу щодо значень ймовірності компрометації повідомлення від ймовірності компрометації каналу $E_{2,3}$ (p^5) для різних значень ймовірностей компрометації інших каналів

Таким чином, навіть для невеликої структури ІКМ (рис. 4.6) з мінімальним числом каналів та одним «містком» використання шляхів, які перетинаються, дозволяє значно знизити ймовірність компрометації КП. При зміні ймовірності компрометації каналів у діапазоні від 0,05 до 0,7 вдавалось знизити P_{msg} від 3,2% до 45%.

Для більш розмірних структур ІКМ, які містять більшу кількість каналів, а головне «містків», модель отримання аналітичного виразу для ймовірності компрометації КП залишається незмінною. У випадку наявності декількох «містків» структура аналізується послідовно для всіх граничних випадків стану кожного «містка». Продемонструємо цей підхід для більш складної структури мережі, наведеної на рис. 4.11. У цьому випадку ІКМ складалась із восьми каналів та містила три «містки» між парами вузлів R_2 і R_3, R_4 і R_5, R_2 і R_5. Конфіденційне повідомлення передавалось між маршрутизаторами R_1 і R_6.

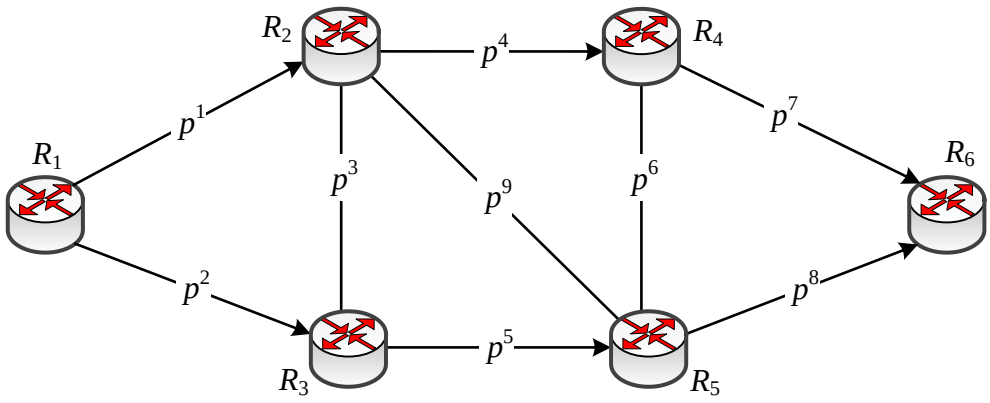
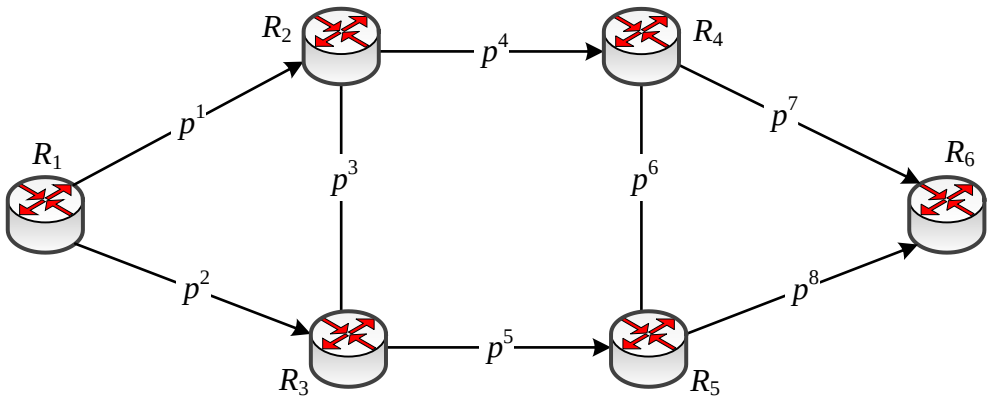


Рисунок 4.11 –Другий досліджуваний фрагмент структури ІКМ

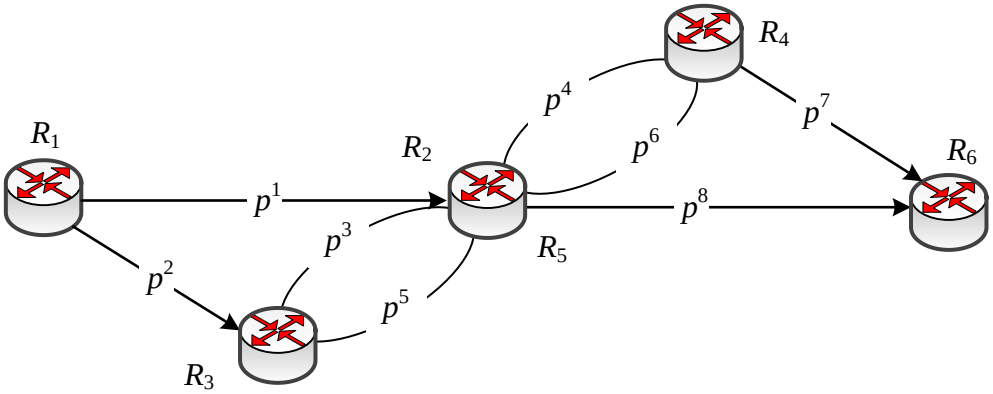
Почнемо аналіз із «містка» між R_2 і R_5, який має ймовірність компрометації p^9. Тоді по аналогії з підходом, показаним на рис. 4.7, в залежності від граничних значень імовірності компрометації цього каналу-«містка» структура ІКМ (рис. 4.11) може аналізуватись у двох варіантах, наведених на рис. 4.12.

Ймовірність компрометації мережі (повідомлення) з двома «містками», структура якої наведена на рис. 4.12 а, позначимо через P_1^*. Ймовірність компрометації мережі (повідомлення), структура якої наведена на рис. 4.12 б, позначимо через P_2^*. Так як ця структура представляє собою паралельно-послідовне з'єднання каналів, то розрахунок значення P_2^* є тривіальною задачею. Тоді ймовірність компрометації повідомлення, а фактично мережі, яка наведена на рис. 4.11, можна розрахувати згідно виразу

$$P_{msg} = p^9 P_1^* + q^9 P_2^* . \qquad (4.18)$$



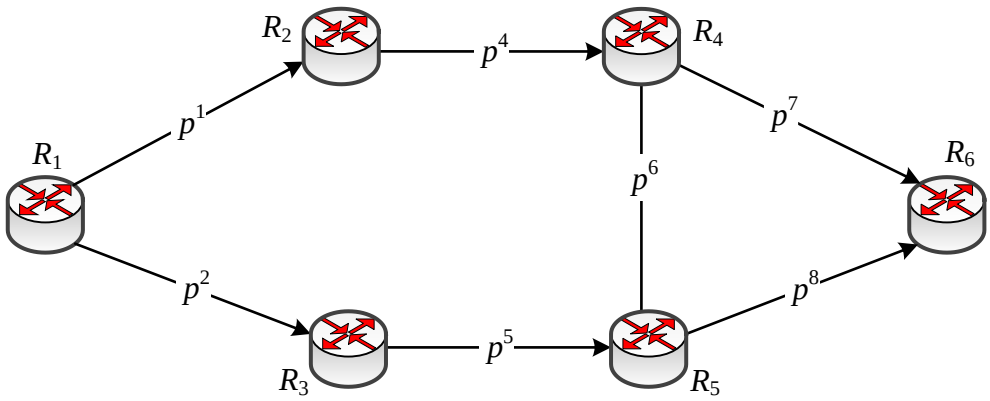
а) $p^9 = 1$



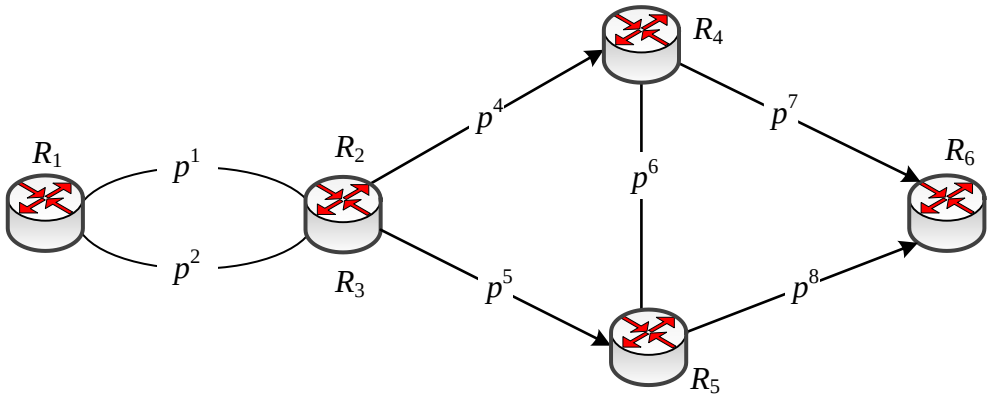
б) $p^9 = 0$

Рисунок 4.12 – Варіанти з’єднань маршрутизаторів ІКМ в залежності від крайніх значень імовірності компрометації каналу $E_{2,5}$

Для розрахунку значення P_1^* розглянемо як «місток» канал між R_2 і R_3. Тоді в залежності від граничних значень імовірності компрометації p^3 цього каналу-«містка» структура ІКМ (рис. 4.12 а) може аналізуватись у двох варіантах, наведених на рис. 4.13.



а) $p^3 = 1$



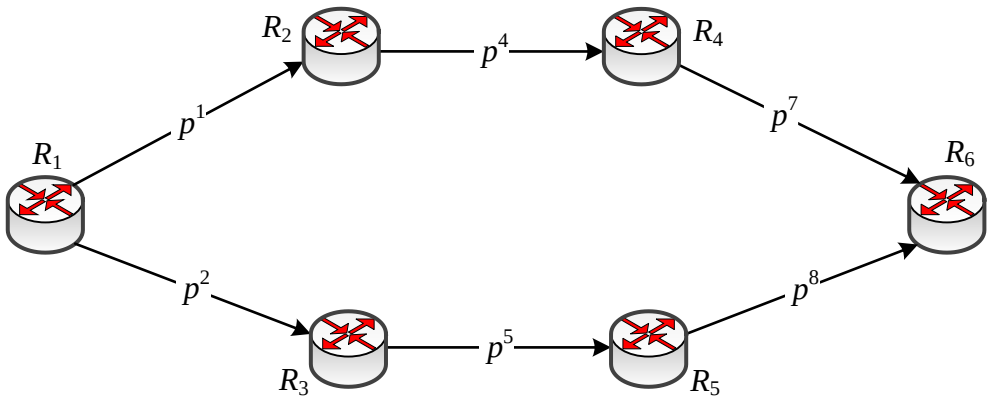
б) $p^3 = 0$

Рисунок 4.13 – Варіанти з’єднань маршрутизаторів ІКМ в залежності від крайніх значень імовірності компрометації каналу $E_{2,3}$

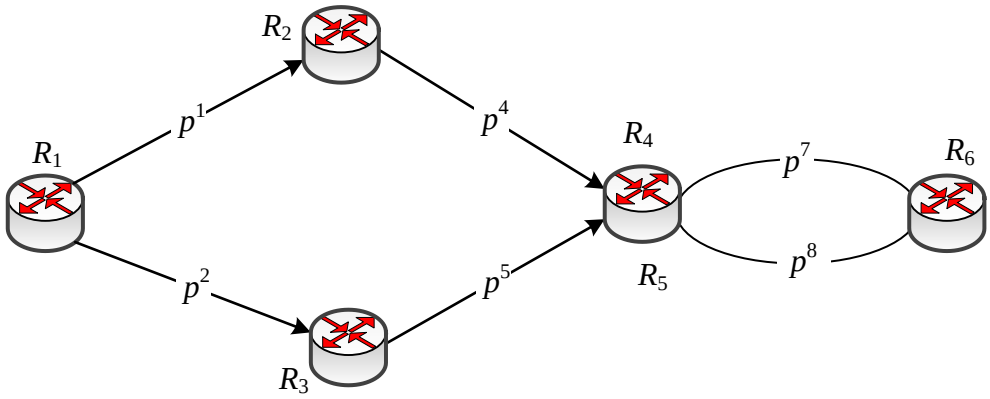
Ймовірність компрометації мережі (повідомлення) з одним «містком», структура якої наведена на рис. 4.13 а, позначимо через P_1^{**}. Ймовірність компрометації мережі (повідомлення), структура якої наведена на рис. 4.13 б, позначимо через P_2^{**}. Тоді ймовірність компрометації повідомлення, а фактично мережі, яка наведена на рис. 4.12 а, можна розрахувати згідно виразу

$$P_1^* = p^3 P_1^{**} + q^3 P_2^{**}. \qquad (4.19)$$

У свою чергу для визначення ймовірності компрометації мережі з одним «містком» (P_1^{**}), який з’єднує вузли R_4 і R_5, в залежності від граничних значень імовірності компрометації p^6 цього каналу-«містка» структура ІКМ (рис. 4.13 а) може також аналізуватись у двох варіантах, наведених на рис. 4.14.



а) $p^6 = 1$



б) $p^6 = 0$

Рисунок 4.14 –Варіанти з’єднань маршрутизаторів ІКМ в залежності від крайніх значень імовірності компрометації каналу $E_{4,5}$

Ймовірність компрометації мережі (повідомлення), яка складається з двох шляхів, які не перетинаються (рис. 4.14 а), позначимо через P_1^{***}. Саме ця ймовірність компрометації КП відповідає рішенню SPREAD та розраховується згідно виразу

$$P_1^{***} = (1 - q_1 q_4 q_7)(1 - q_2 q_5 q_8). \qquad (4.20)$$

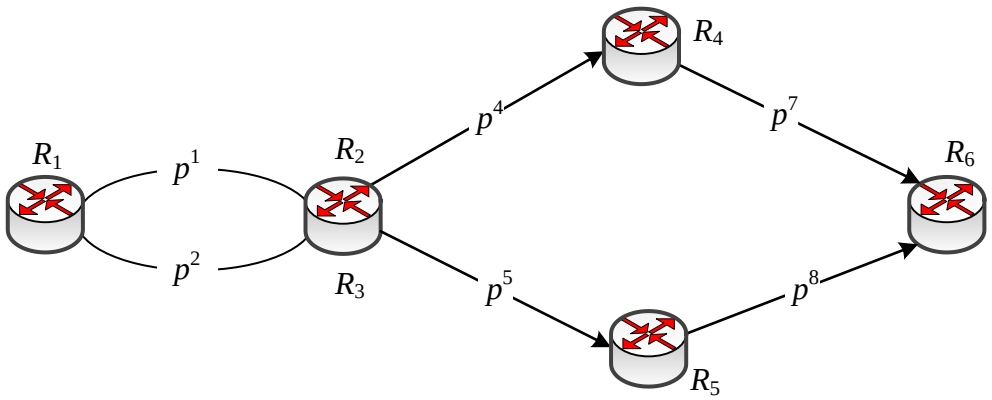
Ймовірність компрометації мережі (повідомлення), структура якої наведена на рис. 4.14 б, позначимо через P_2^{***}. Структури мережі, які наведені на рис. 4.14, представляють собою приклади паралельно-послідовного сполучення її елементів, тому розрахувати ймовірності компрометації P_1^{***} та P_2^{***} нескладно.

Тоді ймовірність компрометації повідомлення, а фактично мережі, яка наведена на рис. 4.13 а, можна розрахувати згідно виразу

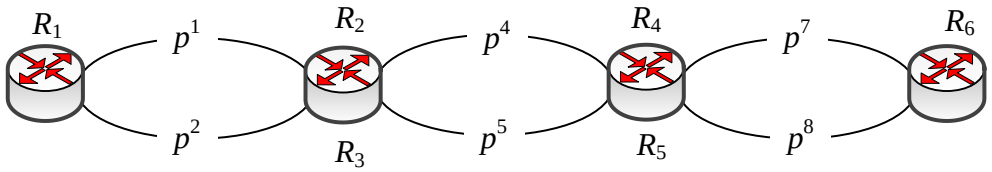
$$P_1^{**} = p^6 P_1^{***} + q^6 P_2^{***}. \qquad (4.21)$$

У свою чергу для визначення ймовірності компрометації мережі, структура якої наведена на рис. 4.13 б, в залежності від граничних значень імовірності компрометації p^6 цього каналу-«містка» топологія ІКМ може також аналізуватись у двох варіантах, наведених на рис. 4.15.

Ймовірність компрометації мережі (повідомлення), яка представлена на рис. 4.15 а), позначимо через P_1^{****}. Ймовірність компрометації мережі (повідомлення), структура якої наведена на рис. 4.15 б, позначимо через P_2^{****}. Структури мережі, які наведені на рис. 4.15, також представляють собою приклади паралельно-послідовного сполучення її елементів, тому розрахувати ймовірності компрометації P_1^{****} та P_2^{****} нескладно.



а) $p^6 = 1$



б) $p^6 = 0$

Рисунок 4.15 – Варіанти з’єднань маршрутизаторів ІКМ в залежності від крайніх значень імовірності компрометації каналу $E_{4,5}$

Тоді ймовірність компрометації повідомлення, а фактично мережі, яка наведена на рис. 4.14 б, можна розрахувати згідно виразу

$$P_2^{**} = p^6 P_1^{****} + q^6 P_2^{****}. \quad (4.22)$$

Таким чином, всі необхідні перетворення проведені, а проміжні ймовірності розраховані, щоб обчислити фінальну ймовірність компрометації повідомлень (4.18) для мережі, структура якої наведена на рис. 4.11.

4.3.2 Результати дослідження ймовірності компрометації конфіденційних повідомлень, яке фрагментовано передається в ІКМ за шляхами, що перетинаються

Проведено детальний аналіз щодо впливу ймовірностей компрометації каналів та кількості «містків» на результуюче значення ймовірності компрометації конфіденційного повідомлення, яке передається в мережі (рис. 4.11) за шляхами, що перетинались. Аналізу піддавались структури ІКМ, які містили різну кількість «містків» (табл. 4.6).

Таблиця 4.6 – Варіанти структур, які аналізувались в ході проведеного дослідження

Номер рішення	Структура ІКМ	Тип шляхів, які використовуються	Формула для розрахунку ймовірності компрометації повідомлень
1	Рис. 4.14 а	шляхи не перетинаються (SPREAD)	(4.20)
2	Рис. 4.13 а	Шляхи перетинаються, 1 «місток»: $E_{4,5}$	(4.21)
3	Рис. 4.12 а	Шляхи перетинаються, 2 «містка»: $E_{2,3}$, $E_{4,5}$	(4.19)
4	Рис. 4.11	Шляхи перетинаються, 3 «містка»: $E_{2,3}$, $E_{4,5}$, $E_{2,5}$	(4.18)

На рис. 4.16 показано залежність ймовірності компрометації повідомлення для різних мережних структур (табл. 4.6) від імовірностей компрометації каналів зв’язку ІКМ, які в межах даного прикладу вважались однаковими.

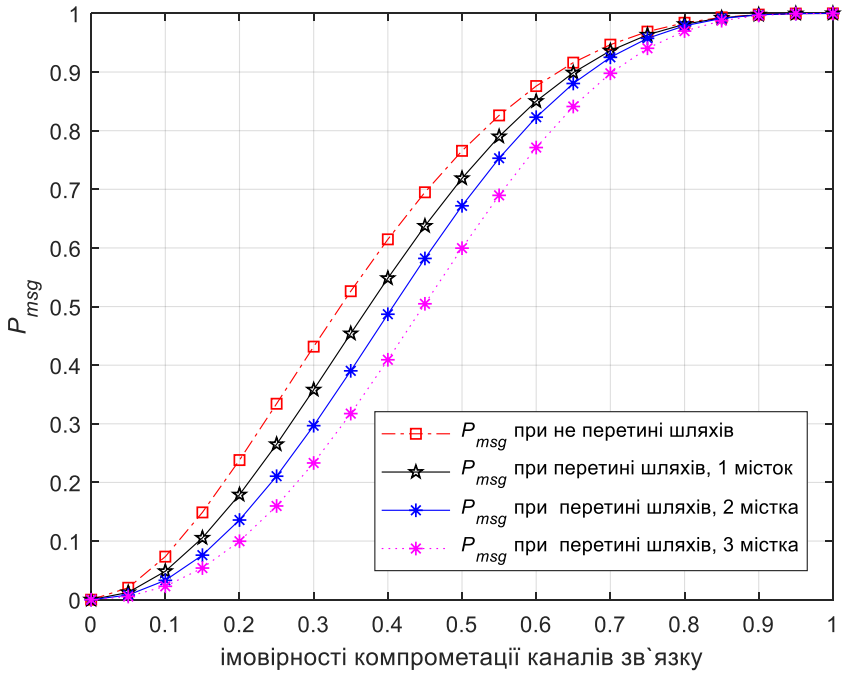


Рисунок 4.16 – Залежність ймовірностей компрометації повідомлення, отриманих для різних мережних структур, від імовірностей компрометації каналів зв’язку

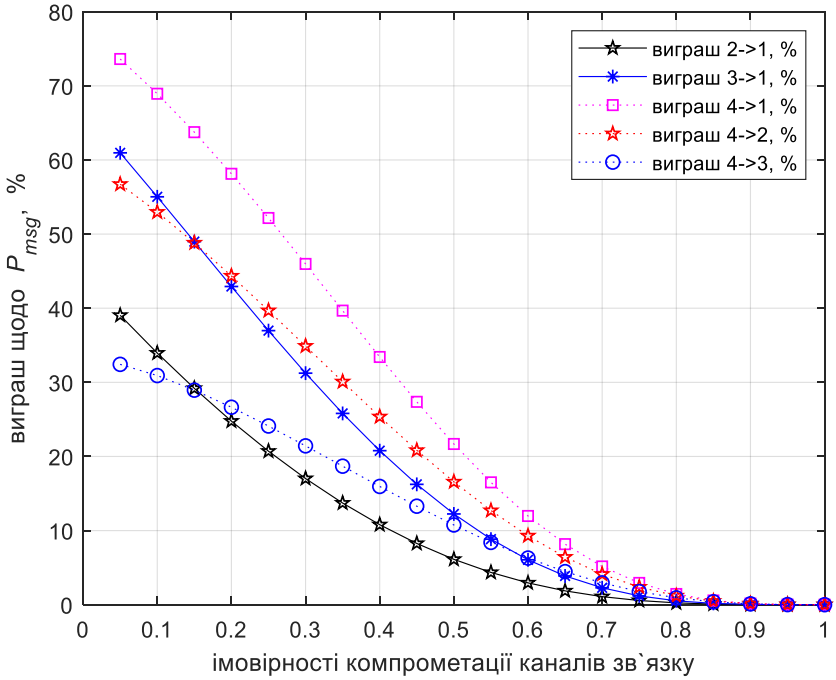


Рисунок 4.17 – Виграш від використання шляхів, які перетинаються, для різних маршрутних рішень (табл. 4.6)

Тоді на рис. 4.17 наведено числові значення виграшу щодо ймовірності компрометації КП від використання рішень 2÷4 (табл. 4.6), які відрізнялись кількістю «містків» у структурі ІКМ, у порівнянні з рішенням SPREAD (рішення №1). На цьому ж рисунку представлені результати порівняння рішення №4, коли використовувались всі три доступні «містки», з рішеннями №2 та №3, коли кількість використаних «містків» становила 1 та 2 відповідно.

Як показали результати дослідження запропонованого методу, найбільший виграш щодо значень ймовірність компрометації повідомлень (у середньому від 20-60%) вдалося отримати в умовах відносно невисокого рівня кіберзагроз у ІКМ, тобто коли ймовірність компрометації каналів (вузлів) зв'язку не перевищувала 0,4. При збільшенні рівня загроз, коли ймовірність компрометації каналів (вузлів) зв'язку збільшувалась до 0,7, виграш щодо значень ймовірність компрометації повідомлень складав у середньому від 3-20%.

Для структури ІКМ (рис. 4.11) збільшення числа «містків» дозволило істотно знизити ймовірність компрометації КП (рис. 4.17). Так, у випадку використання трьох містків (рішення №4, табл. 4.6) вдалось знизити P_{msg} від 3 до 33% у порівнянні з рішенням №3, коли використовувались два «містки»; від 4 до 56% у порівнянні з рішенням №2, коли використовувався один «місток». Таким чином, отримані результати дослідження підтвердили гіпотезу, що при безпечній маршрутизації КП використання шляхів, які перетинаються, призводить до істотного підвищення рівня мережної безпеки в ІКМ.

4.3.3 Метод балансування фрагментів конфіденційного повідомлення за шляхами, які перетинаються

Для забезпечення отриманих у пункті 4.3.2 значень ймовірності компрометації конфіденційних повідомлень необхідно належним чином організувати процес балансування фрагментів КП за шляхами, які перетинаються, в ІКМ. У загальному випадку це нетривіальна задача,

розв’язання якої вимагає деякого перегляду підходу щодо визначення множини шляхів, за якими буде здійснюватися балансування фрагментів КП.

Задля забезпечення виконання умов (4.11) або (4.12) у процесі розв’язання оптимізаційної задачі (4.14) пропонується використовувати лінійно незалежні (один від одного) шляхи, кількість яких у ІКМ розраховується наступним чином

$$\tilde{\mathrm{M}} = V - \rho + 1, \tag{4.23}$$

де $\rho = m - 1$ – це ранг мережі, який на одиницю менше за загальну кількість її вузлів.

Так, наприклад, кількість незалежних шляхів у мережах, що представлені на рис. 4.6 та рис. 4.13 а, дорівнює трьом. Для більш зв’язної структури ІКМ (рис. 4.12 а) число незалежних шляхів збільшилось до чотирьох. Для структури з трьома «містками» (рис. 4.11) число незалежних шляхів дорівнює п’яти.

Для перевірки лінійної незалежності шляхів необхідно використати таку методику:

- провести наскрізну нумерацію каналів зв’язку (e_i, i=$\overline{1,V}$);

- представити кожен з обраних для аналізу шляхів як суму каналів, які його створюють (r_j, j=$\overline{1,\tilde{\mathrm{M}}}$);

- скласти матрицю шляхів $B = \|b_{i,j}\|$, кількість рядків якій визначається числом обраних для аналізу шляхів, а число стовбців відповідає кількості каналів в ІКМ,

$$b_{i,j} = \begin{cases} 1, \text{ якщо } j\text{-й канал входить до } i\text{-го шляху;} \\ 0, \text{ в іншому випадку.} \end{cases}$$

- визначити ранг (rank) матриці шляхів *B*;

- якщо $rank(B) = M$, то обрані для аналізу шляхи є лінійно незалежними.

Продемонструємо вибір лінійно незалежних шляхів на різних мережних структурах. Для цього розглянемо структуру ІКМ, представлену на рис. 4.6. Нехай нумерація каналів e_i співпадає з індексами канальних ймовірностей

компрометації p^i. Тоді перевіримо лінійну незалежність таких шляхів між першим та четвертим маршрутизаторами:

$$\begin{cases} r_1 = e_1 + e_3; \\ r_2 = e_2 + e_4; \\ r_3 = e_1 + e_5 + e_4. \end{cases}$$

Для цього випадку матриця маршрутів буде мати такий вигляд:

$$B = \begin{Vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{Vmatrix}.$$

Ранг цієї матриці дорівнює трьом, що підтверджує правильність вибору цієї множини лінійно незалежних шляхів.

Додатково розглянемо структуру ІКМ, представлену на рис. 4.12 а. Нумерація каналів e_i знову співпадає з індексами канальних ймовірностей компрометації p^i. Перевіримо лінійну незалежність таких шляхів між першим та шостим маршрутизаторами:

$$\begin{cases} r_1 = e_1 + e_4 + e_7; \\ r_2 = e_2 + e_5 + e_8; \\ r_3 = e_1 + e_3 + e_5 + e_8; \\ r_4 = e_2 + e_5 + e_6 + e_7. \end{cases}$$

Для цього випадку матриця маршрутів буде мати такий вигляд:

$$B = \begin{Vmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{Vmatrix}.$$

Ранг цієї матриці дорівнює чотирьом, що підтверджує правильність вибору цієї множини лінійно незалежних шляхів. Проте, у випадку вибору іншої множини шляхів

$$\begin{cases} r_1 = e_1 + e_3 + e_5 + e_8; \\ r_2 = e_2 + e_5 + e_8; \\ r_3 = e_1 + e_3 + e_5 + e_6 + e_7; \\ r_4 = e_2 + e_5 + e_6 + e_7, \end{cases}$$

ранг матриці шляхів

$$B = \begin{Vmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{Vmatrix}$$

буде дорівнювати трьом, що свідчить про лінійну залежність обраної множини шляхів.

Після вибору множини лінійно незалежних шляхів в межах пропонованого методу безпечної маршрутизації здійснюється розв’язання оптимізаційної задачі з мінімізацією цільової функції (4.14) при наявності обмежень (4.10), (4.11) або (4.12) із використанням множини шляхів, які перетинаються ($i=\overline{1,\tilde{M}}$).

4.4 Висновки до четвертого розділу

1. У розділі запропоновано та досліджено два методи безпечної маршрутизації, які можуть бути використані при фрагментованій передачі конфіденційних повідомлень в інфокомунікаційній мережі (ІКМ). Перший метод заснований на розрахунку та використанні шляхів, які не перетинаються, та є подальшим узагальненням механізму безпечної маршрутизації SPREAD. В основу запропонованого методу безпечної маршрутизації конфіденційних

повідомлень за шляхами, що не перетинаються, покладено послідовне розв'язання двох оптимізаційних задач:

– розрахунку маршрутів, що не перетинаються, в інфокомунікаційній мережі за допомогою моделі (4.1)-(4.8);
– безпечного балансування фрагментів конфіденційного повідомлення (4.9)-(4.14) за множиною попередньо розрахованих шляхів (4.1)-(4.8).

2. Модель (4.1)-(4.8) обрана для використання з причини її корисних властивостей щодо розрахунку максимальної кількості шляхів, що не перетинаються, із включенням у них каналів зв'язку з мінімальною ймовірністю компрометації. Модель (4.9)-(4.14) використана з метою забезпечення мінімально можливої ймовірності компрометації повідомлень (4.13), які фрагментовано передавались за попередньо розрахованою множиною шляхів, що не перетинались.

3. Результати проведеного дослідження на обраній мережній конфігурації (рис. 4.2) для трьох різних варіантів ймовірностей компрометації каналів зв'язку ІКМ (рис. 4.3 – рис. 4.5) підтвердили ефективність запропонованого методу безпечної маршрутизації та працездатність закладених в його основу оптимізаційних моделей щодо визначення множини шляхів, що не перетинались, та порядку безпечного балансування за ними фрагментів конфіденційного повідомлення (табл. 4.4). Використання запропонованої оптимізаційної моделі розрахунку шляхів, які не перетинаються, з врахуванням їх рівня мережної безпеки в межах запропонованого методу безпечної маршрутизації дозволила знизити ймовірність компрометації конфіденційних повідомлень в залежності від сценарію компрометації елементів мережі від 23-27% до 47-56%.

4. Запропоновано метод безпечної маршрутизації конфіденційних повідомлень, заснований на використанні шляхів, які можуть перетинатись. Це дозволяє більш повно використати наявний в мережі ресурс щодо пропускної здатності та кіберресурс. В межах даного методу ймовірність компрометації повідомлень розраховується за формулою повної ймовірності з врахуванням рівня мережної безпеки «містків» у структурі ІКМ. Метод не вимагає

попереднього розрахунку множини шляхів, які не перетинаються, що спрощує його реалізацію на практиці.

5. Як показали результати дослідження запропонованого методу, найбільший виграш щодо значень ймовірність компрометації повідомлень (у середньому від 20-60%) вдалося отримати в умовах відносно невисокого рівня кіберзагроз у ІКМ, тобто коли ймовірність компрометації каналів (вузлів) зв'язку не перевищувала 0,4. При збільшенні рівня загроз, коли ймовірність компрометації каналів (вузлів) зв'язку збільшувалась до 0,7, виграш щодо значень ймовірність компрометації повідомлень складав у середньому від 3-20%.

6. В межах запропонованих методів рівень мережної безпеки маршрутів, мережі та конфіденційних повідомлень взагалі оцінювався через ймовірність компрометації каналів зв'язку ІКМ. За необхідності врахування рівня мережної безпеки вузлів (маршрутизаторів) ІКМ вони можуть бути логічно представлені віртуальними каналами зв'язку, які мають вузлову ймовірність компрометації, без зміни змісту запропонованих методів безпечної маршрутизації конфіденційних повідомлень.

7. Представлені методи безпечної маршрутизації конфіденційних повідомлень отримали програмну реалізацію та представлені програмними прототипами протоколів безпечної маршрутизації у середовищі MATLAB та Python. Ці прототипи можу стати основою перспективних протоколів маршрутизації з підтримкою метрик мережної безпеки для подальшого застосування в традиційних IP/MPLS-мережах та програмно-конфігурованих мережах.

8. Перспективи подальших досліджень в області безпечної маршрутизації в інфокомунікаційній мережі пов'язані з урахуванням не тільки ймовірності компрометації каналів зв'язку, але й інших важливих показників мережної безпеки.

5 ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ З ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ ЗАПРОПОНОВАНИХ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ ТА ПРОТОКОЛІВ ВЗАЄМОДІЇ ДЛЯ ВІДОМИХ ЗАСТОСУВАНЬ І НОВИХ СИСТЕМ ВІДСТЕЖЕННЯ КОНТАКТІВ, ОБРОБКИ ТА ДЕПЕРСОНАЛІЗАЦІЇ ДАНИХ

У цьому розділі будуть наведені протоколи взаємодії для системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань. Основними допоміжними інструментами для таких протоколів можна вважати алгоритми кільцевих підписів та так звані алгоритми Безпосередньої Анонімної Атестації (DAA – Direct Anonymous Attestation). Базова ідея таких протоколів взаємодії полягає у наступному: користувач надає певному Авторизованому Центру (це може бути довільна авторизована державна установа, зокрема заклад охорони здоров’я) певну інформацію стосовно цього користувача, але при цьому ця інформація буде містити лише вибіркові дані, які стосуються сфери повноважень саме цієї установи. Більш того, інформацію можна надати анонімно, але разом з підтвердженням того, що особа, яка її надає, дійсно є обізнаною з цією інформацією, або потенційно має доступ до неї.

Кільцеві підписи більш зручно використовувати у ситуації, коли потрібно анонімно надати якусь інформацію, при цьому підтвердивши доступ до неї. Наприклад, це може бути інформація про контакти хворого або про громадські місця, які він відвідував. При цьому інформація може бути надана як самим хворим, так і кимось із його контактів. Така інформація дозволить попередити інших людей, які також є контактерами, про те, що їм потрібно певний час бути на самоізоляції, при цьому не розголошуючи джерело інформації, або навіть не розголошуючи, хто саме з контактів виявився хворим.

Протоколи БАА пристосовані трохи для інших застосувань. Спробуємо це пояснити на такому прикладі. Припустимо, що користувач має деякий електронний носій, який містить деякий, досить значний, набір інформації про цього користувача. Наприклад, це може бути така інформація:

– паспортні дані;
– ідентифікаційний код;
– інформація про громадянство;
– інформація про власність;
– інформація про сплату податків;
– інформація про місце реєстрації;
– інформація про доступ до інформації певного типу;
– медична інформація (діагнози певних хронічних хвороб, протоколи лікування, які було застосовано, щеплення, тощо);
– інформація про освіту;
– інформація про подорожі та перебування на території інших країн, тощо.

Припустимо також, що цей носій створений та виданий певним уповноваженим органом, а вся інформація на ньому підписана певним способом, за певними алгоритмами, що дозволяє розкривати інформацію з різною стелінню деталізації – саме такі алгоритми підпису дозволяють будувати протоколи БАА. Тоді, з використанням цих криптографічних механізмів, буде забезпечено наступне: кожен державний заклад, в межах своєї компетенції, може отримати інформацію з цього носія лише у тій частині та обсязі, яка стосується безпосередньо цього закладу. Наприклад, працівники поліції отримають інформацію, що дана особа має валідне водійське посвідчення, є власником даної машини та зареєстрована за певною адресою; прикордонна служба матиме доступ до інформації про громадянство, про відвідування певних країн та про наявні щеплення; медичні працівники будуть мати доступ до відповідних медичних даних, і т.п. При цьому сам доступ до інформації може бути трьох типів: повний, частковий та "нульовий".

У цьому розділі ми спочатку розглянемо механізми кільцевого підпису та БАА, після чого сформулюємо, як саме можна їх використовувати для побудови відповідних протоколів. Крім того, ми наведемо новий алгоритм кільцевого підпису, який має наступні переваги:

– суттєво менша довжина підпису та час роботи алгоритму, у порівнянні з тими алгоритмами, що використовують функцію типу RSA;

– суттєво вища стійкість, у порівнянні з тими алгоритмами, що використовують функцію типу RSA;

– вдвічі менша довжина ключа та у стільки ж менший обсяг обчислень у порівнянні з іншими алгоритмами, що використовують операцію спарювання.

5.1 Поняття кільцевого підпису та огляд основних робіт

Кільцеві підписи дають можливість користувачам підписувати повідомлення у такий спосіб, що можна ідентифікувати лише кільце можливих підписантів (тобто множину тих, хто потенційно міг би бути підписантом), але неможливо визначити, хто саме з цієї множини створив підпис на повідомленні. Можна назвати три основних напрямки застосування кільцевих підписів:

– для збереження анонімності джерела інформації, з підтвердженням при цьому компетентності цього джерела;

– у особистому листуванні, для запобігання підтвердження авторства отриманого листа другою стороною;

– для доведення права доступу без розголошення особи.

У цьому розділі спочатку ми наведемо стислий огляд робіт стосовно алгоритмів кільцевих підписів, розглянемо історію появи та розвитку таких алгоритмів. Після огляду буде коротко описано одне з найцікавіших на сьогоднішній день застосувань таких підписів – у криптовалюті Monero, для забезпечення анонімності транзакції.

У наступних підрозділах ми розглянемо три основні способи побудови кільцевих цифрових підписів:

– з використанням симетричного та несиметричного алгоритмів шифрування;

– з використанням геш-функцій;

– з використанням операції спарювання на еліптичних кривих.

У кінці розділу буде запропоновано новий алгоритм кільцевого підпису з використанням операції спарювання, який є більш швидким та вимагає меншої кількості відкритих ключів, ніж існуючий.

Поняття кільцевого підпису вперше ввели Rivest, Shamir та Tauman [81], після чого цей напрямок почав активно досліджуватись та розвиватись. Були знайдені деякі вразливості вихідного алгоритму та запропоновані більш стійкі; також були запропоновані алгоритми кільцевого підпису, які мають певні бажані властивості – більше інформації про це можна знайти в роботах [82-90]. Кільцеві підпису де в чому є схожими на групові підписи, але між ними існує велика різниця – і у самій моделі підпису, і у їх призначенні [91]. З одного боку, групові підписи мають додаткову властивість – можливість відкрити особу анонімного підписувача (у випадку його некоректної поведінки) менеджером групи. З іншого боку, кільцеві підписи мають більшу гнучкість та децентралізацію: не існує ніякої довіреної сторони, такої як менеджер групи, яка має додаткову інформацію та додаткові повноваження, а також координує спільну роботу групи підписантів. Більш того, інші користувачі, яких справжній підписант включив до свого кільця, можуть навіть не знати про те, що він використовує їх відкриті ключі. Величину кільця також можна обирати довільну, підвищуючи у такий спосіб імовірність знайти справжнього підписанта. Існує величезна кількість різних застосувань кільцевих підписів (наприклад, описані у роботах [81, 83, 87, 90]).

Найперше застосування кільцевих підписів мало на меті можливість анонімного розкриття деякого секрету, при чому спосіб розкриття повинен був мати такі властивості:

– той, хто перевіряє підпис, буде переконаний, що секрет розкрила деяка особа, яка справді має до нього доступ (наприклад, якщо кільце складається з

співробітників деякої спецслужби, відкриті ключі яких можна перевірити на якомусь офіційному сайті);

– неможливо визначити, хто саме з учасників кільця підписав повідомлення.

Кільцеві підписи також можна використовувати для того, щоб надати певній групі людей доступ до якихось джерел інформації, не розкриваючи, хто саме з них користувався цією інформацією. Також цікавою та корисною є можливість отримати часткову анонімність [92], використовуючи кільце з двох осіб. Наприклад, Аліса хоче розповісти Бобу дещо компрометуюче про Еву. Аліса надсилає Бобу лист з повідомленням, підписаним кільцевим підписом, де кільце складається з двох осіб – Аліси і Боба. Боб знає, що він не писав цього листа, отже він переконаний, що лист від Аліси. Проте він не зможе переконати Еву, що Аліса знає її секрет та написала цього листа – з точки зору Еви, автором повідомлення можуть бути, з однаковою імовірністю, і Аліса, і Боб.

Інші застосування кільцевого підпису для кільця з двох підписантів також можна знайти в [93].

Окремо зазначимо роботу [94]. Ця робота зосереджена як на нових визначеннях стосовно кільцевих підписів, так і на їх конструкціях. Вихідна робота стосовно кільцевих підписів не обґрунтовує їх стійкість настільки строго, як це вимагається зараз. Зокрема, при обґрунтуванні стійкості неявно припускається, що відкриті ключі всіх учасників кільця побудовані коректно, тобто відповідні їх секретні ключі були вибрані випадково. Робота [94] якраз і обґрунтовує стійкість запропонованого алгоритму кільцевого підпису навіть у випадках, коли один з учасників кільця є зловмисником. Також у цій роботі наведено ряд корисних визначень стосовно стійкості схем кільцевих підписів.

Слід зазначити, що на рівні держав використання кільцевих підписів є суттєво меншим, ніж звичайних цифрових підписів. Проте ці підписи достатньо

успішно використовуються у криптовалютах – основними прикладами можна вважати крипто валюти CryptoNote[25], Bytecoin[26] (BCN) та Monero[27].

Розробник «найголовнішої» анонімної криптовалюти Monero [95] Рікардо Спаньї вважає, що цифровій індустрії необхідна фінансова приватність. В іншому випадку, ринок буде заповнений таргетованою (направленою) рекламою, а в гіршому – почнуться злочини, направлені на власників значної суми криптовалют (адже з «традиційного» блокчейну кожен може дізнатися баланс будь-якого чужого біткоін-гаманця). Monero – це поки єдина монета, всі операції з якою є анонімними за замовчуванням. Для всіх інших криптовалют функцію анонімності потрібно додатково налаштовувати (як BTC-міксери) або підключати при проведенні транзакції (як у криптовалюті Dash).

Не дивлячись на те, що всі знають, що ця валюта забезпечує високий рівень приватності, далеко не всі розуміють, які саме криптографічні механізми забезпечують цю анонімність.

З публічного блокчейну Monero можна дізнатись, чи існує та чи інша адреса рахунку, але неможливо перевірити баланс цього рахунку та отримати доступ до історії транзакцій, з ним пов’язаних. Анонімність Monero забезпечується наступними складними криптографічними засобами та механізмами:

– *кільцевими конфіденційними транзакціями* з використанням доведення діапазону та криптографічними коммітментами (підтвердженнями), які дозволяють приховувати величини коштів, що пересилаються у транзакції,

– *неінтерактивними доведеннями без розголошень*, які дозволяють перевіряти транзакцію без знання відправника та отримувача коштів, без знання кількості монет та без використання довіреної сторони;

[25] https://en.wikipedia.org/wiki/CryptoNote
[26] https://en.wikipedia.org/w/index.php?title=Ring_signature&oldid=795547045#cite_note-9
[27] https://en.wikipedia.org/wiki/Monero_(cryptocurrency)

– *одноразовими адресами*, та *одноразовими відкритими ключами*, які користувач повинен генерувати за допомогою криптографічних механізмів та які приховують шлях пересування коштів;

– *кільцевими підписами*, що дозволяють приховати, з якої саме адреси (з певної групи, що складається з 11 адрес) було відправлено кошти.

Ще однією безумовною перевагою є відкритий код цієї криптовалюти та високий ступінь довіри до її розробників у криптовалютному суспільстві.

До недоліків Monero можна віднести високі комісії за транзакції.

5.2 Загальна ідея побудови алгоритмів кільцевих підписів

У цьому параграфі розглянемо, як виглядає алгоритм кільцевого підпису в загальному вигляді [81]. Після цього у наступних параграфах ми наведемо три основні способи побудови алгоритмів кільцевого підпису та стислий порівняльний аналіз цих алгоритмів.

Для побудови алгоритму кільцевого підпису нам будуть потрібні наступні криптографічні об’єкти, які ми будемо позначати GRSP (general ring signature parameters).

$h: V^* \to V_n$ – криптографічна геш-функція;

$g_i : D \to D,\ i = \overline{1,l}$ – набір однобічних функцій, або функцій з секретом, або асиметричних алгоритмів шифрування, де i -та функція належить i -му учаснику кільця, $D \subset V_n$ а l є розміром кільця;

$K_i,\ i = \overline{1,l}$ – набір відповідних відкритих ключів всіх учасників кільця (тобто K_i є відкритим ключем алгоритму зашифрування g_i);

g_s, K_s, k_s для деякого $s \in \{1,...,l\}$ – функція, відкритий ключ та секретний ключ, відповідно, які належать s-му учаснику кільця, який і є справжнім підписантом.

Також позначимо M повідомлення, яке буде підписуватись.

Нагадаємо, що кільце, тобто учасників підпису, підписувач обирає сам перед початком процесу підписування. Для цього йому потрібно знати лише відкриті ключі цих учасників. Вони можуть при цьому навіть не знати, що їх ключі будуть використовуватись.

Зараз ми наведемо загальний алгоритм побудови кільцевого підпису. З такого алгоритму не зовсім зрозуміло, як будується основне рівняння підпису, але він потрібен нам для того, щоб передати основну ідею, на якій базується створення такого підпису. Тут ми дамо лише необхідні властивості, які повинно мати рівняння підпису, щоб ця ідея могла бути реалізованою. Потім на конкретних прикладах стане більш зрозуміло, як може будуватись таке рівняння.

5.2.1 Алгоритм формування підпису (у загальному вигляді)

1. Обчислити $k = h(M)$.

2. Випадково обрати $v \in V_n$.

3. Випадково обрати $x_1,...,x_{s-1},x_{s+1},...,x_l \in D$.

4. Використовуючи відкриті ключі учасників кільця, обчислити $y_i = g_i(x_i)$, $i = \overline{1,n}$, $i \neq s$. Зазначимо, що *саме на цьому етапі підписант використовує відкриті ключі* K_i, $i = \overline{1,l}$, $i \neq s$ *всіх інших учасників* для обчислення значень відповідних однобічних функцій або результатів застосування відповідних асиметричних алгоритмів зашифрування.

5. Побудувати рівняння кільцевого підпису:

$$C_{k,v}(y_1,...,y_l) = v. \tag{5.1}$$

6. З рівняння (5.1) знайти y_s.

7. Використовуючи свій секретний ключ k_s, обчислити $x_s = g_s^{-1}(y_s)$.

8. Сформувати підпис $S = (v; x_1,...,x_l)$.

5.2.2 Алгоритм перевіряння підпису (у загальному вигляді)

1. Використовуючи відкриті ключі учасників кільця, для всіх $x_1,...,x_l$ обчислити $y_i = g_i(x_i)$.

2. Обчислити $k = h(M)$.

3. Перевірити виконання рівності (5.1).

4. Якщо рівність (5.1) виконується, підпис приймається, в іншому випадку підпис вважається недійсним.

З наведених алгоритмів природнім чином випливають властивості, які повинно мати рівняння (5.1).

1. Всі змінні $y_1,...,y_l$ повинні входити в нього симетрично, інакше можна буде виявити справжнього підписанта.

2. При фіксованих значеннях $k, v, y_1,...,y_{s-1}, y_{s+1},...,y_l$ функція $C_{k,v}(y_1,...,y_l)$ повинна бути бієкцією, тобто повинна виконуватись така вимога:

$$\forall k \in V_m, v \in V_n, y_1,...,y_{s-1}, y_{s+1},...,y_l \in D \; \exists! y_s \in D : C_{k,v}(y_1,...,y_l) = v.$$

3. Рівняння (5.1), при фіксованих значеннях $k, v, y_1,...,y_{s-1}, y_{s+1},...,y_l$, повинно легко розв’язуватись відносно y_s.

5.3 Кільцеві підписи, що використовують симетричні алгоритми шифрування

Тепер розглянемо один з варіантів рівняння (5.1) на конкретному прикладі з самої першої роботи [81] за цією темою.

У цьому прикладі в якості однобічної функції з секретом, що буде використовуватись для асиметричного шифрування, виберемо RSA-функцію. Тобто ми будемо вважати, що i-ий учасник кільця має свій відкритий ключ

$K_i = (n_i, e_i)$, де n_i є добутком двох простих Блюма, $(e_i, \varphi(n_i)) = 1$, $i = \overline{1,l}$. Відповідний секретний ключ будемо позначати d_i.

Крім GRSP об'єктів, перелічених вище для загального алгоритму кільцевого підпису, потрібно буде ще симетричний алгоритм шифрування:

$E_k : V_m \to V_m$ – деякий симетричний алгоритм шифрування, $k \in V_n$;

$D_k : V_m \to V_m$ – відповідний алгоритм розшифрування.

Також для спрощення викладок будемо вважати, що розмір кільця $l = 3$. Загальний випадок нічим не відрізняється від випадку потрійного кільця, крім більш громіздких викладок.

Також вважаємо, що справжнім підписантом є учасник кільця з номером 2, тобто $s = 2$.

5.3.1 Алгоритм формування підпису

1. Обчислити $k = h(M)$.

2. Випадково обрати $v \in V_n$.

3. Випадково обрати $x_1, x_3 \in D$.

4. Використовуючи відкриті ключі учасників кільця, обчислити $y_i = g_i(x_i) = x_i^{e_i} \bmod n_i$, $i = 1,3$.

5. Побудувати рівняння кільцевого підпису (тут відомі всі величини, крім y_2):

$$E_k\left(y_3 \oplus E_k\left(y_2 \oplus E_k\left(y_1 \oplus v\right)\right)\right) = v. \qquad (5.2)$$

6. З рівняння кільцевого підпису знайти y_2 (нижче буде пояснення, як сааме це можна зробити).

7. Використовуючи свій секретний ключ d_2, обчислити $x_2 = g_2^{-1}(y_2) = y_2^{d_2} \bmod n_2$.

8. Сформувати підпис $S = (v;\, x_1, x_2, x_3)$.

Покажемо, як знайти y_2 з рівняння (5.2). Спочатку до лівої і правої частини рівняння застосуємо перетворення розшифрування D_k, після чого отримаємо:

$$y_3 \oplus E_k\left(y_2 \oplus E_k\left(y_1 \oplus v\right)\right) = D_k\left(v\right).$$

Тепер до лівої і правої частини додаємо (XOR) величину y_3, після чого знову до обох частин застосуємо перетворення D_k; отримаємо:

$$y_2 \oplus E_k\left(y_1 \oplus v\right) = D_k\left(y_3 \oplus D_k\left(v\right)\right),$$

звідки легко знайдемо y_2 як

$$y_2 = D_k\left(y_3 \oplus D_k\left(v\right)\right) \oplus E_k\left(y_1 \oplus v\right).$$

Аналогічно обчислюється підпис для більшої кількості учасників та для іншого значення s.

5.3.2 Алгоритм перевіряння підпису

1. Використовуючи відкриті ключі учасників кільця, для $x_1, x_2, x_3 \in D$ обчислити $y_i = g_i\left(x_i\right) = x_i^{e_i} \bmod n_i$, $i = \overline{1,3}$.

2. Обчислити $k = h\left(M\right)$.

3. Перевірити виконання рівності (5.2).

4. Якщо рівність (5.2) виконується, підпис приймається, в іншому випадку підпис вважається недійсним.

5.4 Кільцеві підписи, що використовують криптографічну геш-функцію

Перевагою таких підписів є те, що для них не потрібен симетричний алгоритм шифрування. Але необхідність у однобічній функції або асиметричному алгоритмі шифрування певного типу все одно залишається. Тут також вважаємо, що справжній підписував має номер s.

5.4.1 Алгоритм формування підпису

1. Випадково обрати $V \in V_n$.

2. Випадково обрати $x_1,...,x_{s-1},x_{s+1},...,x_l \in D$.

3. Використовуючи відкриті ключі учасників кільця, обчислити $y_i = g_i(x_i) = x_i^{e_i} \bmod n_i$, $i = \overline{1,n}$, $i \neq s$.

4. За допомогою обраного у пункті 1 $V \in V_n$, обчислити таке $v \in V_n$, що:

$$v = H\Big(M \parallel y_n \oplus H\Big(M \parallel y_{n-1} \oplus ... \oplus H\big(M \parallel y_{s+1} \oplus H(M \parallel v)...\big)\Big)...\Big) \qquad (5.3)$$

(нижче буде пояснення, як саме його обчислити, і чому в цьому рівнянні немає V).

5. З рівняння (5.3) кільцевого підпису знайти y_s (нижче буде пояснення, як саме це можна зробити).

6. Використовуючи свій секретний ключ d_s, обчислити $x_s = g_s^{-1}(y_s) = y_s^{d_s} \bmod n_s$.

7. Сформувати підпис $S = (v; x_1,...,x_n)$.

Тепер на прикладі кільця з чотирьох учасників покажемо, як знаходити потрібне значення $v \in V_n$ для побудови (5.3) та як потім знаходити y_s, що є розв'язком цього рівняння.

Отже, нехай $l = 4$.

Для кільця з чотирьох учасників, рівняння (5.3) повинно мати наступний вигляд:

$$v = H\Big(M \parallel \Big(y_4 \oplus H\Big(M \parallel \Big(y_3 \oplus H\Big(M \parallel \big(y_2 \oplus H\big(M \parallel (y_1 \oplus v)\big)\big)\Big)\Big)\Big)\Big)\Big). \qquad (5.4)$$

Розглянемо варіанти вибору підходящого $v \in V_n$ для різних значень s. Якщо при цьому, наприклад, $s = 4$, то обчислення вектору v відбувається так:

1. Випадково обраємо $V \in V_n$.

2. Випадково обираємо $x_1,...,x_{s-1},x_{s+1},...,x_l \in D$.

3. Використовуючи відкриті ключі учасників кільця, обчислюємо $y_i = g_i(x_i) = x_i^{e_i} \bmod n_i$, $i = \overline{1,n}$, $i \neq s$.

4. Обчислюємо $v = H(M \| V)$.

Тобто при побудові (5.4), враховуючи п.п. 3 і 4, повинна виконуватись рівність:

$$V = y_4 \oplus H\Big(M \| \Big(y_3 \oplus H\Big(M \| \Big(y_2 \oplus H\big(M \| (y_1 \oplus v)\big)\Big)\Big)\Big)\Big), \qquad (5.5)$$

або, що те ж саме,

$$y_4 = V \oplus U,$$

де

$$U = H\Big(M \| \Big(y_3 \oplus H\Big(M \| \Big(y_2 \oplus H\big(M \| (y_1 \oplus v)\big)\Big)\Big)\Big)\Big)$$

і може бути легко обчислено.

Звідси видно, що вибором $V \in V_n$ ми повністю визначаємо і $v \in V_n$, і $y_4 \in V_n$ (нагадаємо, що всі інші $y_i \in V_n$, крім $y_4 \in V_n$, вже обчислені у п.3, і змінювати можна тільки y_4), причому обидва ці значення можуть бути легко обчислені.

Формально, у цьому випадку пункти 5, 6 і 7 алгоритму підпису будуть виглядати так:

5. Обчислити

$$y_4 = V \oplus U,$$

де

$$U = H\Big(M \| \Big(y_3 \oplus H\Big(M \| \Big(y_2 \oplus H\big(M \| (y_1 \oplus v)\big)\Big)\Big)\Big)\Big).$$

6. Використовуючи свій секретний ключ d_s, обчислити $x_s = g_s^{-1}(y_s) = y_s^{d_s} \bmod n_s$.

7. Сформувати підпис $S = (v; x_1, ..., x_n)$.

У випадку $s = 3$ обчислення будуть виконуватись трохи інакше, хоча основна ідея залишається такою ж: ми спочатку вибираємо довільне випадкове

$V \in V_n$, обчислюємо $v \in V_n$, а потім користуючись тим, що y_s може бути довільним, вибираємо його у такий спосіб, щоб виконувалось рівняння (5.4).

Для кращого розуміння, розберемо ще випадки, коли $s = 3$ та $s = 2$.

Випадок $s = 3$.

1. Випадково обираємо $V \in V_n$.

2. Випадково обираємо $x_1, ..., x_{s-1}, x_{s+1}, ..., x_l \in D$.

3. Використовуючи відкриті ключі учасників кільця, обчислюємо $y_i = g_i(x_i) = x_i^{e_i} \bmod n_i$, $i = \overline{1,n}$, $i \neq s$.

4. Обчислюємо

$$v = H\left(M \| \left(y_4 \oplus H\left(M \| V\right)\right)\right)$$

та

$$U = H\left(M \| \left(y_2 \oplus H\left(M \| \left(y_1 \oplus v\right)\right)\right)\right)$$

(значення U немає у загальному алгоритмі, ми його тут обчислюємо лише для зручності подальших обчислень).

5. Обчислюємо

$$y_3 = V \oplus U.$$

6. Використовуючи свій секретний ключ d_3, обчислюємо

$$x_3 = g_3^{-1}(y_3) = y_3^{d_3} \bmod n_3.$$

7. Формуємо підпис $S = (v; x_1, ..., x_4)$.

Випадок $s = 2$.

1. Випадково обираємо $V \in V_n$.

2. Випадково обираємо $x_1, ..., x_{s-1}, x_{s+1}, ..., x_l \in D$.

3. Обчислюємо $y_i = g_i(x_i) = x_i^{e_i} \bmod n_i$, $i = \overline{1,n}$, $i \neq s$.

4. Обчислюємо

$$v = H\left(M \,\|\, \left(y_4 \oplus H\left(M \,\|\, \left(y_3 \oplus H\left(M \,\|\, V\right)\right)\right)\right)\right)$$

та

$$U = H\left(M \,\|\, \left(y_1 \oplus v\right)\right).$$

5. Обчислюємо

$$y_2 = V \oplus U.$$

6. Використовуючи свій секретний ключ d_2, обчислюємо

$$x_2 = g_2^{-1}\left(y_2\right) = y_2^{d_2} \bmod n_2.$$

7. Формуємо підпис $S = \left(v;\, x_1, ..., x_4\right)$.

Алгоритм перевіряння підпису є дуже простим і, звичайно, не залежить від того, який номер у справжнього підписувача.

5.4.2 Алгоритм перевіряння підпису

1. Використовуючи відкриті ключі учасників кільця, обчислити $y_i = g_i\left(x_i\right),\ i = \overline{1,n}$.

2. Перевірити виконання рівності (5.4).

3. Якщо рівність (5.4) виконується, підпис приймається, в іншому випадку підпис вважається недійсним.

Наведені вище два типи алгоритмів кільцевих підписів мають один спільний недолік – вони потребують використання асиметричного алгоритму шифрування типу RSA, або RSA-подібної однобічної функції з секретом. Оскільки безпека таких функцій зараз суттєво знизилась, то для забезпечення стійкості цих алгоритмів потрібно обирати величезні параметри для таких функцій (прості числа розміром від 2000 біт), що суттєво знижує швидкодію алгоритму і робить його незручним на практиці. Тому постає питання щодо створення відповідних алгоритмів, що базуються на еліптичних кривих, для яких

не існує субекспоненційних алгоритмів розв’язку задачі DLP, а в недалекій перспективі – взагалі постквантових алгоритмів.

Нижче ми наведемо якраз два таких алгоритми. Але вони базуються не просто на використанні складності розв’язку задачі DLP, а на операції спарювання на еліптичних кривих, що, по-перше, суттєво ускладнює вимоги до еліптичних кривих, придатних до використання в цих алгоритмах, а по-друге – робить обчислювання більш складними. Проте навіть враховуючи їх складність, вони будуть працювати швидше, ніж два попередніх, з їх величезними параметрами.

Перший з наведених нижче алгоритмів є трохи складнішим, він вимагає по дві ключові пари (секретний-відкритий ключ) на кожного учасника кільця. Для другого алгоритму достатньо однієї ключової пари для кожного учасника.

Перед тим, як сформулювати ці алгоритми, введемо необхідні позначення та визначення, які стосуються операції спарювання та будуть використовуватись у цих алгоритмах. Також ми припускаємо, що у відповідній групі точок еліптичної кривої задача CDH є складною, а задача DDH – простою.

5.5 Кільцеві підписи, що використовують операцію спарювання на еліптичних кривих

Нехай E – деяка еліптична крива над полем F_{q^t}, де $20 \le t \le 50$ (за сучасних обчислювальних потужностей, саме така степінь розширення вважається оптимальною для побудови операції спарювання).

Нехай параметри поля та еліптичної кривої такі, що існують такі три групи

$$G_1 < E,\ G_2 < E,\ G_{TG} < F_{q^t}{}^*,$$

що $|G_1| = |G_2| = |G_{TG}| = p$, для деякого простого $p \mid q^t - 1$.

Далі для простоти вважатимемо, що $G_1 = G_2$.

Позначимо P базову точку кривої (генератор груп G_1 та G_2), $\operatorname{ord} P = p$.

Нехай розмір кільця дорівнює l. Позначимо ключові пари кожного учасника (k_i, U_i) та (y_i, V_i), $i = \overline{1,l}$, де $k_i \in F_p$ та $y_i \in F_p$ – секретні ключі, U_i та V_i – відповідні відкриті ключі.

Нехай $e: G_1 \times G_2 \to G_{TG}$ – невироджене білінійне відображення спарювання.

Алгоритми, наведені нижче, були запропоновані у [96].

5.5.1 Алгоритм формування підпису - 1

1. Обчислити $m = H(M)$ (далі вважаємо, що $m \in F_p^*$, оскільки ми завжди можемо обрати відповідні параметри поля та геш-функції, для яких це виконується).

2. Вибираємо випадкове $r \in F_p^*$.

3. Обираємо випадкові $a_i \in F_p^*$, $i = \overline{1,l}$, $i \neq s$.

4. Обчислюємо $\sigma_i = a_i P$, $i = \overline{1,l}$, $i \neq s$.

5. Обчислити

$$\sigma_s = \frac{1}{m + k_s + r\, y_s}\left(P - \sum_{\substack{i=1 \\ i \neq s}}^{n} \{ m\sigma_i + a_i U_i + r a_i V_i \} \right). \tag{5.6}$$

6. Сформувати підпис $S = (r; \sigma_1, ..., \sigma_l)$.

5.5.2 Алгоритм перевіряння підпису - 1

1. Обчислити $m = H(M)$.

2. Перевірити виконання рівності

$$\prod_{i=1}^{n} e(mP + U_i + rV_i, \sigma_i) = e(P, P). \tag{5.7}$$

3. Якщо рівність виконується, підпис приймається, в іншому випадку підпис вважається недійсним.

Доведемо коректність цих алгоритмів, тобто те, що якщо підпис побудовано правильно, то рівність (5.7) завжди буде виконуватись.

Згідно до (5.6), ми можемо написати $\sigma_s = a_s P$, де a_s можна виразити через секретні ключі учасників кільця наступним чином:

$$a_s = \frac{1 - \sum\limits_{\substack{i=1 \\ i \neq s}}^{n} \{m + k_i + r\, y_i\}}{m + k_s + r\, y_s}. \tag{5.8}$$

Звичайно, оскільки підписант не знає секретних ключів, то він не може обчислити a_s безпосередньо, але він може обчислити відповідне σ_s.

Використовуючи рівність (5.8), ми можемо переписати ліву частину (5.7) наступним чином:

$$\prod_{i=1}^{n} e\left(mP + U_i + rV_i, \sigma_i\right) = \prod_{i=1}^{n} e\left(\left(m + k_i + ry_i\right)P, a_i P\right) = \prod_{i=1}^{n} \left\{ e\left(P, P\right)^{(m+k_i+ry_i)a_i} \right\} =$$

$$= e\left(P, P\right)^{\sum\limits_{i=1}^{n}(m+k_i+ry_i)a_i} = e\left(P, P\right)^{\sum\limits_{\substack{i=1 \\ i \neq s}}^{n}(m+k_i+ry_i)a_i + (m+k_s+ry_s)a_s} = e\left(P, P\right)^{\sum\limits_{\substack{i=1 \\ i \neq s}}^{n}(m+k_i+ry_i)a_i + (m+k_s+ry_s)\frac{1-\sum\limits_{\substack{i=1 \\ i \neq s}}^{n}(m+k_i+ry_i)a_i}{(m+k_s+ry_s)}} =$$

$$= e\left(P, P\right),$$

що й доводить коректність підпису.

Тепер наведемо алгоритм кільцевого підпису [97], який також використовує спарювання на еліптичних кривих, але при цьому не вимагає двох ключових пар для кожного учасника.

5.5.3 Алгоритм формування підпису - 2

1. Обчислити $h = H(M)$.

2. Обчислити $U = hP$, де під бітовим рядком h ми розуміємо відповідне натуральне число.

3. Випадково обрати $a_i,\ i = 1,...,n,\ i \neq s$.

4. Обчислити $\sigma_i = a_i P,\ i = \overline{1,n},\ i \neq s$.

5. Обчислити $\sigma_s = k_s^{-1}\left(U - \sum_{\substack{i=2 \\ i \neq s}}^{n} a_i K_i\right)$.

6. Сформувати кільцевий підпис як $S = (\sigma_1,...,\sigma_n)$.

5.5.4 Алгоритм перевіряння підпису - 2

1. Обчислити $h = H(M)$.

2. Обчислити $U = hP$, де під бітовим рядком h ми розуміємо відповідне натуральне число.

3. Перевірити виконання рівності $e(U,P) = \prod_{i=1}^{n} e(K_i, \sigma_i)$.

4. Якщо рівність виконується, підпис приймається, в іншому випадку підпис вважається недійсним.

Коректність цього алгоритму перевіряється безпосередніми обчисленнями. Його стійкість базується на припущенні про складність задачі q-SDH у відповідній групі точок еліптичної кривої.

5.6 Безпосередня анонімна атестація (БАА)

Припустимо, що деякий користувач бажає виконати певну дію або отримати певну послугу. При цьому перевіряючий, який з ним спілкується, бажає переконатись, що цей користувач має валідні документи, зокрема у тій сфері, що стосується саме цього перевірчого органу. Така постановка задачі нагадує задачу віддаленої авторизації, але в нашому випадку мова йде не тільки про віддалене спілкування. Ця проблема може бути також сформульована як необхідність доведення того, що атестаційні дані цього користувача були створені і підписані певним уповноваженим органом, і даний користувач дійсно є їх власником. Але при цьому користувач хоче максимально зберегти свою анонімність – як мінімум, не надавати державним органам інформації, що не стосується сфери їхньої компетенції. Для цього інформація стосовно цього користувача повинна бути структурована певним чином, щоб мати можливість відкривати якісь її частини повністю, якісь частково, а якісь не відкривати взагалі.

Частковий розв’язок цієї задачі вперше було запропоновано у [98]. Основним недоліком такого розв’язку було використання RSA-функції, що або призводить до дуже повільної роботи протоколу (внаслідок використання величезних простих чисел), або до зниження стійкості.

Більш зручні та стійкі протоколи були запропоновані у роботі [99], і там же вперше було використано термін direct anonymous attestation (DAA). Запропонований розв’язок використовував одразу і техніку групових підписів, і доведень без розголошень, і сліпих підписів, і ідентифікації, для доведення приналежності до певної групи. На сьогодні найбільш детальний огляд таких алгоритмів та протоколів наведено у [100]. Фактично, БАА схеми можна вважати модифікованими схемами групового підпису – без можливості викриття підписанта певно є довіреною стороною, менеджером групи. В залежності від варіанту використання, БАА може бути і протоколом, і алгоритмом.

Одним з найзручніших способів побудови БАА є спосіб, що використовує операцію спарювання у групі точок еліптичної кривої. Він є ефективним за швидкодією і забезпечує необхідний рівень стійкості навіть при достатньо невеликих параметрах.

5.7 Використання наведених криптографічних механізмів для побудови відповідних протоколів моніторингу з максимальним забезпеченням анонімності

Використовуючи наведені механізми, можна побудувати наступні протоколи, які дають можливість:

– надавати інформацію з підтвердженням відповідної обізнаності, але без розкриття особи, яка цю інформацію надає;

– підтверджувати валідність дій якоїсь особи, або підтверджувати дозволи, їй надані, без розкриття іншої інформації стосовно цієї особи.

У першому випадку застосовується алгоритм кільцевого підпису, у другому – механізми БАА.

Для того, щоб побудувати відповідні протокол з використанням описаних механізмів, необхідно виконання наступних умов.

1. Всі користувачі системи повинні мати пари "секретний ключ – відкритий ключ", відповідно до алгоритмів підпису, які застосовуються у системі. Як було показано у цьому розділі та у наведених роботах стосовно БАА, найбільш перспективними є алгоритми підпису, що базуються на операції спарювання у групі точок еліптичної кривої.

2. Система повинна використовувати криптографічну геш-функцію, яка є стандартизованою, та алгоритми вкладання цієї геш-функції у точку еліптичної кривої, що є одним з параметрів цієї системи.

3. Інформація стосовно користувача повинна бути розбита на так звані блоки інформації таким чином, що кожна установа, уповноважена перевіряти інформацію, має доступ до повної інформації в одних блоках; має частковий

доступ до інформації в інших блоках; взагалі не має доступу до інформації в певних блоках, але може перевірити, що вони містять валідну інформацію.

4. Для кожного набору блоків інформації (вважаємо, що такий набір відповідає компетенціям певної установи) виконані певні математичні перетворення, згідно з [98-100], необхідні для реалізації механізмів БАА.

Після формування цих параметрів та виконання відповідних підготовчих обчислень, отримуємо безпосередньо протоколи анонімного надання інформації в межах компетентності (на базі кільцевих підписів) та протоколи підтвердження валідності документів, або підтвердження дозволів, або прав на певну діяльність, з максимальною анонімністю (на базі БАА).

5.8 Висновки до п’ятого розділу

1. У цьому розділі було наведено основну ідею стосовно використання кільцевих підписів та БАА для побудови протоколів моніторингу та інформування населення, які дозволяють максимально зберігати анонімність користувачів. Зокрема, було наведено огляд робіт стосовно кільцевого підпису та БАА, розглянуто кілька варіантів побудови алгоритмів кільцевого підпису та запропоновано новий, що має суттєві переваги. Зазначимо, що стійкість кожного способу побудови таких підписів базується на певних криптографічних твердженнях або припущеннях – наприклад, припущення про існування однобічної функції, або припущення про стійкість криптографічної геш-функції, або припущення про різні модифікації задачі Діффі-Хелмана у групі точок еліптичної кривої. Для кожного способу побудови підпису будується своє рівняння, на перевірці виконання якого і базується алгоритм перевірки підпису. Крім того, на прикладах було детально розглянуто, як працюють ці алгоритми для кожного варіанту підпису.

2. Слід зазначити, що на даний час основною проблемою, пов'язаною зі складністю використання кільцевих підписів, є їх довжина. Так, в загальному випадку вона є пропорційною розміру кільця. Тому кільцеві підписи не є

ефективними для кільця великого розміру, що обмежує їх анонімність. Існують певні способи зменшення розміру кільцевого підпису, але вони можуть бути застосовані лише для окремих випадків. Тому актуальним на сьогодні є напрямок подальших досліджень, пов'язаний зі зменшенням довжини кільцевого підпису.

3. Ще одним напрямком досліджень можна вважати побудову таких кільцевих підписів, які мають певні додаткові властивості, наприклад порогових підписів, сліпих підписів, тощо.

4. У розділі також було показано, як наведені криптографічні механізми дозволяють підтверджувати валідність інформації стосовно певної особи, зберігаючи при цьому її анонімність та, за необхідності, не розкриваючи деталі цієї інформації.

6 ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ З ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ СИСТЕМ ЗБЕРІГАННЯ ТА ПОШИРЕННЯ ІНФОРМАЦІЇ У ДЕЦЕНТРАЛІЗОВАНИХ СЕРЕДОВИЩАХ

У цьому розділі будуть наведені механізми економічного стимулювання підключення до системи й протоколи активної взаємодії як звичайних громадян (що отримують інформацію у системі й розповсюджують її у визначених безпечних рамках), так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури. При цьому запропоновані протоколи взаємодії будуть забезпечувати максимальну децентралізацію системи, а механізми економічного стимулювання матимуть виключно добровільний характер з відсутністю будь-якої каральної складової. Кінцевою метою таких механізмів є охоплення системою переважної більшості суспільства із загальним позитивним сприянням.

Слід зазначити, що з появою блокчейну багато баз даних, для яких важливою складовою є хронологія надходження інформації, почали структурувати інформацію таким чином, щоб було можливо зберігати її у блокчейні. На сьогоднішній день у практично всі, хто має справу з базами даних, зрозуміли, що використання блокчейна у сфері криптовалют реалізує лише невеликий відсоток його можливостей, а найбільшу користь він може принести саме для зберігання інформації, що має певну структуру, надходить у певній послідовності та потребує певних криптографічних механізмів для підтвердження її валідності.

Для реалізації нашої мети по якомога ширшому залученню населення до поширення інформації, протоколам функціонування такого інформаційного блокчейну повинні бути притаманні наступні риси:

– децентралізація, тобто можливість підключатись до мережі та виконувати свої функції автономно і незалежно від інших, і при цьому не заважаючи іншим;

– можливість обирати свою роль у цій системі відповідно до наявного часу/бажання/ресурсів/зацікавленості, тощо;

– отримувати певну економічно вигідну нагороду за підтримку функціонування цієї системи, відповідно до обраної ролі (виду діяльності), причому винагорода повинна бути пропорційна затраченому часу та/або ресурсам;

– можливість працювати за зручним графіком та у зручному форматі, який кожен учасник обирає автономно;

– можливість обробляти інформацію, що розповсюджується, з використанням простих зрозумілих алгоритмів, або можливість повної автоматизації своєї участі;

– сприяння саме командній роботі, тобто існування, у певному сенсі, рівноваги Нешап у відповідній грі, що забезпечує стабільність функціонування мережі завдяки досягнення взаємовигідної поведінки всіх учасників.

Такий великий список вимог може бути реалізований далеко не кожним протоколом консенсусу. Так, для вибору моделі, на базі якої з'являється можливість реалізувати, хоча б частково, зазначені вимоги, довелося опрацювати величезну кількість найсучасніших джерел та виконати порівняльний аналіз запропонованих в них протоколів. За результатами аналізу було вирішено за основу взяти модель сайдчейнів з так званим Латус-консенсусом.

Сайдчейни (англ. sidechains) [101-104], а також подібні конструкції, такі як [105, 106], можна вважати актуальним та корисним інструментом для сучасних блокчейнів. Їх можна розглядати як доповнення до блокчейну, що дозволяє отримати деякі додаткові функції, які не реалізовані в основному блокчейні (англ. mainchain).

Загалом, сайдчейни можуть використовувати довільний протокол консенсусу з доведеною стійкістю з урахуванням умов, за яких ця стійкість була доведена [107-110]. В цьому розділі ми будемо розглядати лише сайдчейни на основі протоколу консенсусу Latus [111], який є гібридним PoS-протоколом, що базується на протоколі Ouroboros Praos [112], з додатковим прив'язкою до основного блокчейну на основі PoW. Прив'язка до основного блокчейну є необхідною вимогою для сайдчейну [101-104, 111], щоб гарантувати такі

властивості блокчейну, як життєздатність і стійкість [113]. Для забезпечення рівня безпеки транзакцій у сайдчейні деяка інформація повинна регулярно надсилатися від сайдчейну до основного блокчейну. Основний блокчейн може мати велику кількість сайдчейнів, тому потрібно зменшити обсяг інформації, що надсилається, але таким чином, щоб не збільшувати ризики для сайдчейну. У консенсусі Latus ця інформація містить серію рекурсивних доведень zk-SNARK [114, 115], які забезпечують децентралізований обмін даними між блокчейнами з можливістю верифікації, а також надають додаткового захисту інформації, що розповсюджується у блокчейні.

Абревіатура «zk-SNARK» розшифровується як «zero-knowledge Succinct Non-interactive Argument of Knowledge» (стислий неінтерактивний аргумент знань з нульовим знанням) [116]. Це дійсно геніальна техніка для доведення того, що хтось знає якусь інформацію, не розкриваючи нічого про цю інформацію, або для того, щоб довести, що певне твердження істинне, не розкриваючи його деталей. zk-SNARK можна розглядати як неінтерактивну систему доведення без розголошення, прообраз якої вперше було введено близько 40 років тому[28]. З того часу ця тематика дуже інтенсивно розвивалася. Вперше термін «zk-SNARK» був введений у роботі [117], яка суттєво спиралась на результати [118]. У [119] і [120] був представлений протокол Pinoccio, що робить zk-SNARK більш зручним та придатним для застосування для більш загальних потреб.

Як зазначалося, zk-SNARK є стислим аргументом, що означає, що довжина доведення досить мала. Наприклад, він може бути постійним[29], де його довжина залежить лише від заданого рівня безпеки і не залежить від розміру даних, які ми підтверджуємо. Саме тому zk-SNARK є дуже привабливим інструментом для використання в блокчейнах, де проблема зменшення розміру блоку є дуже актуальною. Доведення zk-SNARK використовуються, наприклад, у таких

[28] Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proofs. SIAM Journal on Computing 1989, 18, 186–208. https://doi.org/10.1137/0218012.

[29] Groth, J. On the Size of Pairing-Based Non-interactive Arguments. In Advances in Cryptology – EUROCRYPT 2016; Fischlin, M.; Coron, J.S., Eds.; Springer-Verlag, 2016; Vol. 9666, - Lecture Notes in Computer Science, pp. 305–326. https://doi.org/10.1007/978-3-662-49896-5_11.

блокчейнах, як zCash[30], MINA[31], Horizen [111]. Для більшої зручності їх використання навіть створюються спеціальні криптографічні примітиви, такі як блочні шифри та геш-функції, розраховані саме для застосування в zk-SNARK[32,33].

Кожен блокчейн обирає найбільш підходящу для нього версію zk-SNARK. Протокол Latus використовує Darlin[34], тобто вдосконалену композицію Marlin[35] і Halo[36].

У цьому розділі не йдеться про розвиток концепції zk-SNARK, і, власне, для наших досліджень не має значення, який zk-SNARK використовується в Latus. Як і роботи [101-104], ми концентруємось на забезпеченні стабільного та коректного функціонування сайдчейнів, які забезпечують зазначені на початку розділу властивості. Але, на відміну від згаданих робіт, ми досліджуємо ці питання в межах кожного окремого блоку, оскільки створення блоку в Latus є досить громіздкою процедурою. У Latus, децентралізована генерація доведень використовує спеціальну схему відправки, яка дозволяє всім зацікавленим сторонам, або обчислювачам, створювати доведення, обране випадково, а потім надсилати його до блокчейну, отримуючи певну винагороду (заохочення) за

---

[30] Hopwood, D.; Bowe, S.; Hornby, T.; Wilcox, N. Zcash Protocol Specification: Version 2021.2.16 [NU5 proposal], 2021. https://zips.z.cash/protocol/protocol.pdf.

[31] Mina. Started by O(1) Labs. The world's lightest blockchain, powered by participants, 2021. https://minaprotocol.com.

[32] Grassi, L.; Khovratovich, D.; Rechberger, C.; Roy, A.; Schofnegger, M. Poseidon: new Hash Functions for Zero Knowledge Proof Systems. Cryptology ePrint Archive, Report 2019/458, 2019. https://ia.cr/2019/458.

[33] Kovalchuk, L.; Oliynykov, R.; Rodinko, M. Security of the Poseidon Hash Function Against Non-Binary Differential and Linear Attacks. Cybern Syst Anal 2021, 57, 268–278. https://doi.org/10.1007/s10559-021-00352-y Translated from Kibernetyka ta Systemnyi Analiz, No. 2, March-April, 2021, pp. 115-127.

[34] Haböck, U.; Garoffolo, A.; Benedetto, D.D. Darlin: Recursive Proofs using Marlin. Cryptology ePrint Archive, Report 2021/930, 2021. https://ia.cr/2021/930.

[35] Chiesa, A.; Hu, Y.; Maller, M.; Mishra, P.; Vesely, N.;Ward, N. Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS. Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I; Canteaut, A.; Ishai, Y., Eds. Springer, 2020, Vol. 12105, - Lecture Notes in Computer Science, pp. 738–768. https://doi.org/10.1007/978-3-030-45721-1_26.

[36] Boneh, D.; Drake, J.; Fisch, B.; Gabizon, A. Halo Infinite: recursive zk-SNARKs from any additive polynomial commitment scheme. Cryptology ePrint Archive, Report 2020/1536, 2020. https://ia.cr/2020/1536.

кожне прийняте доведення. Якщо два або більше обчислювачів створили одне й те саме доведення, лідер блоку (суб'єкт, який створює блок) обирає одне з них. Іншими словами, протокол консенсусу Latus дозволяє всім зацікавленим сторонам одночасно брати участь у процесі генерації одного блоку. З одного боку, це посилює децентралізацію; з іншого, це вимагає створення складніших протоколів взаємодії між лідером блоку та обчислювачами, а також вибору параметрів цих протоколів та обґрунтування їх коректності та надійності. У цьому розділі розглядаються саме ці питання.

Основною особливістю протоколу консенсусу Latus є зменшення обсягу інформації, що надсилається до основного блокчейну з сайдчейну, за допомогою рекурсивної композиції доведень zk-SNARK, що дозволяє побудувати стислі доведення правильності переходів станів сайдчейну на період епохи переведення даних. Наприкінці епохи створюється zk-SNARK для сертифіката відкликання, щоб довести правильність переходів стану сайдчейну для всієї епохи, і він перевіряє зворотні переведення (backward transfers). Така процедура дозволяє основному блокчейну забезпечити ефективну перевірку діяльності сайдчейну, не використовуючи жодних посередників, таких як сертифікатори [104], і не заглиблюючись у деталі процесів, що відбуваються всередині сайдчейну.

У сайдчейні лідер блоку збирає транзакції, які він має намір включити до свого блоку, впорядковує їх, а потім формує відповідні пропозиції для обчислювачів. У наших застосуваннях ми теж будемо використовувати термін «транзакції», але під кожною транзакцією ми будемо розуміти додавання до блоку певної інформації, що має деяку задану структуру та підтверджується zk-SNARK-доведеннями. Кожен блок містить певний повністю впорядкований набір транзакцій (його розмір є степенем 2) та досконале бінарне дерево, вузли якого теж є zk-SNARK-доведеннями. Далі ми будемо називати це дерево «деревом доведень». Кожне доведення в нижній частині дерева доводить певне твердження про правильність переходу з деякого стану до додавання нової інформації до наступного стану, який є станом після додавання відповідної інформації, тобто після наступної транзакції. Такі твердження будемо називати

«базовими твердженнями», а доведення нижнього рівня, які є листками дерева доведень – «базовими доведеннями». Інші, внутрішні вузли дерева доведень є так званими доведеннями «поєднання» [104], і вони доводять правильність двох послідовних доведень у дочірніх вузлах. Отже, доведення у кореневому вузлі доводить правильність переходів між послідовними станами, що відповідають усьому блоку.

Усі zk-SNARK-доведення для дерева доведень децентралізовано будуються учасниками, які виявили бажання брати учать у функціонуванні цієї мережі. Ми їх будемо називати обчислювачами. Кожен обчислювач, який створює zk-SNARK-доведення, встановлює ціни на свої доведення в межах певного інтервалу або множини, що визначається в кінці попередньої епохи. Якщо для деякого вузла дерева доведень існує більше одного доведення, лідер блоку обирає найдешевше з них. За цих умов взаємна діяльність лідера блоку та обчислювача повинна забезпечувати ефективне та стабільне функціонування сайдчейну.

У цьому розділі уточнюються та розширюються результати, представлені у роботі[37]: описується та пояснюється функціонування сайдчейну, і насамперед поведінка лідера блоку та обчислювача, за допомогою теорії ймовірностей та комбінаторного апарату; використовуються ланцюги Маркова для моделювання процесу розподіленого генерування доведень у блокчейнах на основі zk-SNARK. Основні цілі наших досліджень наступні:

– оцінити кількість кроків (або знайти математичне сподівання та дисперсію їх значення), необхідних для побудови повного набору zk-SNARK-доведень для базових тверджень, що відповідають транзакціям, які лідер блоку має включити до блоку, який він створює;

– використовуючи ці результати, рекомендувати максимальну кількість транзакцій, які лідер блоку повинен включити в блок, щоб гарантувати, що

[37] Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Models of distributed proof generation for zk-SNARKbased blockchains. In Theoretical and Applied Cryptography; Belarusian State University: Minsk, Belarus, 2020; pp. 112–120. http://conf.bsu.by/data/theoreticalandappliedcrypto/doc/TAC_2020_Proceedings.pdf.

відповідне дерево доведень з високою ймовірністю буде створено протягом одного часового інтервалу.

Ми розглядаємо дві різні моделі, які відповідають двом типам конструкції доведення. Перша модель описує простіший випадок, коли всі доведення будуються незалежно (як один рівень дерева доведень). Друга модель досліджує більш складну проблему, коли доведення розташовані у вузлах з різних рівнів дерева доведень. Такий набір доведень має природний частковий порядок, оскільки доведення з верхнього рівня дерева можна побудувати лише тоді, коли побудовані доведення з попередніх рівнів.

На початку розділу ми даємо деякі попередні відомості з комбінаторики, теорії ймовірностей та теорії ланцюгів Маркова, необхідні для подальших досліджень. Концепція факторизації (англ. lumping) для ланцюгів Маркова є окремим випадком загальної ідеї факторізації для математичних структур, яка є природною та корисною для контролю гранулярності. Нажаль, лише деякі підручники приділяють увагу цьому поняттю. Ми вважаємо, що проблема може бути описана кількома ланцюгами Маркова з різними рівнями факторізації, залежно від того, скільки деталей ми хочемо знати на даний момент. Ми проілюструємо цю ідею на прикладі так званої задачі колекціонера купонів, широко відомої у теорії імовірності.

Потім ми проаналізуємо кількість окремих кроків, необхідних для побудови повного набору доведень, які є листками недоведеної частини дерева доведень. У цьому випадку вони можуть генеруватися незалежно і одночасно. Ми наведемо ряд прикладів різних стохастичних моделей, які будемо використовувати у наших дослідженнях. Зокрема, буде доведено, що дві моделі, описані в Прикладі 5 і Прикладі 6, стохастично еквівалентні, хоча перша спочатку була сформульована як немарківська, а друга була сформульована в термінах ланцюга Маркова. Ми будемо досліджувати факторизовану (або грудковану, англ. lumped) форму цієї моделі в Прикладі 7. Використовуючи методику факторизації ланцюгів Маркова, ми отримали рекурентні формули для математичного сподівання та дисперсії кількості кроків в залежності від

кількості доведень n та кількості листків m, а потім асимптотично звели математичне сподівання до функції h з одним параметром n/m та описали його поведінку.

Нарешті, ми вивчаємо процес створення доведень для всього досконалого бінарного дерева і показуємо, що ця конструкція зручна для узагальнення раніше вивчених моделей для випадку частково впорядкованої множини. У результаті цього узагальнення з'явилось кілька корисних висновків, наприклад, було створено більш зручний розподіл ймовірностей на елементах множини. Ми завершуємо цей розділ представленням числових результатів щодо кількості транзакцій, які лідер блоку повинен включити в поточний блок. Ця кількість залежить від параметрів мережі, таких як довжина часового інтервалу, кількість активних обчислювачів, час, необхідний для генерації доведень тощо. Ми наведемо таблиці з рекомендованою кількістю транзакцій для різних заздалегідь заданих ймовірностей успішного створення блоку.

6.1 Основні позначення, поняття та визначення

Тут ми наводимо необхідні факти щодо факторизації (грудкування) для ланцюгів Маркова та описуємо ланцюг Маркова, що відповідає задачі збирача купонів, як результат двох послідовних конструкцій факторизації. Ця техніка та приклади є необхідними для отримання подальших стосовно основних моделей.

Позначення 1. Потужність скінченної множини S ми будемо позначати двома способами (залежно від зручності):

$$\#S = |S|.$$

Позначення 2. Для невід'ємного цілого числа m, відповідною жирною літерою $\mathbf{m}$ ми позначаємо (залежно від контексту) повністю впорядковану множину $\{1 < 2 < \cdots < m\}$ або множину $\{1, 2, \ldots, m\}$.

Позначення 3. *Дужка Айверсона* для твердження P переводить булеве значення у відповідне число:

$$[\![P]\!] := \begin{cases} 1, & \text{if } P \text{ is true,} \\ 0, & \text{if } P \text{ is false.} \end{cases} \tag{6.1}$$

Позначення 4. Ми використовуємо загальноприйняті позначення для:

– спадаючих факторіалів:

$$n^{\underline{r}} = (n)_r = n(n-1)\cdots(n-r+1);$$

– біноміальних та мультиноміальних коефіцієнтів:

$$\binom{m}{k} := \frac{m!}{k!(m-k)!}; \qquad \binom{m}{m_1,\ldots,m_n} := \frac{m!}{m_1!\cdots m_n!}, \quad \text{де} \quad m_1+\cdots+m_n = m.$$

6.1.1 Числа Стірлінга другого роду

Так званий «дванадцятикратний спосіб» у комбінаториці[38,1.9] підраховує кількість відображень (ін'єкцій, сюр'єкцій або всіх можливих) між двома скінченними множинами, розрізняючи або не розрізняючи елементи в кожній з них. Наприклад, симетричні групи S_m та S_n діють на множині $Sur(\mathbf{m},\mathbf{n})$ сюр'єкцій $\mathbf{m} \twoheadrightarrow \mathbf{n}$ за допомогою пре- та посткомпозиції, відповідно. *Число розбиттів Стірлінга* (*числа Стірлінга другого роду*) можуть бути визначені як число орбіт:

$$S(m,n) = \left\{ \frac{m}{n} \right\} := | S_n \setminus Sur(\mathbf{m},\mathbf{n}) |,$$

тобто як кількість розбиттів m позначених елементів на n непорожніх немаркованих підмножин, або як кількість способів вкладення m матрьошок так, що можна бачити n (матрьошки лінійно впорядковані за розміром).

Дія S_n на $Sur(\mathbf{m},\mathbf{n})$ є вільною, тому

$$| Sur(\mathbf{m},\mathbf{n}) | = n! \left\{ \frac{m}{n} \right\}.$$

[38] Stanley, R.P. Enumerative combinatorics, 2nd ed.; Vol. 1, - Cambridge studies in advanced mathematics, 49, Cambridge University Press, 2011. http://www-math.mit.edu/~rstan/ec/ec1.pdf.

З іншого боку, за умови сюр'єкції $\pi:\mathbf{m}\twoheadrightarrow\mathbf{n}$, елементи орбіти $\pi\circ S_m$ ототожнюються з суміжними класами з $S_m / St_\pi = S_m / (S_{m_1}\times\cdots\times S_{m_n})$, де $m_i = \#\pi^{-1}(i)$. Усі сюр'єкції можна обчислити за допомогою суми за n-композиціями m:

$$n!\left\{\frac{m}{n}\right\} = |\operatorname{Sur}(\mathbf{m},\mathbf{n})| = \sum_{\substack{m_1+\cdots+m_n=m\\ m_1,\ldots,m_n\geqslant 1}}\left|\frac{S_m}{S_{m_1}\times\cdots\times S_{m_n}}\right| = \sum_{\substack{m_1+\cdots+m_n=m\\ m_1,\ldots,m_n\geqslant 1}}\binom{m}{m_1,\ldots,m_n}. \quad (6.2)$$

Помноживши обидві частини (6.2) на $z^m / m!$ та обчисливши суму за m, можна отримати експоненціальну генеруючу функцію $n!mn$:

$$\sum_{m=0}^{\infty} n!\left\{\frac{m}{n}\right\}\frac{z^m}{m!} = (e^z - 1)^n. \quad (6.3)$$

Кожне відображення $f:\mathbf{m}\to\mathbf{n}$ розкладається як $f = (\mathbf{m}\twoheadrightarrow \operatorname{Im} f \rightarrowtail \mathbf{n})$. Тоді загальна кількість функцій $\mathbf{m}\to\mathbf{n}$

$$n^m = \sum_{S\subseteq\mathbf{n}} |S|!\left\{\frac{m}{|S|}\right\} = \sum_{r=0}^{n}\left\{\frac{m}{r}\right\}(n)_r. \quad (6.4)$$

Можна розглядати (6.4) як тотожність між цілими поліномами з вільною змінною n. Таким чином, ми отримуємо альтернативне визначення чисел Стірлінга як коефіцієнтів матриці переходів між двома поліноміальними базисами.

Інверсія Мебіуса у випадку булеана $\mathcal{P}\mathbf{m}$ допускає простіше формулювання як принцип включення-виключення[11,2.1]. Це дозволяє, на відміну від (6.4), виразити кількість сюр'єкцій через кількість усіх функцій:

$$n!\left\{\frac{m}{n}\right\} = \sum_{S\subseteq\mathbf{n}}(-1)^{n-|S|}|S|^m = \sum_{r=0}^{n}(-1)^r\binom{n}{r}(n-r)^m. \quad (6.5)$$

Обернений оператор різниці діє на числових послідовностях (x_k) як $\Delta: x_k \mapsto x_{k+1} - x_k$. Його степені можна виразити за допомогою біноміальної формули $\Delta^n x_k = \sum_{r=0}^{n}(-1)^r\binom{n}{r}x_{k+n-r}$. Таким, чином, вираз (6.5) може бути переписаний як

$$n!\left\{\frac{m}{n}\right\} = \Delta^n 0^m = \Delta^n k^m |_{k=0} .$$

Додаткова інформація щодо чисел Стірлінга другого роду може бути знайдена тут[39].

6.1.2 Факторизація ланцюгів Маркова

Ми припускаємо, що ланцюги Маркова є дискретними, стаціонарними та мають скінченний або злічений простір станів *S*. Елементи матриці переходів *p* записуємо у формі

$$p_{ij} = p(i, j) = \mathbf{P}r(X(n+1) = j \mid X(n) = i), \qquad i, j \in S.$$

Таке положення індексів відповідає правильній дії *p* на вектор-матрицю станів. Це правильна стохастична матриця з $\sum_{j\in S} p_{ij} = 1$.

Тут ми розглядаємо концепцію факторизованих ланцюгів Маркова; див., наприклад.[40,§6.3]. Загальна математична ідея переходу структури від множини до фактор-множини також працює й у випадку ланцюгів Маркова. Враховуючи сюр'єкцію $\pi : S \twoheadrightarrow T$, розглянемо відповідну логічну матрицю v_π та її інверсію за Муром-Пенроузом $v_\pi^\dagger$ (див.[41]).

$$v_\pi := (\delta_{\pi(s),t})_{s\in S, t\in T}, \qquad v_\pi^\dagger := (v_\pi^t v_\pi)^{-1} v_\pi^t.$$

У нашому окремому випадку логічна матриця, що відповідає сюр'єкції, є проекцією, і, отже, інверсія за Муром-Пенроузом $v_\pi^\dagger$ є дійсною односторонньою інверсією: $v_\pi^\dagger v_\pi = 1$.

Лема 1. Нехай $p = (p_{ss'})_{s,s'\in S}$ є стохастичною матрицею над простором станів S. Для сюр'єкції $\pi : S \twoheadrightarrow T$, наступні умови є еквівалентними:

---

[39] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. https://oeis.org.
[40] Kemeny, J.G.; Snell, J.L. Finite Markov Chains; - Undergraduate Texts in Mathematics, Springer-Verlag, 1976. https://www.math.pku.edu.cn/teachers/yaoy/Fall2011/Kemeny-Snell1976.pdf.
[41] Ben-Israel, A.; Greville, T.N. Generalized Inverses: Theory and Applications, 2nd ed.; - CMS Books in Mathematics, Springer-Verlag, 2003. https://www.doi.org/10.1007/b97366.

– для будь-якого $t' \in T$ сума $\sum_{s' \in \pi^{-1}(t')} p_{ss'}$ локально постійна на $s \in \pi^{-1}(t)$ для кожного $t \in T$;

– $v_\pi v_\pi^\dagger p v_\pi = p v_\pi$.

Визначення 1. Нехай $p = (p_{ss'})_{s,s' \in S}$ є стохастичною матрицею над простором станів S. Сюр'єкція $\pi : S \twoheadrightarrow T$, що задовольняє умовам попередньої леми, називається *факторизуючим відображенням* (а відповідне розбиття $S = \coprod_{t \in T} \pi^{-1}(t)$ називається факторизуючим розбиттям).

Твердження 1. Нехай $p = (p_{ss'})_{s,s' \in S}$ є стохастичною матрицею та $\pi : S \twoheadrightarrow T$ є факторизованим відображенням.

Тоді можна визначити нову стохастичну матрицю p^π над простором станів T з елементами

$$p^\pi_{tt'} := \sum_{s' \in \pi^{-1}(t')} p_{ss'}, \qquad s \in \pi^{-1}(t). \tag{6.6}$$

Факторизована k-кратна матриця переходу може бути записана як

$$(p^\pi)^k = (v_\pi^\dagger p v_\pi)^k = v_\pi^\dagger p^k v_\pi. \tag{6.7}$$

Будемо вважати, що наступне твердження є своєрідним «фольклорним» результатом.

Твердження 2. Припустимо, що скінченна група G діє на множині станів S за правилом $S \times G \ni (s,g) \mapsto s^g \in S$, а стохастична матриця $p = (p(s,s'))_{s,s' \in S}$ є G-інваріантною, тобто

$$p(s_1^g, s_2^g) = p(s_1, s_2), \qquad s_1, s_2 \in S, \quad g \in G.$$

Тоді канонічна проєкція $\pi : S \twoheadrightarrow S/G$ на множину орбіт є факторизуючим відображенням.

Доведення. Позначимо як $St := \{g \in G \mid s^g = s\}$ стабілізатор підгрупи стану s. Для орбіти $s^G := \{s^g \mid g \in G\}$, сума з Леми 1 набуває вигляду

$$\sum_{s'' \in \pi^{-1}(s^G)} p(s_1, s'') = \frac{1}{|St_s|} \sum_{g \in G} p(s_1, s^g).$$

Тоді стандартний аргумент показує, що остання сума є G-інваріантною як функція за s_1:

$$\sum_{g\in G} p_(s_1^h, s^g) = \sum_{g\in G} p_(s_1, s^{gh^{-1}}) = \sum_{g'\in G} p(s_1, s^{g'}).$$

□

6.1.3 Модель колекціонера купонів з використанням добутків та факторизації

Класичну проблему колекціонера купонів можна описати наступним чином.

Приклад 1. Нехай в урні є n різних купонів. Колекціонер вибирає з поверненням один випадковий купон за крок. Нам потрібно обчислити імовірнісні розподіли наступних випадкових величин:

– кількість різних купонів, вибраних після m кроків;

– кількість кроків, необхідних для отримання точно r різних купонів.

Схрещені добутки ланцюгів Маркова (та їх узагальнення) описані у роботі[42]. Ми отримуємо версію моделі колекціонера купонів як схрещений добуток простого детермінованого процесу. Інші дві версії є результатами його подальших факторизацій. Це підводить до класичного розподілу заповнюваності, описаного за допомогою чисел розбиття Стірлінга. Цей контекст тісно пов’язаний з нашими подальшими моделями.

Приклад 2. (Гіпероктант – повна інформація). Розглянемо повністю детермінований ланцюг Маркова, який приймає значення $X_0 = 0, X_1 = 1, X_2 = 2, \ldots$. Його матриця переходу є напівнескінченною коміркою Жордана:

[42] D’Angeli, D.; Donno, A. Crested products of Markov chains. Annals of Applied Probability 2009, 19, 414–453. arXiv:0903.0513.

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Таким чином, n-ий схрещений добуток вищенаведеного ланцюга Маркова має множину станів $\mathbb{Z}_{\geqslant 0}^n$ та матрицю переходу

$$p = \frac{1}{n}\sum_{i=1}^{n} \underbrace{1_{\mathbb{Z}_{\geqslant 0}} \otimes \cdots \otimes 1_{\mathbb{Z}_{\geqslant 0}}}_{i-1} \otimes J \otimes \underbrace{1_{\mathbb{Z}_{\geqslant 0}} \otimes \cdots \otimes 1_{\mathbb{Z}_{\geqslant 0}}}_{n-i},$$

де $1_{\mathbb{Z}_{\geqslant 0}}$ тотожня матриця на $\mathbb{Z}_{\geqslant 0}$.

Розглянемо асиметричне випадкове блукання по n-вимірному гіпероктанту $\mathbb{Z}_{\geqslant 0}^n$ з ненульовими ймовірностями переходу

$$p(a, a+e_i) = 1/n, \qquad a \in \mathbb{Z}_{\geqslant 0}^n, \qquad e_i = (\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i}).$$

Тоді ненульові елементи m-кратної матриці переходів мають вигляд

$$p^m(a, a+h) = n^{-m}\binom{m}{h_1,\ldots,h_n}, \quad \text{де} \quad h_i \geqslant 0 \quad \text{та} \quad h_1 + \cdots + h_n = m.$$

Отже, кожен рядок цієї матриці представляє мультиноміальний розподіл на векторах h.

Наступний крок – коли колекціонер хоче запам’ятати про кожен фіксований купон, чи був він розіграний, але незалежно від того, скільки разів.

Позначення 5. Для $a \in \mathbb{Z}_{\geqslant 0}^N$ або $a \in \{0.1\}^N$, носій a визначається наступним чином:

$$\operatorname{supp} a := \{i \in N \mid a_i \neq 0\}.$$

Приклад 3. (Гіперкуб – часткова інформація). Дужка Айверсона (6.1), застосована до кожної координати $(a_i)_{i\in\mathbf{n}} \mapsto ([\![a_i > 0]\!])_{i\in\mathbf{n}}$, визначає факторизуюче відображення $\mathbb{Z}_{\geqslant 0}^n \to \{0,1\}^n$ для попереднього ланцюга Маркова. Відповідно до рівняння (6.7), для отриманого ланцюга Маркова на гіперкубі $\{0,1\}^n$, m-кратна

матриця переходу p^m є наступною: якщо $p^m(a,b) > 0$, тоді $a_i \leqslant b_i$ для всіх i; і за принципом включення-виключення:

$$p^m(a,b) = n^{-m} \sum_{\substack{m_1+\cdots+m_n=m \\ m_1,\ldots,m_n \geqslant 0 \\ m_i > 0 \Rightarrow i \in \operatorname{supp} b \\ i \notin \operatorname{supp} a \Rightarrow m_i > 0}} \binom{m}{m_1,\ldots,m_n} = n^{-m} \sum_{r=|\operatorname{supp} a|}^{|\operatorname{supp} b|} (-1)^{\operatorname{supp}|b|-r} \binom{|\operatorname{supp}(b-a)|}{r-|\operatorname{supp} a|} r^m.$$

Зокрема,

$$p^m(a,a) = (|\operatorname{supp} a|/n)^m, \qquad p^m(0,b) = n^{-m}|\operatorname{supp} b|!m|\operatorname{supp} b|.$$

Якщо колекціонер може зберегти в пам’яті лише одне число, ми продовжуємо факторизацію.

Приклад 4. Проекція гіперкуба на головну діагональ

$$\{0,1\}^n \to \{0,1,\ldots,n\}, \qquad (a_i)_{1 \leqslant i \leqslant n} \mapsto \sum_i a_i$$

є грудкуючим відображенням. Поєднуючи стани, ми отримуємо так званий ланцюжок збору купонів[43,2.2], де ненульові ймовірності переходу за m кроків є такими:

$$p^m(k,k+r) = n^{-m} \binom{n-k}{r} \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} (k+s)^m.$$

Кількість $\xi_m = \xi_0 p^m$ різних купонів, зібраних після m кроків, має класичний розподіл заповнюваності[44]:

$$\mathbf{P}r(\xi_m = r) = p^m(0,r) = \frac{(n)_r}{n^m} mr. \tag{6.8}$$

[43] Levin, D.A.; Peres, Y.; Wilmer, E.L. Markov chains and mixing times, 2nd ed.; AMS, 2017. http://www.ams.org/books/mbk/107/mbk107-endmatter.pdf.

[44] O’Neill, B. The Classical Occupancy Distribution: Computation and Approximation. The American Statistician 2021, 75, 364–375. https://doi.org/10.1080/00031305.2019.1699445.

Математичне сподівання числа ζ_r^n кроків для отримання рівно r різних купонів описується за допомогою гармонійних чисел $H_n = 1 + 1/2 + \cdots + 1/n$:

$$\mathbf{E}\zeta_r^n = n(H_n - H_{n-r}). \tag{6.9}$$

6.2 Розподілена генерація наборів доведень

У цьому підрозділі представлені основні результати щодо розподіленої генерації наборів окремих незалежних доведень. Це спрощена модель, де всі доведення можуть бути згенеровані одночасно і незалежно. Ця модель відповідає, зокрема, випадку генерації доведень, що знаходяться на одному рівні дерева доведень.

6.2.1 Модель розподіленої генерації наборів доведень

Наступні два приклади показують два можливі підходи до опису цієї моделі, які потім виявляться еквівалентними.

Приклад 5. (Стани є підмножинами). Нехай *обчислювачі* є спеціальними вузлами в одноранговій мережі. Їм потрібно побудувати zk-SNARK-доведення для скінченного набору N так званих кандидатів на перевірку.

На кожному кроці в стані N' кожен перевіряючий самостійно вибирає одного кандидата з N' і будує його доказ, тобто вибір надається функцією g: $\mathbf{m} \to N'$, рівномірно розподіленою між усіма функціями $m \to N'$. Для даного вибору наступний стан отримується шляхом видалення всіх кандидатів, доведених на цьому кроці. Отже, ненульові ймовірності переходу описуються кількістю сюр'єкцій

Ми описуємо цей процес як ланцюг Маркова, стани якого є підмножинами $N' \subseteq N$ кандидатів, доведення яких ще не побудовані. Кількість обчислювачів $m > 0$ є фіксованою. На кожному кроці в стані N', кожен обчислювач незалежно та з однаковою ймовірністю вибирає одного кандидата з N' і будує його доведення, тобто вибір надається функцією $g : \mathbf{m} \to N'$ рівномірно розподіленою між всіма функціями $\mathbf{m} \to N'$. Результуючим станом є різниця $N'' := N' \setminus Img$, отримана шляхом видалення всіх доведених елементів. Ненульові ймовірності

переходу $p(N',N'')$ дорівнює частці всіх функцій $\mathbf{m}\to N'$ отриманих від сюр'єкції до $N'\setminus N''$, тобто $g=\left(\mathbf{m}\twoheadrightarrow N'\setminus N''\rightarrowtail N'\right)$.

$$p(N',N'')=\frac{|Sur(\mathbf{m},N'\setminus N'')|}{|N'|^m}=\frac{|N'\setminus N''|!}{|N'|^m}m|N'\setminus N''|,\qquad N''\subseteq N'. \quad (6.10)$$

Альтернативним способом є визначення міри ймовірності на траєкторіях:

Позначення 6. *Лінійне впорядкування* набору N – це бієкція $\sigma:N\xrightarrow{\cong}\{1,2,\ldots,|N|\}$. Позначимо як $OrdN$ набір лінійних впорядкувань N.

Приклад 6. (Немарківська модель). Припустимо, що на початку кожен обчислювач самостійно вибирає для $1\leqslant i\leqslant m$ власний так званий пріорітет. Це визначає ланцюг станів, тобто, підмножини разом з лінійними впорядкуваннями:

$$N=N_0\supset N_1\supset\cdots\supset N_{k-1}\supset N_k=\varnothing,$$
$$\sigma_i^{(j)}\in Ord(N_j),\qquad \sigma_i^{(0)}=\sigma_i,\qquad 1\leqslant i\leqslant m,\qquad 0\leqslant j\leqslant k.$$

На j-ому кроці, $1\leqslant j\leqslant k$, перебуваючи у стані N_{j-1}, i-ий обчислювач обирає кандидата у доведення відповідно до функції $g_j:\mathbf{m}\to N_{j-1}$, заданої як $g_j(i):=\left(\sigma_i^{(j-1)}\right)^{-1}(1)$. Наступний стан – це $N_j=N_{j-1}\setminus Im(g_j)$. Існує природна проєкція $\rho_{N'}^{N}:Ord(N)\to Ord(N')$, яка видаляє елементи $N\setminus N'$ із впорядкування. Тоді ми задамо

$$\sigma_i^{(j)}=\rho_{N_j}^{N}(\sigma_i). \quad (6.11)$$

Твердження 3. Моделі з Прикладів 5 та 6 є стохастично еквівалентними.

Доведення. Наведемо ескіз доведення. Більш загальна ситуація описана в Прикладі 12. Вибірки $(\sigma_i)_{1\leqslant i\leqslant m}$ рівномірно розподілені на $(OrdN)^m$. Це означає

– рівномірний розподіл g_j на множині функцій $\mathbf{m}\to N_{j-1}$, та

– рівномірний розподіл $\sigma_i^{(j)}\in Ord(N_j)$.

Другий пункт випливає з Визначення 11 і з того факту, що шар $\rho_{N'}^{N}$ над кожною точкою має однакову потужність $|OrdN|/|OrdN'|=|N|!/|N'|!$.

Приклад 7. (Стани – це числа). Функція потужності $N'\mapsto|N'|$ є грудкуючим відображенням для ланцюга Маркова з Прикладу 5. Станами

факторизованого ланцюга Маркова є $\{0,1,\ldots,|N|\}$, а єдиними ненульовими елементами матриці переходів є наступні:

$$\begin{aligned} p(0,0) &= 1, \\ p(n,n-r) &= \frac{1}{n^m}\binom{n}{r} r!mr = \frac{(n)_r}{n^m} mr, \quad n > 0, 1 \leqslant r \leqslant m. \end{aligned} \tag{6.12}$$

Зауважте, що кожен рядок цієї матриці збігається з класичним розподілом заповнюваності з Прикладу 4.

Отже, почнемо зі стану $\xi_0^{mn} \equiv n$. Еволюція визначається степенями матриці переходів:

$$\xi_k^{mn} = \xi_0^{mn} p^k.$$

Поглинаючий стан – це 0. Усі траєкторії строго зменшуються, і $\xi_k^{mn} \equiv 0$ для $k \geqslant n$.

Час поглинання τ^{mn} – це випадкова величина, що вимірює точну кількість кроків, необхідну m обчислювачам для генерації всіх n доведень, тобто, $\tau^{mn} = k+1$ тоді і тільки тоді, коли $\xi_{k+1}^{mn} = 0$ та $\xi_k^{mn} \neq 0$.

Беручи до уваги нижню трикутну форму нашої матриці переходів, ми отримуємо рекурентні та явні формули для ймовірностей:

$$\begin{aligned} \mathbf{P}r(\tau^{mn} = 0) &= \delta_{n0}, \\ \mathbf{P}r(\tau^{mn} = k+1) &= \sum_{r=1}^{\min(m,n)} p_{nn-r} \mathbf{P}r(\tau^{mn-r} = k) = \sum_{r=0}^{\min(m,n)} \frac{(n)_r}{n^m} mr \mathbf{P}r(\tau^{mn-r} = k) \end{aligned} \tag{6.13}$$

$$\begin{aligned} \mathbf{P}r(\tau^{mn} = k) &= \sum_{0<n_k<\cdots<n_2<n_1=n} p_{n_1 n_2} \cdots p_{n_{k-1} n_k} p_{n_k 0} \\ &= \sum_{0<n_k<\cdots<n_2<n_1=n} \frac{n!}{(n_1 n_2 \cdots n_k)^m} mn_1 - n_2 \cdots mn_{k-1} - n_k mn_k \\ &= \sum_{r_1+\cdots+r_k=n r_1,\ldots,r_k>0} \frac{n!}{(r_1(r_1+r_2)\cdots n)^m} mr_1 \cdots mr_k \\ &= \sum_{s_1+\cdots,s_{2k}=n s_1,s_3,\ldots,s_{2k-1}\geqslant 0 s_2,s_4,\ldots,s_{2k}>0} \binom{n}{s_1,\ldots,s_{2k}} \times \\ &\times \frac{(-1)^{s_1+s_3+\cdots+s_{2k-1}} (s_2 s_4 \cdots s_{2k})^m}{((s_1+s_2)(s_1+s_2+s_3+s_4)\cdots n)^m}. \end{aligned} \tag{6.14}$$

Помноживши рівняння (6.13) на k^{ℓ} і взявши суму по k, отримуємо рекурентну формулу для ℓ-го моменту:

$$\mathbf{E}(\tau^{mn}-1)^{\ell} = \sum_{r=1}^{\min(n,m)} p_{mn-r}\mathbf{E}(\tau^{mn-r})^{\ell}.$$

Зокрема, це дозволяє розрахувати математичне сподівання та дисперсію.

Твердження 5. Нехай $m>0$. Тоді $\tau^{m0}\equiv 0$, та для $n>0$

$$\begin{aligned}
\mathbf{E}\tau^{mn} &= 1+\sum_{r=1}^{\min(n,m)}\frac{(n)_r}{n^m}mr\mathbf{E}\tau^{mn-r},\\
\mathbf{E}(\tau^{mn})^2 &= -1+2\mathbf{E}\tau^{mn}+\sum_{r=1}^{\min(n,m)}\frac{(n)_r}{n^m}mr\mathbf{E}(\tau^{mn-r})^2, \qquad (6.15)\\
\mathbf{V}ar\tau^{mn} &= \mathbf{E}(\tau^{mn})^2-(\mathbf{E}\tau^{mn})^2.
\end{aligned}$$

В Таблиці 6.1, наприкінці розділу, наведено розподіли ймовірностей τ^{mn} з точністю до 10^{-6} (за виключенням останнього стовпця). Комірка містить список пар $k; p_k^{mn}$ – значення k та відповідної ймовірності p_k^{mn} (ненульову до встановленого значення точності). Кількість доведень n проходить через степені 2, що відповідає кількості листків досконалого бінарного дерева.

Ми порівнюємо значення $\mathbf{E}\tau^{mn}$ як результати аналітичного розрахунку відповідно до (6.15) за допомогою Wolfram Mathematica та проведення 10^5 випадкових тестів, написаних на мові C++, для моделі з Прикладу 6. Для $m,n\in\{10,20,30,40,50,100,200,300\}$ числові результати, отримані цими двома різними методами, збігаються до 2 цифр після коми.

Зауваження 1. Для фіксованого позитивного цілого m, ми розглядаємо дві модифікації моделі колекціонера купонів з Прикладу 4:

– Після m, $2m$, $3m,\ldots$ кроків, усі купони, витягнуті за останні m кроків, видаляються з урни назавжди.

– Кожен раз, коли колекціонер витягує m нових різних купонів, ці m купонів видаляються з урни назавжди.

Зауважимо, що якщо для першої модифікації застосувати масштабування за часом, тобто розглянути підпроцес у моменти $0,m,2m,\ldots$, ми отримаємо модель генерації доведень з Прикладу 7 . Друга модифікація дещо повільніша за

першу, тобто математичне сподівання кількості кроків для отримання точно r різних купонів у другій модифікації не менше, ніж у першій модифікації. Ці спостереження показують, що математичне сподівання часу τ^{mn} генерації доведення з Прикладу 7 може бути мажоровано математичним сподіванням часу ζ_r^n з моделі колекціонера купонів з Прикладу 4:

$$\begin{aligned}\mathbf{E}\tau^{mbm} \quad & -\mathbf{E}\tau^{mm} \leqslant (\mathbf{E}\zeta_m^{bm} + \mathbf{E}\zeta_m^{(b-1)m} + \cdots + \mathbf{E}\zeta_m^{2m}) / m \\ & = b(H_{bm} - H_{(b-1)m}) + (b-1)(H_{(b-1)m} - H_{(b-2)m}) + \cdots + 2(H_{2m} - H_m) \\ & = bH_{bm} - (H_{(b-1)m} + H_{(b-2)m} + \cdots + H_{2m} + 2H_m) \\ & \approx \ln\frac{b^b}{(b-1)!} \underset{b \gg 1}{\approx} b + \frac{1}{2}\ln\frac{b}{2\pi}.\end{aligned} \tag{6.16}$$

6.2.2 Асимптотика τ^{mn}

Для загальних формул (6.14), для ймовірностей $\mathbf{P}r(\tau^{mn} = k)$, дуже важко отримати апроксимацію в явному вигляді. Однак, $\mathbf{P}r(\tau^{mn} = 1)$ – це лише частина сюр'єктивних відображень $\mathbf{m} \to \mathbf{n}$ серед усіх таких відображень:

$$\mathbf{P}r(\tau^{mn} = 1) = \frac{n!S(m,n)}{n^m}.$$

6.2.2.1 Велика кількість обчислювачів

Спочатку розглянемо випадок великої кількості обчислювачів, тобто, $m \gg n$. Еквівалентно, це означає $\mathbf{P}r(\tau^{mn} = 1) \approx 1$ або $\mathbf{E}\tau^{mn} \approx 1$. Відмітимо, що $\tau^{mn} = 1$ тоді і тільки тоді, якщо на першому кроці відповідне відображення $\mathbf{m} \to \mathbf{n}$ обчислювачів на доведення-кандидати є сюр'єктивним.

Твердження 5. Для фіксованого числа $n > 0$ доведень-кандидатів, виконується наступна асимптотика:

$$\mathbf{P}r(\tau^{mn} = 1) \underset{m \to \infty}{\sim} 1 - n\left(\frac{n-1}{n}\right)^m + o\left(\left(\frac{n-1}{n}\right)^m\right). \tag{6.17}$$

$$\mathbf{E}\tau^{mn} \underset{m\to\infty}{\sim} 1+n\left(\frac{n-1}{n}\right)^m + o\left(\left(\frac{n-1}{n}\right)^m\right). \qquad (6.18)$$

Доведення. Для кожного доведення-кандидата i, нехай A_i є такою подією, що i не доведено на першому кроці, $\mathbf{P}rA_i = \left(\frac{n-1}{n}\right)^m$, з доповненням $\overline{A_i}$. З принципу включення-виключення:

$$\mathbf{P}r(\tau^{mn}=1) = \mathbf{P}r\bigcup_i \overline{A_i} = 1-\sum_i \mathbf{P}rA_i + \sum_{i<j}\mathbf{P}rA_i \cap A_j - \cdots,$$

де слідуючи суми є малими у порівнянні з першими. Для розрахунку математичного сподівання $\mathbf{E}\tau^{mn}$, ми можемо брати до уваги лише значення $\tau = 1,2$; внесок інших значень асимптотично малий.

□

Зауваження 2. У дописі в блозі[45], було помічено, що верхня границя

$$\mathbf{P}r(\tau^{mn}=1) \leqslant \left(1-(1-1/n)^m\right)^n \qquad (6.19)$$

може бути отримана з нерівності між звичайною та умовною ймовірностями.

$$\mathbf{P}r\bigcap_i \overline{A_i} = \prod_i \mathbf{P}r\left(\overline{A_i} \mid \bigcap_{j<i}\overline{A_j}\right) \leqslant \prod_i \mathbf{P}r\,\overline{A_i}$$

Зауважимо, що права частина (6.17) має ту саму асимптотику, що й $\mathbf{P}r(\tau^{mn}=1)$ у (6.19), тому її можна розглядати як асимптотичну верхню оцінку для $\mathbf{P}r(\tau^{mn}=1)$.

6.2.2.2 Асимптотика чисел Стірлінга та ймовірностей $\mathbf{P}r(\tau^{mn}=1)$

Асимптотика чисел Стірлінга другого роду вивчалася починаючи з Лапласа (1814). З довгого списку публікацій ми розглядаємо лише результати, пов’язані з нашим контекстом.

Звичайним способом є застосування формули інтегрування Коші до генеруючої функції (6.3):

[45] Jiang, Z. An Upper Bound on Stirling Number of the Second Kind, 2015. https://blog.zilin.one/2015/02/25/an-upper-boundon-stirling-number-of-the-second-kind/.

$$n!S(m,n) = m![z^m](e^z - 1)^n = \frac{m!}{2\pi i}\oint_C (e^z - 1)^n z^{-(m+1)} dz = \frac{m!}{2\pi i}\oint_C e^{\phi(z)} \frac{dz}{z},$$

де C – відповідний контур навколо початку координат, та $\phi(z) = n\ln(e^z - 1) - m\ln(z)$. Сідлова точка ρ є коренем рівняння $\phi'(\rho) = 0$ або $\frac{\rho}{1 - e^{-\rho}} = \frac{m}{n}$, або, нарешті,

$$\rho = \frac{m}{n} + W_0\left(-\frac{m}{n}e^{-m/n}\right).$$

Функція Ламберта W є багатозначною функцією, оберноною до $w \mapsto we^w$, та W_0 – це його головна гілка; див.[46].

Наступний вираз збігається з першим членом[47,(5.1)] або з отриманим у контексті локальної граничної теореми[48,(5.9)], або з[49,(2.9)]:

$$S(m,n) \sim \frac{m!(e^\rho - 1)^{n+1}}{n!\rho^{m+1}e^\rho \sigma\sqrt{2\pi m}},$$

де $\sigma^2 = \left(\frac{n}{m}\right)^2\left(1 - \frac{\rho}{e^\rho - 1}\right)$ – дисперсія граничного нормального розподілу. Це наближення є рівномірним для n/m у кожному замкнутому підінтервалі $(0,1)$.

Використовуючи формулу Стірлінга для $m!$, ми можемо отримати асимптотику ймовірності як функцію двох параметрів n/m та m:

$$\mathbf{P}r(\tau^{mn} = 1) = \frac{n!S(m,n)}{n^m} \sim \alpha\gamma^m, \tag{6.20}$$

де α та γ залежать лише від співвідношення n/m:

$$\alpha = \frac{1}{\left(1 - \frac{\rho}{e^\rho - 1}\right)^{1/2}}, \qquad \gamma = \frac{e^{\rho - 1}}{(e^\rho - 1)^{1 - n/m}}.$$

---

[46] Corless, R.; Gonnet, G.; Hare, D.; Jeffrey, D.; Knuth, D. On the Lambert W function. Advances in Computational Mathematics 1996, 5, 329–359. http://www.apmaths.uwo.ca/~djeffrey/Offprints/W-adv-cm.pdf.

[47] Moser, L.; Wyman, M. Stirling numbers of the second kind. Duke Math. J. 1958, 25, 29–48. https://doi.org/10.1215/S0012-7094-58-02504-3.

[48] Bender, E.A. Central and local limit theorems applied to asymptotic enumeration. J. Combin. Theory Ser. A 1973, 15, 91–111. https://doi.org/10.1016/0097-3165(73)90038-1.

[49] Temme, N.M. Asymptotic estimates of Stirling numbers. Studies in Applied Mathematics 1993, 89, 233–243. https://doi.org/10.1002/sapm1993893233.

Ці залежності показані на Рисунках 6.1-6.2. Можна побачити, що при n/m, що знаходиться в діапазоні від 0 до 1, функції $\alpha(n/m)$ та $\gamma(n/m)$ змінюються відповідно від 1 до ∞ та від 1 до $1/e$.

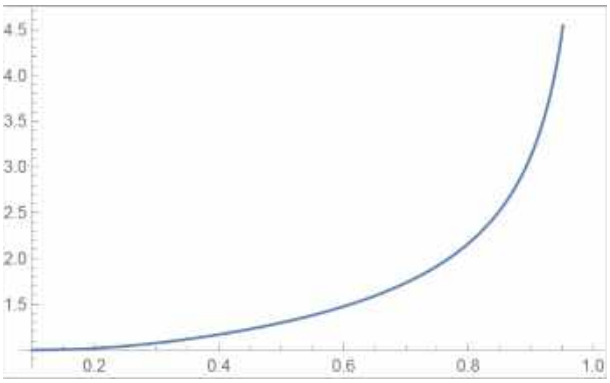


Рисунок 6.1 – $\alpha(n/m)$

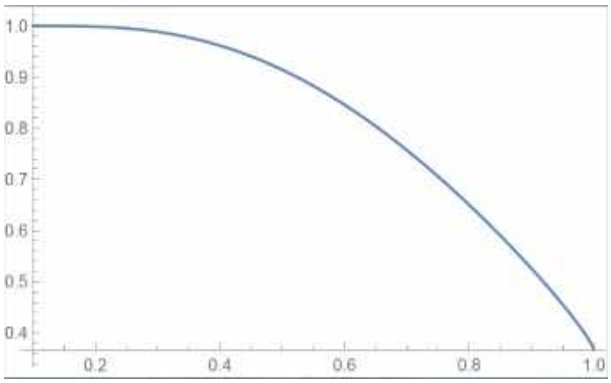


Рисунок 6.2 – $\gamma(n/m)$

6.2.2.3 Залежність від співвідношення n/m

Далі ми вивчимо асимптотичну поведінку τ^{mn} залежно від m та n, і сформулюємо пов'язані результати як гіпотези. На даний момент ми можемо довести лише деякі переходи, а інші можна отримати за допомогою обчислень нескінченної точності. Зауважимо, що $\mathbf{E}\tau^{mn}$ для великих m та n асимптотично залежать тільки від співвідношення n/m, і ми вивчаємо характер цієї залежності.

Серія обчислень з нескінченною точністю дозволяє сформулювати наступну послідовність гіпотез.

Гіпотеза 1. Для кожного фіксованого $m,n \in \mathbb{Z}_{>0}$, послідовність $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\tau^{kmkn}$ є зростаючою та обмеженою зверху.

Зауваження 3. Нагадаємо, що Зауваження 1 зазначає зв'язок між моделями колекціонера купонів і моделями генерації доведень. Беручи до уваги вираз (16) і той факт, що для ζ_r^n з Прикладу 4 послідовність $k \mapsto \zeta_{kr}^{kn}$ зростаюча і обмежена зверху, можна довести наступне. Якщо послідовність $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\tau^{kk}$ зростаюча

і обмежена зверху, тоді для кожного фіксованого $m,n \in \mathbb{Z}_{>0}$ з $n > m$ послідовність $\mathbb{Z}_{>0} \ni k \mapsto \mathbf{E}\tau^{kmkn}$ є зростаючою і обмеженою зверху.

Отже, за припущеннями Гіпотези 1 існує функція $h : \mathbb{Q}_{\geqslant 0} \to \mathbb{R}_{\geqslant 1}$, визначена границею

$$h(n/m) = \lim_{k\to\infty} \mathbf{E}\tau^{kmkn}, \qquad \text{зокрема,} \quad h(0) = 1.$$

Функція $h(x)$ є неспадною тому, що $\mathbf{E}\tau^{mn}$ строго зростає по n та строго спадає по m.

У випадку $m = 750$ обчислювачів, точки $(\frac{n}{750}, \mathbf{E}\tau^{750n})$ графіка Рисунку 6.3 апроксимують відповідні точки зображення графіка функції $h(x)$. Для малого x, це виглядає як сходовий проліт зі сходами висотою 1, що починаються в точці $(0,1)$.

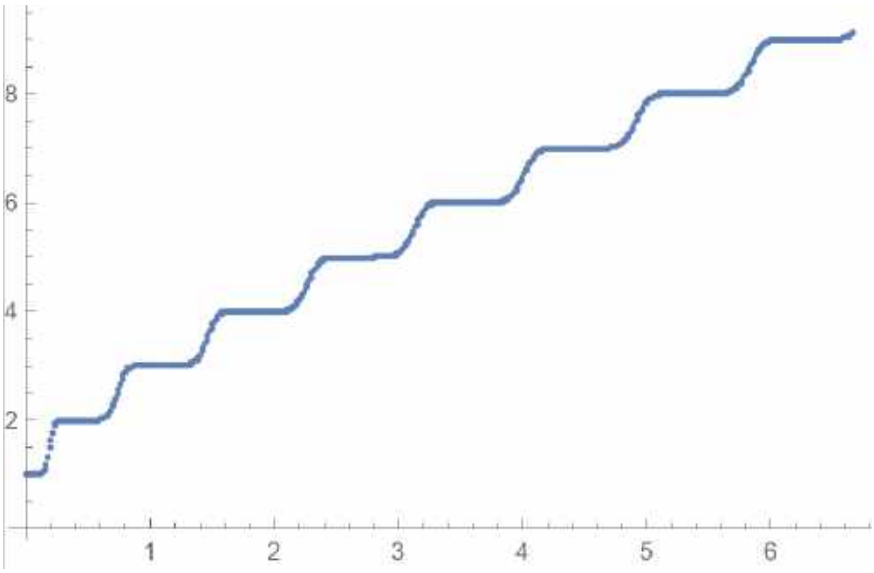


Рисунок 6.3 – Графік функції $\frac{n}{750} \mapsto \mathbf{E}\tau^{750n}$ як апроксимація для $h(x)$

Асимптотика (6.20) для $\mathbf{P}r(\tau^{mn} = k)$, $k = 1$ означає, що $h(x)$ не може бути (правою) безперервною при 0: $\lim_{q \downarrow 0} h(q) > h(0)$.Наші подальші розрахунки для асимптотики $k \geqslant 2$ вказують на наявність точки розриву для кожного k. Можна було б сподіватися, що функція $h(x)$ є ліво-неперервною.

Гіпотеза 2. Існує ліво-неперервна неспадна функція $h:\mathbb{R}_{\geqslant 0}\to\mathbb{R}_{\geqslant 1}$ визначена границею

$$h(x):=\lim_{\substack{m\to\infty\\ n/m\nearrow x}}\mathbf{E}\tau^{mn}=\sup_{m/n\leqslant x}\lim_{k\to\infty}\mathbf{E}\tau^{kmkn}. \tag{6.21}$$

Гіпотеза 3. Існує зростаюча послідовність дійсних чисел $0=\zeta_1<\zeta_2<\cdots$ з $\zeta_k<k$ таких, що наступні два еквівалентні твердження є істинними:

– $h(x)$ є сумою дужок Айверсона

$$h(x)=1+\sum_{k=1}^{\infty}[\![x>\zeta_k]\!]=\begin{cases}1, & if x=0,\\ k, & if\ \zeta_{k-1}<x\leqslant\zeta_k\ for k\geqslant 2.\end{cases} \tag{6.22}$$

– $$\lim_{\substack{m\to\infty\\ n/m\nearrow x}}\mathbf{P}r(\tau^{mn}=k)=1 \quad \text{iff} \quad (k=1\wedge x=0)\vee(k\geqslant 2\wedge x\in(\zeta_{k-1},\zeta_k]) \tag{6.23}$$

Гіпотеза 4. Функція $h(x)$ допускає асимптотику для $x\to+\infty$:

$$h(x)=x+\frac{1}{2}\ln(x)+o(\ln(x)), \tag{6.24}$$

або, еквівалентно:

$$\zeta_k=k-\frac{1}{2}\ln(k)+o(\ln(k)).$$

Більше того,

$$\zeta_1=0,\qquad \zeta_2=1/3,\qquad \zeta_3=1. \tag{6.25}$$

Зауваження 4. Для випадку $m=50$ обчислювачів, точки $(\frac{n}{50},\mathbf{E}\tau^{50n}-\frac{n}{50}-\frac{1}{2}\ln(\frac{n}{50}))$ графіка на Рисунку 6.4 апроксимують відповідні точки зображення графіка функції $h(x)-x-\frac{1}{2}\ln(x)$.

Апроксимація (6.24) для $h(x)$ узгоджується з оцінкою (6.16).

Для доведення (6.25), необхідно розрахувати:

$$\mathbf{P}r(\tau^{3nn}\neq 2)|_{n=2000}\approx 3.5\cdot 10^{-21},\qquad \mathbf{E}\tau^{900300}\approx 1.99999994;$$
$$\mathbf{P}r(\tau^{nn}\neq 3)|_{n=900}\approx 3.7\cdot 10^{-10},\qquad \mathbf{E}\tau^{500500}\approx 2.999994.$$

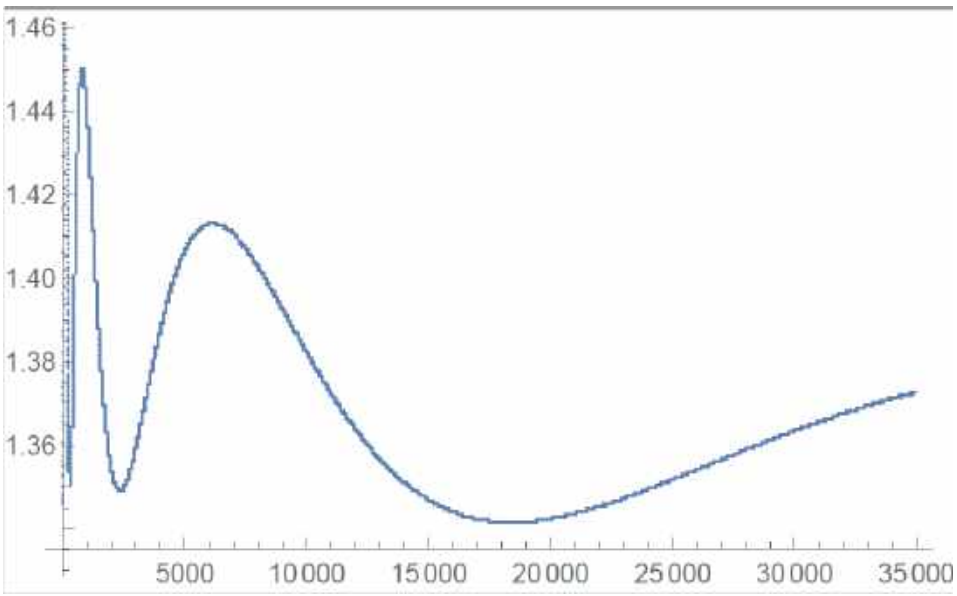


Рисунок 6.4 – Графік функції $\frac{n}{50} \mapsto \mathbf{E}\tau^{50n} - \frac{n}{50} - \frac{1}{2}\ln(\frac{n}{50})$ як апроксимація для $h(x) - x - \frac{1}{2}\ln(x)$

Ми хотіли б отримати асимптотику для всіх ймовірностей $\mathbf{P}r(\tau^{mn} = k)$, подібно до випадку $k = 1$. Зауважимо, що $\mathbf{P}r(\tau^{mn} = k) \neq 0$, коли $n / m \in (0, k]$, та, згідно з Гіпотезою 3, границею цієї ймовірності є 1 або 0. Наші розрахунки показують, що в обох випадках можна очікувати асимптотику у вигляді, подібному до (6.20).

Гіпотеза 5. Для $n, m \to \infty$ та $n / m \nearrow x$,

$$\mathbf{P}r(\tau^{mn} = k) \asymp \gamma_k(x)^m, \qquad x \in h^{-1}(k),$$
$$1 - \mathbf{P}r(\tau^{mn} = k) \asymp \lambda_k(x)^m, \qquad x \in (0, k] \setminus h^{-1}(k),$$

для деякого $\gamma_k, \lambda_k \in (0,1)$.

Результати розрахунків представлені у вигляді графіків $\gamma_k(x), \lambda_k(x)$ На Рисунках 6.5-6.6 для $k = 2$ та Рисунках 6.7-6.9 для $k = 3$.

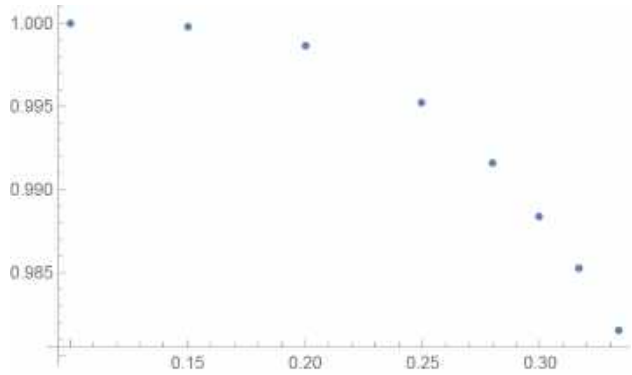


Рисунок 6.5 – $\lambda_2(n/m)$

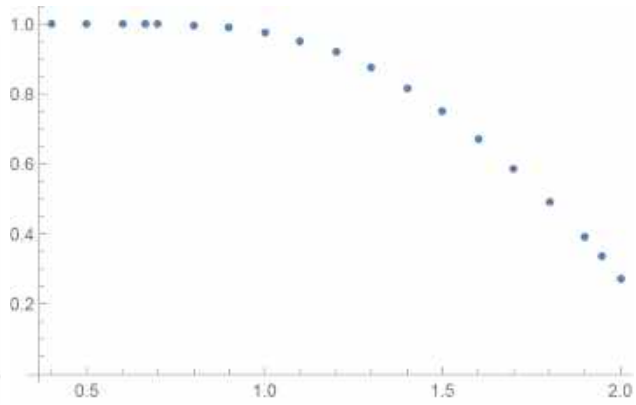


Рисунок 6.6 – $\gamma_2(n/m)$

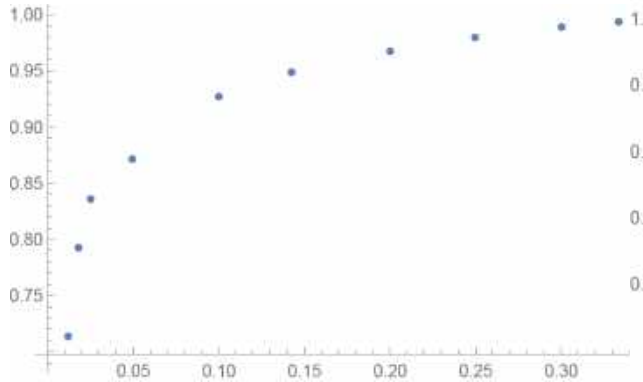


Рисунок 6.7 – $\gamma_3(n/m)$

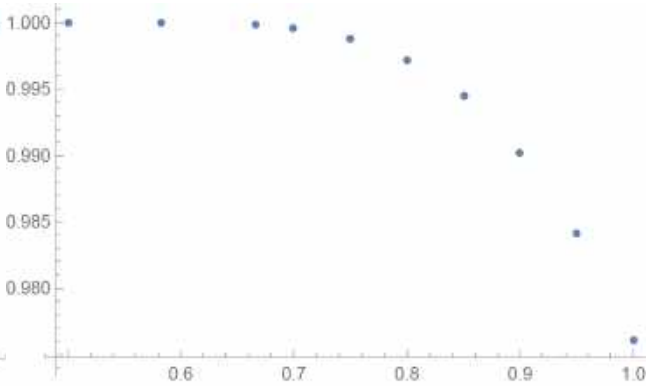


Рисунок 6.8 – $\lambda_3(n/m)$

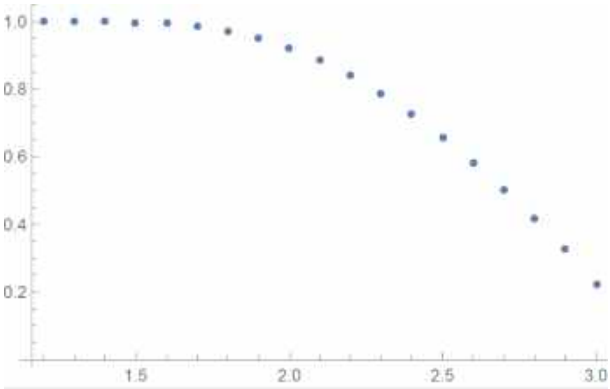


Рисунок 6.9 – $\gamma_3(n/m)$

Гіпотеза 6. Для $k \geqslant 2$,

$$\lambda_k(x) = \gamma_{k-1}(x) > \gamma_{k'}(x), \quad \text{для} \quad k' \neq \{k-1, k\}, \quad x \in (\zeta_{k-1}, \zeta_k). \qquad (6.26)$$

Зауваження 5. Нерівності (6.26) означають, що для достатньо великого m та $n/m \to x \in (\zeta_{k-1}, \zeta_k)$ розподіл τ^{mn} прагне до розподілу Бернуллі зі значеннями $k-1, k$. Можна побачити це у Таблиці 6.1, де для великих значень обчислювачів

m та доведень-кандидатів n списки значень і ймовірностей містять не більше двох елементів (тобто для інших значень ймовірності дуже малі).

Крім того, дисперсія τ^{mn} прагне до дисперсії розподілу Бернуллі:

$$\mathbf{V}ar\tau^{mn} \to \mathbf{P}r(\tau^{mn} = k-1)\cdot \mathbf{P}r(\tau^{mn} = k) \leqslant 1/4.$$

Дійсно, наші чисельні розрахунки дозволяють припустити, що $\mathbf{V}ar\tau^{mn} < 1$, якщо $m \geqslant 10$, $n/m < 10^4$.

6.3 Розподілена генерація дерев доведень

У цьому підрозділі розглядається складніша і водночас корисніша для реальних додатків модель генерації доведень. Згідно з консенсусом Latus, zk-SNARK-доведення утворюють досконалі бінарні дерева (дерева доведень) подібно до того, як геш-значення транзакцій формують подібні дерева в основному блокчейні. Вузли дерева утворюють частково впорядковану множину, діаграмою Хассе якої є саме дерево. Тому, цілком природно сформулювати частину наших результатів у термінах загальних множин.

6.3.1 Впорядковані множини та решітки

Основні факти про частково впорядковані множини, згадані нижче, можна знайти в основному в[50,51(ch.3)].

Частково впорядкована множина (англ. poset) – це множина, оснащена частковим порядком, тобто бінарним відношенням, яке є транзитивним, рефлексивним і антисиметричним.

Нехай P – множина. *Ланцюг* в P є підмножиною з повним індукованим порядком. *Антиланцюг* в P є підмножиною, де будь-які два різні елементи

---

[50] Roman, S. Lattices and Ordered Sets; Springer-Verlag, 2008. https://www.doi.org/10.1007/978-0-387-78901-9.

[51] Stanley, R.P. Enumerative combinatorics, 2nd ed.; Vol. 1, - Cambridge studies in advanced mathematics, 49, Cambridge University Press, 2011. http://www-math.mit.edu/~rstan/ec/ec1.pdf.

непорівнянні. *Висота* $ht(P)$ скінченної множини P – це максимальна потужність ланцюга в P. *Ширина* $wd(P)$ скінченної множини P – максимальна потужність антиланцюга в P.

Підмножина $I \subseteq P$ у множині P називається *нижньою множиною* (або *верхньою множиною*), якщо для кожного $x \in I$ і $y \in P$ з $y \leq x$ (або, відповідно) ми маємо $y \in I$. Зауважимо, що down-sets в P є up-sets у протилежній множині P^{op} і навпаки.

Позначимо як $\mathcal{O}_d(P)$ (та $\mathcal{O}_u(P)$) решітку нижньої множини (або верхньої множини, відповідно). Підмножина $I \subseteq P$ є нижньою множиною тоді і тільки тоді, коли його доповнення $P \setminus I$ є up-set. Набір верхніх множин в P утворює розподільну решітку, упорядковану за включенням. Мапа $\mathcal{O}_d(P) \to \mathcal{O}_u(P)$, $I \mapsto P \setminus I$ є антиізоморфізмом решіток.

Позначимо як $MinI$ (або $MaxI$) множину мінімальних (або максимальних, відповідно) елементів в $I \subseteq P$. Зауважимо, що $MinI$ і $MaxI$ є антиланцюгами. Для довільної підмножини $X \subseteq P$, позначимо як $X^{\downarrow}$ (або $X^{\uparrow}$) *нижнє замикання* (*down closure*) (або *верхнє замикання* (*up closure*), відповідно), тобто найменшу нижню множину (або верхню множину), що містить X. У випадку одиничного значення, нижня множина $\{x\}^{\downarrow}$ називається *принципом*.

$$I = (MinI)^{\uparrow} \text{ for } I \in \mathcal{O}_u(P), \qquad J = (MaxJ)^{\downarrow} \text{ for } J \in \mathcal{O}_d(P). \tag{6.27}$$

Таким чином, верхні множини (відповідно нижні множини) перебувають у взаємно однозначній відповідності з антиланцюгами.

Зауважимо, що наведена вище відповідність $P \mapsto \mathcal{O}_u(P), \mathcal{O}_d(P)$ є частиною теореми представлення Біркгофа, яка у сучасному формулюванні стверджує антиеквівалентність категорій скінченних множин і скінченних розподільних решіток.

Прямий наслідок теореми Біркгофа стверджує, що група симетрії $AutP$ скінченної множини P природним чином ізоморфна групі симетрії $Aut\mathcal{O}(P)$ відповідної решітки $\mathcal{O}(P) = \mathcal{O}_d(P)$ або $\mathcal{O}_u(P)$.

Наслідок 1. *Канонічне відображення* $\alpha : AutP \to Aut\mathcal{O}(P)$, $Q^{\alpha(g)} = \{p^g \mid p \in Q\}$, $g \in AutP$, $Q \in \mathcal{O}(P)$ є ізоморфізмом групи.

Для двох множин P і Q, існують нові множини:

– добуток $P \times Q$, де $(p,q) \leqslant (p',q')$ тоді і тільки тоді, якщо $p \leqslant p'$ в множині P і $q \leqslant q'$ в множині Q. Добуток розподільних решіток — розподільна решітка;

– кодобуток $P \sqcup Q$, який є непересічним об'єднанням, порядки, обмежені на P та Q, збігаються з початковими порядками, елементи з різних множин непорівнянні;

– лінійна сума $P + Q$ це непересічне об'єднання, де порядки, обмежені на P і Q збігаються з початковими порядками і $p < q$ для кожного $p \in P$, $q \in Q$. Лінійна сума розподільних решіток є розподільною решіткою.

Для двох множин P і Q існують такі природні ізоморфізми решіток:

$$\mathcal{O}_d(P \sqcup Q) \simeq \mathcal{O}_d(P) \times \mathcal{O}_d(Q), \qquad \mathcal{O}_u(P \sqcup Q) \simeq \mathcal{O}_u(P) \times \mathcal{O}_u(Q), \tag{6.28}$$

$$\mathcal{O}_d(P+Q) \simeq \frac{\mathcal{O}_d(P) + \mathcal{O}_d(Q)}{\mathrm{T}_{\mathcal{O}_d(P)} \sim \perp_{\mathcal{O}_d(Q)}}, \qquad \mathcal{O}_u(P+Q) \simeq \frac{\mathcal{O}_u(Q) + \mathcal{O}_u(P)}{\mathrm{T}_{\mathcal{O}_u(Q)} \sim \perp_{\mathcal{O}_u(P)}}, \tag{6.29}$$

де верхній елемент однієї підрешітки склеєний з нижнім елементом іншої.

Визначення 2. Нехай P – скінченна частково впорядкована множина. *Сумісне повне впорядкування* P є монотонною біекцією до скінченного порядкового $\sigma : P \xrightarrow{\cong} \{1 < 2 < \cdots < |P|\}$. Позначимо як $Ord(P)$ множину усіх сумісних загальних впорядкувань P.

Для скінченних множин P і Q існують природні бієкції

$$\begin{aligned} Ord(P+Q) &\simeq Ord(P) \times Ord(Q), \\ Ord(P \sqcup Q) &\simeq Ord(P) \times Ord(Q) \times Ord(\mathbf{p} \sqcup \mathbf{q}), \qquad p = |P|, q = |Q|. \end{aligned} \tag{6.30}$$

Сумісні загальні впорядкування $Ord(\mathbf{p} \sqcup \mathbf{q})$, $p, q \in \mathbb{Z}_{\geqslant 0}$ для кодобутку двох ланцюгів знаходяться у взаємно однозначній відповідності до перестановок у випадковому порядку $\sigma \in S_{p,q} \subseteq S_{p+q}$, тобто такий, що $\sigma(i) < \sigma(j)$ для $i < j \leqslant p$ або $p < i < j$. Кількість таких перестановок задається біноміальним коефіцієнтом $\dfrac{(p+q)!}{p!q!}$.

Визначення 3. Для множини P і підмножини $Q \subseteq P$ з індукованим порядком існує природне відображення з обмеженням $Ord(P) \to Ord(Q)$, $\sigma \mapsto \sigma|_Q$, де пара монотонної бієкції $\sigma|_Q$ і монотонна ін'єкція ι однозначно визначається з наступної комутативної діаграми

$$\begin{tikzcd} Q \arrow[r, "\sigma|_Q", "\cong"'] \arrow[d, hook] & \{1 < 2 < \cdots < |Q|\} \arrow[d, hook, "\iota"] \\ P \arrow[r, "\sigma", "\cong"'] & \{1 < 2 < \cdots < |P|\} \end{tikzcd} \tag{6.31}$$

Твердження 6. Нехай P – скінченна частково впорядкована множина. Тоді $Ord(Q)$ для $Q \subset P$ з природними відображеннями з обмеженням утворюють передпучок на підмножинах P впорядкованих за включенням.

Доведення. Можна безпосередньо перевірити, що для ланцюжка підмножин $Q'' \subseteq Q' \subseteq Q \subseteq P$ і $\sigma \in Ord(Q)$ ми маємо $\sigma|_{Q'}|_{Q''} = \sigma|_{Q''}$. □

Зауважимо, що дуже схожі конструкції навколо подвійності Біркгофа описують форми клітин вищих категорій в роботі[52].

6.3.2 Модель колекціонера купонів з частково впорядкованими множинами

У кандидатській дисертації[53] було розглянуто процес колекціонування купонів на частково впорядкованих множинах. Тут ми описуємо узагальнення ланцюгів Маркова з Прикладів 2–4 до випадку частково впорядкованої множини N.

Позначення 7. Для $a \in \mathbb{Z}^N_0$ або $a \in \{0.1\}^N$, множина елементів, доступних з a визначається наступним чином:

$$acc(a) := supp(a) \cup Min(N \setminus supp(a)).$$

[52] Bespalov, Y. Categories: Between Cubes and Globes. Sketch I. Ukrainian Journal of Physics 2019, 64, 1125–1128. https: //doi.org/10.15407/ujpe64.12.1125.
[53] Sidenko, S. Kac's Random Walk and Coupon Collector's Process on Posets. PhD thesis, MIT, Cambridge, 2008. https: //dspace.mit.edu/handle/1721.1/43781.

Приклад 8. (Гіпероктант із забороненими розмірами). Розглянемо асиметричне випадкове блукання по $|N|-$ розмірному цілочисельному гіпероктанту $\mathbb{Z}^N_0$ з ненульовими ймовірностями переходу

$$p(a,a+e_i)=\frac{1}{|acc(a)|},\qquad a\in\mathbb{Z}^N_{\geqslant 0},\qquad e_i=(\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{|N|-i})\quad \text{для}\quad i\in acc(a).$$

Приклад 9. (Гіперкуб із забороненими розмірами). Дужка Айверсона, що застосовується до кожної координати $(a_i)_{i\in\mathbf{n}}\mapsto([\![a_i>0]\!])_{i\in\mathbf{n}}$, дає грудкуюче відображення $\mathbb{Z}^n_{\cdot 0}\to\{0,1\}^n$ для попереднього ланцюга Маркова. Для отриманого ланцюга Маркова на гіперкубі $\{0,1\}^N$ відмінні від нуля ймовірності переходів є такими:

$$\begin{aligned} p(a,a+e_i) &= 1/|acc(a)|, \qquad a,a+e_i\in\{0,1\}^N,\quad i\in Min(N\setminus supp(a))\\ p(a,a) &= \frac{|supp(a)|}{|acc(a)|}=\frac{\sum_i a_i}{|acc(a)|}. \end{aligned}$$

Зверніть увагу, що вершина $a\in\{0,1\}^N$ доступна з 0 тоді і тільки тоді, якщо $supp(a)$ є нижньою множиною. Таким чином, ми можемо звести графік ланцюга Маркова (без циклів) до відповідного підграфа гіперкуба, який збігається з діаграмою Хассе решітки нижніх множин.

Приклад 10. (Факторизація за симетріями). Розглянемо групу симетрії $Aut\mathcal{O}_d(N)\simeq Aut\,N$ нижньої множини $\mathcal{O}_d(N)$. За Пропозицією 2, канонічна проєкція $\pi:\mathcal{O}_d(N)\to\mathcal{O}_d(N)/Aut\mathcal{O}_d(N)$ на орбітальну множину є грудкуючим відображенням.

Особливі випадки:

– Якщо N є дискретною частково впорядкованою множиною (де будь-які два різні елементи є незрівнянними), то елементи $\mathcal{O}_d(N)$ є довільними підмножинами N. Група симетрії $Aut\mathcal{O}_d(N)$ ізоморфна повній групі перестановок N, і діє транзитивно на підмножини фіксованої потужності, а орбіти ототожнюються з потужностями $0,1,\ldots,|N|$. Отже, це модель колекціонера купонів із Прикладу 4.

– Розглянемо випадки, коли $N = \mathbb{N}$ – натуральні числа зі звичайним лінійним порядком. Решітку $\mathcal{O}_d(\mathbb{N})$ можна ототожнювати з $\mathbb{N}$ через потужність. Група симетрії $Aut\mathcal{O}_d(N)$ є тривіальною, усі орбіти є одиночними. Ненульові ймовірності переходу дорівнюють:

$$p(k,k) = k/(k+1), \qquad p(k,k+1) = 1/(k+1).$$

$$p^m(k,k) = k^m/(k+1)^m, \qquad p^m(k,k+m) = 1/(k+m)_m.$$

$$p^m(k,k+1) = \sum_{i=0}^{m-1} \frac{k^i}{(k+1)^{i+1}} \frac{(k+1)^{m-i-1}}{(k+2)^{m-i-1}} = \frac{(k+1)^{2m} - k^m(k+2)^m}{(k+1)^m(k+2)^{m-1}}$$

6.3.3 Про досконалі бінарні дерева

Визначення 4. Укорінене бінарне дерево називається *досконалим*, якщо всі його внутрішні вузли мають по два дочірніх, а всі листки мають однакову глибину або однаковий рівень.

Досконале бінарне дерево повністю визначається кількістю його листків. Щоб створити досконале бінарне дерево з ℓ рівнями ми повинні створити $2^\ell - 1$ доведень.

Досконале бінарне дерево M_ℓ з $2^\ell - 1$ вузлами як частково впордкована множина складається зі слів довжини $< \ell$ в алфавіті з двох літер, скажімо $\{0,1\}$; і $w \geqslant w'$ тоді і тільки тоді, якщо w' починається з w. Тож пусте слово ϵ відповідає найбільшому елементу – кореню. Рисунок 6.10 ілюструє випадок для M_4.

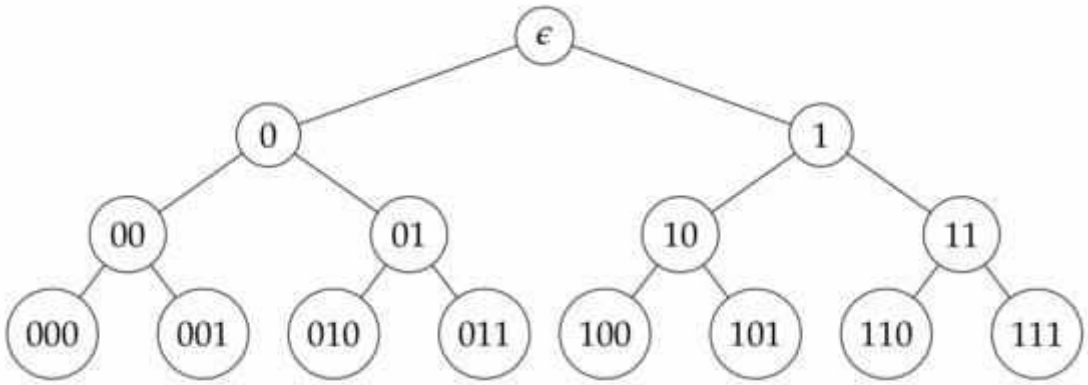


Рисунок 6.10. – Маркування вузлів досконалого двійкового дерева M_4

Кожне досконале бінарне дерево $M_{\ell+1}$ з $\ell+1$ рівнями як частково впорядкована множина є непересічною сумою двох копій дерев меншого рівня з додаванням найбільшого елемента

$$M_{\ell+1} \simeq (M_\ell \sqcup M_\ell) + \{\varepsilon\}. \tag{6.32}$$

Остання тотожність разом з (6.28) і (6.29) передбачає

$$\begin{aligned} \mathcal{O}_u(M_{\ell+1}) &\cong \{\varnothing\} + (\mathcal{O}_u(M_\ell) \times \mathcal{O}_u(M_\ell)), \\ \mathcal{O}_d(M_{\ell+1}) &\cong (\mathcal{O}_d(M_\ell) \times \mathcal{O}_d(M_\ell)) + \{M_\ell\}, \end{aligned}$$

тобто верхня множина або порожня, або складається з ϵ, а також з будь-яких верхніх множин у лівому та правому піддеревах. Зауважимо, що для двох незрівнянних вузлів x та y відповідні піддерева непересічні: $\{x\}^{\downarrow} \cap \{y\}^{\downarrow} = \varnothing$. Отже, нижні множини в дереві – це свого роду ліси, тобто непересічні об'єднання піддерев.

Твердження 7. Наступні послідовності описані рекурсивно.

Кількість $u_\ell = |\mathcal{O}_u(M_\ell)|$ верхніх множин у досконалому бінарному дереві M_ℓ :

$$u_{-1} = 0, \qquad u_{\ell+1} = u_\ell^2 + 1.$$

Це послідовність A003095[54]: 0, 1, 2, 5, 26, 677, 458330, ….

Кількість $v_\ell = |\mathcal{O}_u(M_\ell) / Aut M_\ell|$ орбіт таких верхніх множин:

$$v_0 = 1, \qquad v_{\ell+1} = \binom{v_\ell + 1}{2} + 1.$$

Це послідовність A006894[27]: 1, 2, 4, 11, 67, 2279 ….

Кожне сумісне загальне впорядкування на $M_{\ell+1}$ задається (6.32), згідно з (6.30) можна отримати як перемішування двох упорядкувань M_ℓ. Отже, кількість сумісних загальних упорядкувань досконалого бінарного дерева задовольняє рекурентним співвідношенням

$$|Ord(M_{\ell+1})| = |Ord(M_\ell)|^2 \binom{2^\ell - 2}{2^{\ell-1} - 1}$$

[54] The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. https://oeis.org.

і, отже, допускає явну формулу

$$|Ord(M_{\ell+1})| = (2^{\ell}-1)!/\prod_{k=1}^{\ell}(2^k-1)^{2^{\ell-k}},$$

яку можна інтерпретувати як кількість усіх перестановок на вузлах дерева, помножену на ймовірність того, що випадкова перестановка вузлів є сумісним порядком на дереві. Це послідовність A056972[27]: 1,2,80,21964800,748368258618359808000000, ….

Твердження 9. Групу симетрії досконалого бінарного дерева можна описати рекурсивно як сплетіння груп, тобто напівпрямий добуток:

$$\mathrm{Aut}(M_{\ell+1}) \simeq S_2 \ltimes (\mathrm{Aut}(M_\ell)\times \mathrm{Aut}(M_\ell)),$$

де симетрична група $S_2 = \{e,\tau\}$ діє справа шляхом перестановки на множники $\mathrm{Aut}(M_\ell)$. Тому

$$M_\ell \simeq S_2 \ltimes ((S_2 \ltimes ((S_2 \ltimes \cdots)\times(S_2 \ltimes \cdots)))\times(S_2 \times ((S_2 \ltimes \cdots)\times(S_2 \ltimes \cdots)))), \qquad (6.33)$$

де копії S_2 індексуються внутрішніми вузлами M_ℓ, тобто словами $w \in \{0,1\}^*$ довжини $<\ell-1$. Позначимо як τ_w транспонування з відповідної копії S_2, *‘симетрію у w’*. Відбувається перемикання між лівим і правим піддеревами на w (тобто $(w0v)^{\tau_w} = w1v$ і $(w1v)^{\tau_w} = w0v$ для $v \in \{0,1\}^*$) і залишає залишок фіксованим.

Група симетрії $\mathrm{Aut}\, M_\ell$ допускає представлення з усіма наведеними вище симетріями τ_w як генератори та відношення:

– $\tau_w^2 = e$;

– $\tau_w\tau_{w'} = \tau_{w'}\tau_w$ кожний раз, коли w і w' непорівнянні в M_ℓ (в цьому випадку τ_w і $\tau_{w'}$ існує в двох різних факторах прямого добутку в (6.33));

– $\tau_{wv}\tau_w = \tau_w\tau_{(wv)^{\tau_w}}$ (це правило множення для напівпрямого добутку в (6.33)).

Подання (6.33) елементів $\mathrm{Aut}\, M_\ell$ означає, що в кожну позицію, яка відповідає внутрішньому вузлу, позначеному словом w, можна поставити або транспозицію τ або нейтральний елемент e. Таким чином $\mathrm{Aut}\, M_\ell$ має $2^{2^{\ell-1}}-1$ елементів τ_w, які перебувають у взаємно однозначній відповідності з

підмножинами W на внутрішніх вузлах (де розташовані транспозиції τ). Для будь-якого сумісного загального впорядкування $\sigma \in Ord(W)$,

$$\tau_W := \tau_{\sigma^{-1}(|W|)} \tau_{\sigma^{-1}(|W|-1)} \cdots \tau_{\sigma^{-1}(1)}.$$

6.3.4 Розподілена генерація частково впорядкованих множин

Спочатку розглянемо моделі з Прикладів 11-13 які є узагальненнями моделей із Прикладів 5-7. Переходимо від множин до частково впорядкованих множин.

Позначення 8. Скінченну частково впорядковану множину N, позначимо $\mathcal{M}(N) = \prod_{\varnothing \neq N' \in \mathfrak{C}_u(N)} \mathcal{M}(MinN')$ як – декартовий добуток множин розподілів ймовірностей на всіх непорожніх антиланцюгах $MinN'$.

Приклад 11. Нехай N – частково впорядкована множина, а $\mu = (\mathbf{P}r_{Min(N')})_{\varnothing \neq N' \in \mathfrak{C}_u(N)} \in \mathcal{M}(N)$ – фіксовані розподіли ймовірностей. Ми розглядаємо ланцюг Маркова, де перебувають стани верхніх множин в N. Ненульовими елементами матриці переходів є

$$p(N', N'') = \sum_{g \in Sur(m, N' \setminus N'')} \prod_{i=1}^{m} \mathbf{P}r_{Min(N')}(g(i)), \qquad N' \setminus MinN' \subseteq N'' \subseteq N', \quad (6.34)$$

і існування сюрекції $m \twoheadrightarrow N' \setminus N''$ означає $|N' \setminus N''| \leqslant m$. У разі рівномірних розподілів ненульовими елементами матриці переходів є

$$p(N', N'') = |N' \setminus N''|! \cdot \left\{ \frac{m}{|N' \setminus N''|} \right\} \cdot |MinN'|^{-m}.$$

Якщо N є дискретною частково впорядкованою множиною, то $MinN' = N'$ є довільними підмножинами, і ми отримуємо ланцюг Маркова з Прикладу 5 .

Для ланцюга Маркова порожня множина $\varnothing$ є поглинаючим станом, і всі траєкторії строго спадають при включенні. Предметом нашого інтересу є час поглинання $\tau^{mN'} = \tau_{\mathbf{m}}^{mN'}$, що є випадковою величиною, яка дорівнює кількості кроків, які потрібно виконати для створення всіх доказів в верхній множині N'. Зауважимо, що $\tau^{mN} = k$ тоді і тільки тоді, якщо $p_{N\varnothing}^{k-1} = 0$ і $p_{N\varnothing}^{k} = 1$. Випадкова

величина τ^{mN} приймає значення в інтервалі $[ht(N),|N|]$, тобто $p^n_{N\varnothing}=0$ для $n<ht(N)$ і $p^n_{N\varnothing}=1$ для $n\geqslant|N|$. Тому можна виразити сподівання часу поглинання через елементи потужностей матриці переходів:

$$\mathbf{E}\tau^{mN}=\sum_{k=1}^{|N|}k(p^k_{N\varnothing}-p^{k-1}_{N\varnothing})=|N|-1-\sum_{k=1}^{|N|-1}p^k_{N\varnothing}. \qquad (6.35)$$

З іншого боку, у нас є рекурентна формула, що включає матричні елементи верхнього рядка p як коефіцієнти:

$$\mathbf{E}\tau^{mN}=1+\sum_{\varnothing\neq M\subseteq MinN}p_{NN\setminus M}\mathbf{E}\tau^{mN\setminus M}. \qquad (6.36)$$

Тепер ми можемо докладно розглянути Приклад 6 і Пропозицію 3 про стохастичну еквівалентність двох моделей для випадку частково впорядкованих множин. Для цього нам потрібно перейти від рівномірного розподілу ймовірностей до довільного.

Приклад 12. (Немарківська модель). Нехай дано розподіл ймовірностей $\mathbf{P}r_{Ord(N)}$ на множині сумісних загальних порядків $Ord(N)$. Потім для кожної верхньої множини $N'\in\mathcal{O}_u(N)$ розподіли ймовірностей на $Ord(N')$ і $MinN'$

$$\mathbf{P}r_{Ord(N')}(\sigma'):=\sum_{\substack{\sigma\in Ord(N)\\ \sigma|_{N'}=\sigma'}}\mathbf{P}r_{Ord(N)}(\sigma),$$

$$\mathbf{P}r_{MinN'}(a):=\sum_{\substack{\sigma'\in Ord(N')\\ \sigma'(a)=1}}\mathbf{P}r_{Ord(N')}(\sigma'), \qquad (6.37)$$

є унікальними, перетворюючи відображення $N\xrightarrow{\sigma\mapsto\sigma|_{N'}}N'\xrightarrow{\sigma'\mapsto(\sigma')^{-1}(1)}MinN'$ на морфізми ймовірнісних просторів. (Тут обмеження $\sigma|_{N'}$ визначається за (6.31)) Тоді ми можемо розглянути ланцюг Маркова з попереднього Прикладу 11 з розподілами ймовірностей на анти ланцюгах $MinN'$, отримані шляхом (6.37)

$$\mathbf{P}r_{MinN'}(a):=\sum_{\substack{\sigma\in Ord(N)\\ \sigma|_{N'}(a)=1}}\mathbf{P}r_{Ord(N)}(\sigma). \qquad (6.38)$$

Елемент декартового ступеня $(OrdN)^m$ відповідає обраному діапазону $\sigma_i\in Ord(N)$ кожним обчислювачем $1\leqslant i\leqslant m$. Він повністю визначає траєкторію для

цього ланцюга Маркова, тобто строго спадаючу послідовність верхніх множин ще не доведених кандидатів

$$N = N_0 \supset N_1 \supset N_2 \supset \cdots \supset N_k = \varnothing, \qquad N_{j+1} = N_j \setminus \left\{ \left(\sigma_i |_{N_j} \right)^{-1} (1) \,|\, 1 \leqslant i \leqslant m \right\},$$

разом із вибором в кожен момент часу $0 \leqslant j < k$ кожним обчислювачем $1 \leqslant i \leqslant m$ першого можливого кандидата на доказ $\left(\sigma_i |_{N_j} \right)^{-1} (1) \in MinN_j$ відповідно до власного діапазону. Тож з визначення видно, що умовні ймовірності таких відборів задаються за допомогою (6.38).

Розглянемо випадок, коли N є дискретною множиною і, отже, $MinN' = N'$ є довільними підмножинами. Якщо додатково припустити, що початковий розподіл $\mathbf{P}r_{OrdN}$ є рівномірним, то для кожного N' відповідні розподіли $\mathbf{P}r_{OrdN'}$ і $\mathbf{P}r_{MinN'}$ також є рівномірними, оскільки кількість доданків у (6.37) є незалежними від $\sigma' \in N'$ і $a \in MinN'$ відповідно. Вони індексуються в першому випадку за допомогою $|N|!/|N'|!$ перестановки N збереження порядку між елементами N', а в другому випадку – шляхом $(|N'|-1)!$ перестановок збереження a. Отже, це охоплює випадок Прикладу 6 і Пропозиції 6.

Слід підкреслити, що конструкція в цьому прикладі менш універсальна, ніж загальний випадок Прикладу 11. Наприклад, у разі $N = \{a\} \sqcup \{b < c\}$ з (6.38) отримуємо $\mathbf{P}r_{\{a,b\}}(a) = \mathbf{P}r_N(a < b < c)$, $\mathbf{P}r_{\{a,c\}}(a) = \mathbf{P}r_N(a < b < c, b < a < c)$ і обмеження $\mathbf{P}r_{\{a,b\}}(a) \leqslant \mathbf{P}r_{\{a,c\}}(a)$. Зокрема, розподіли ймовірностей $\mu = (\mathbf{P}r_{MinN'})_{\varnothing \neq N' \in \mathfrak{C}_u(N)}$, які мінімізують $\mathbf{E}\tau_{\mathbf{m}}^{mN}$, не можна отримати з цього прикладу.

Приклад 13. (Факторизація за групою симетрії). Розглянемо дані з Прикладу 11 у випадку, коли всі міри ймовірності $(\mathbf{P}r_{MinN'})_{\varnothing \neq N' \in \mathfrak{C}_u(N)}$ є $\mathrm{Aut}\, N$ - інваріантні, тобто

$$\mathbf{P}r_{MinN'} \circ \sigma = \mathbf{P}r_{MinN'}, \qquad \sigma \in \mathrm{Aut}\, N.$$

За Пропозицією 2, канонічна проекція $\pi : \mathcal{O}_u(N) \to \mathcal{O}_d(N) / \mathrm{Aut}\mathcal{O}_u(N)$ на орбітальну множину є грудкуючим відображенням.

Отже, ми отримуємо ланцюг Маркова з множиною станів $\mathcal{O}_u(N) / \mathrm{Aut}\, N$, а ймовірності переходу між орбітами задаються сумами (6.6) стосовно до (6.34)

$$p([N'],[N'']) = \sum_{N'''\in[N'']} p(N',N''') = \sum_{\substack{N'''\in[N'']\\ N'\setminus MinN'\subseteq N'''\subseteq N'}} \sum_{g:m\twoheadrightarrow N'\setminus N'''} \prod_{i=1}^{m} \mathbf{P}r_{Min(N')}(g(i)) \qquad (6.39)$$

У разі дискретної частково впорядкованої множини N, елементи $\mathcal{O}_u(N)$ є підмножинами N, група симетрії $\mathrm{Aut}\,N$ складається з усіх перестановок і орбіт $\mathcal{O}_u(N)/\mathrm{Aut}\,N$, які є цілими числами $0,1,\ldots,|N|$, що ототожнюються з потужностями підмножин. Отже, ми отримуємо ланцюг Маркова з Прикладу 7.

У випадку $N = M_\ell$ досконалого бінарного дерева з ℓ рівнями, стани ланцюга Маркова з Прикладу 11 (та з Прикладу 13 відповідно) є верхніми множинами в M_ℓ (орбіти таких верхніх множин під дією $\mathrm{Aut}\,M_\ell$). Відповідно до Пропозиції 7, кількість таких множин N' або орбіт множин швидко зростають залежно від ℓ. Більше того, якщо ми вирішимо розглядати не тільки рівномірні розподіли ймовірностей на антиланцюгах $MinN'$, то отримаємо багато додаткових параметрів.

Для випадку $\ell = 3$, орієнтований граф ланцюга Маркова з Прикладу 13 для M_3 представлений на Рисунку 6.11. Він має 11 станів, не має циклів (крім циклу для кінцевого стану $\varnothing$); матриця переходів трикутна; $\mathrm{Aut}\,M_3$ – інваріантні ймовірнісні міри на різних $MinN'$ повністю залежать від 3 параметрів.

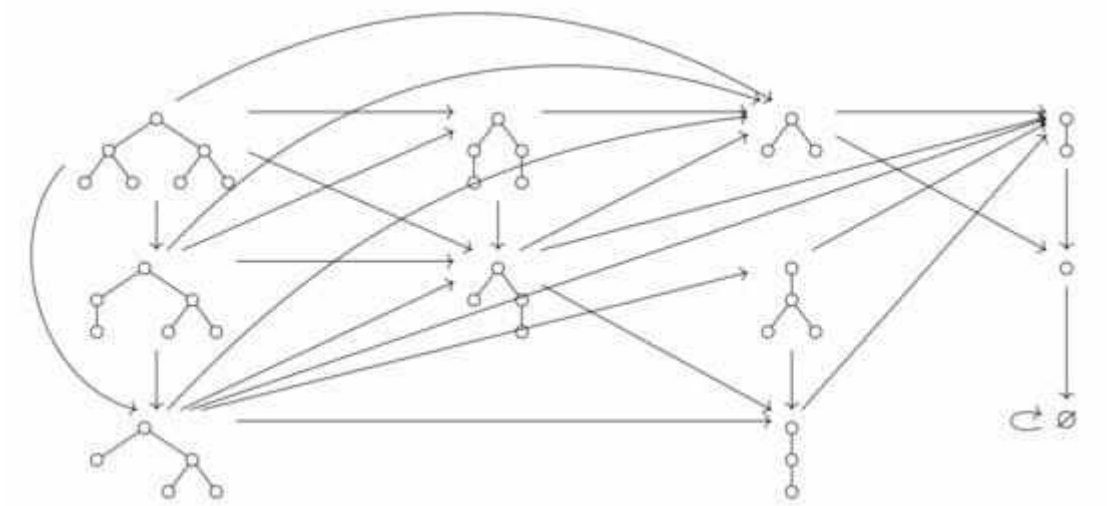


Рисунок 6.11 – Ланцюг Маркова для M_3 (факторизований $\mathrm{Aut}\,M_3$)

6.3.5 Деяка асимптотика для τ^{mN}

Для фіксованої скінченної частково впорядкованої множини $N \neq \varnothing$ та фіксованого числа обчислювачів $m \geqslant 2$, предметом нашого інтересу є пошук мінімуму $\mathbf{E}\tau_{\mathbf{m}}^{mN}$ серед усіх можливих ($\mathrm{Aut}\, N$ - інваріант) мір $\mathbf{m} = (\mathbf{P}r_{MinN'})_{\varnothing \neq N' \subseteq N}$, та їх границь, коли $m \to \infty$. Ми описуємо цю асимптотичну поведінку в термінах верхніх множин.

Далі ми покажемо, що математичне сподівання $\mathbf{E}\tau^{mN}$ прагне до свого мінімально можливого значення (рівного висоті $ht(N)$), коли число обчислювачів m зростає. Відмітимо, що кожна фіксована скінченна частково впорядкована множина N можна представити у вигляді непересічного об'єднання

$$N = \bigcup_{k=0}^{ht(N)-1} MinN_{/k}, \qquad N_{/0} := N, \quad N_{/(k+1)} = N_{/k} \setminus MinN_{/k}. \tag{6.40}$$

Твердження 10. Нехай $\mathbf{P}r_{MinN_{/k}}(a) > 0$ для всіх цілих $k \in [0, ht(N)-1]$ та для всіх $a \in MinN_k$. Тоді

$$\lim_{m \to \infty} \mathbf{E}\tau^{mN} = ht(N).$$

Доведення. Для кожного $\varepsilon > 0$, існує $m_0 \in \mathbb{N}$ таке, що для всіх $m \geqslant m_0$ для всіх k з $[0..htN)$ всі елементи $MinN_{/k}$ будуть обчислені (доведені) на кроці $(k+1)$ з імовірністю $> 1-\varepsilon$. □

Для деяких типів частково впорядкованих множин N, ми отримаємо асимптотику у вигляді

$$\min_{\mathbf{m} \in \mathfrak{M}(N)} \mathbf{E}\tau_{\mathbf{m}}^{mN} \underset{m \to \infty}{\sim} ht(N) + \alpha_N \gamma_N^m + o(\gamma_N^m), \qquad 0 \leqslant \gamma_N < 1. \tag{6.41}$$

Випадок актуальний, коли N допускає досить багату симетрію.

Твердження 11. Нехай N є скінченною частково впорядкованою множиною такою, що у позначеннях (6.40) для кожного $N_{/k}$, $k = 0,1,\ldots,htN-1$ його симетрична група $\mathrm{Aut}\, N_{/k}$ діє транзитивно на $MinN_{/k}$. У цьому випадку, для великої кількості обчислювачів m з точністю до $o\left((1-1/wdN)^m\right)$ маємо

$$\min_{\mathbf{m} \in \mathfrak{M}(N)} \mathbf{E}\tau_{\mathbf{m}}^{mN} \underset{m \to \infty}{\sim} htN + \kappa_N \cdot wdN \cdot (1-1/wdN)^m, \tag{6.42}$$

де κ_N є кількістю таких k, що $\#MinN_{/k} = wdN$.

Доведення. Дія транзитивності $\mathrm{Aut}\, N_{/k}$ на $MinN_{/k}$ означає, що рівномірний розподіл ймовірностей на $MinN_{/k}$ є оптимальним. Позначимо праву частину (6.42) як $\Phi(N)$ та $n_k = |MinN_{/k}|$. За індукцією, ми можемо записати $\min_{\mathbf{m}\in\mathcal{M}(N_{/k})}\mathbf{E}\tau_{\mathbf{m}}^{mN_{/k}}$ як суму

$$1+\frac{n_k!mn_k}{n_k^m}\min_{\mathbf{m}\in\mathcal{M}(N_{/(k+1)})}\mathbf{E}\tau_{\mathbf{m}}^{mN_{/(k+1)}}+n_k\frac{(n_k-1)!mn_k-1}{n_k^m}\min_{\mathbf{m}\in\mathcal{M}(N^+_{/(k+1)})}\mathbf{E}\tau_{\mathbf{m}}^{mN^+_{/(k+1)}}+\cdots,$$

де $N^+_{/(k+1)}$ - це $N_{/(k+1)}$ з одним додатковим елементом з $MinN_{/k}$ (у всіх випадках ми отримуємо ізоморфні частково впорядковані множини); та "$\cdots$" означає доданки, які є малими у порівнянні з $(1-1/wdN)^m$. Далі, ми вилучаємо малі доданки з формули включення-виключення (6.5) для чисел Стірлінга:

$$\begin{aligned}\min_{\mathbf{m}\in\mathcal{M}(N_{/k})}\mathbf{E}\tau_{\mathbf{m}}^{mN_{/k}} &\underset{m\to\infty}{\sim} 1+\left(1-n_k(1-1/n_k)^m\right)\Phi(N_{/(k+1)})+n_k(1-1/n_k)^m\cdot htN^+_{/k}\\ &\underset{m\to\infty}{\sim}\Phi(N_{/(k+1)})+\Phi(MinN_{/k}).\end{aligned}$$

Тоді у всіх трьох можливих випадках $wdN_{/(k+1)}=wdN_{/k}, n_k=wdN_{/k}$ або $wdN_{/(k+1)}<wdN_{/k}, n_k=wdN_{/k}$ або $wdN_{/(k+1)}=wdN_{/k}, n_k<wdN_{/k}$ маємо $\Phi(N_{/(k+1)})+\Phi(MinN_{/k})\sim\Phi(N_{/k})$ з точністю до $o\left((1-1/wdN)^m\right)$.

□

Досконале бінарне дерево M_ℓ задовольняє припущенням Пропозиції 11; ми маємо $htM_i=\ell$, $wdM_i=2^{i-1}$ та $\kappa_{M_i}=1$.

Наслідок 2. Для досконалого бінарного дерева M_ℓ та великої кількості обчислювачів m

$$\min_{\mathbf{m}\in\mathcal{M}(M_i)}\mathbf{E}\tau_{\mathbf{m}}^{mM_i}\underset{m\to\infty}{\sim}\ell+2^{i-1}\left(\frac{2^{i-1}-1}{2^{i-1}}\right)^m, \tag{6.43}$$

та відповідна ймовірність

$$\mathbf{P}r(\tau^{mM_i}=\ell)\underset{m\to\infty}{\sim}1-2^{i-1}\left(\frac{2^{i-1}-1}{2^{i-1}}\right)^m. \tag{6.44}$$

Далі розглянемо випадок співдобутків ланцюгів

$$N=\coprod_{1\le i\le k}\mathbf{n}_i=\{(i,j)\,|\,1\le i\le k\wedge 1\le j\le n_i\},\qquad n_i>0. \tag{6.45}$$

k-ий спільний добуток $N = \bigsqcup_{1 \le i \le k} \mathbf{n}$ ланцюга $\mathbf{n}$ задовольняє припущенням Пропозиції 11. Ми маємо $htN = \kappa_N = n$ та $wdN = k$.

Наслідок 3. Для позитивних цілих k та n,

$$\min_{\mathbf{m} \in \mathcal{M}(\bigsqcup_{1 \le i \le k} \mathbf{n})} \mathbf{E}\tau_{\mathbf{m}}^{m \bigsqcup_{1 \le i \le k} \mathbf{n}} \underset{m \to \infty}{\sim} n + kn(1-1/k)^m + o\left((1-1/k)^m\right). \tag{6.46}$$

Якщо припущення Пропозиції 11 щодо симетрії частково впорядкованої множини N порушуються, асимптотичні формули (6.41) стають більш складними. Ми можемо отримати явну формулу для найпростішого випадку.

Твердження 12. Для позитивних цілих n_1, n_2,

$$\min_{\mathbf{m} \in \mathcal{M}(\mathbf{n}_1 \sqcup \mathbf{n}_2)} \mathbf{E}\tau_{\mathbf{m}}^{m \mathbf{n}_1 \sqcup \mathbf{n}_2} \underset{m \to \infty}{\sim} n_1 \vee n_2 + \left(\binom{n_1 \vee n_2}{n_1 \wedge n_2} \frac{n_1 + n_2 + 1}{|n_1 - n_2| + 1} - 1 \right) \left(\frac{1}{|n_2 - n_1| + 2} \right)^m$$

з точністю до $o\left((|n_2 - n_1| + 2)^{-m}\right)$, де $n_1 \vee n_2 = \max\{n_1, n_2\}$ та $n_1 \wedge n_2 = \min\{n_1, n_2\}$.

Доведення. По-перше, покажемо що, якщо $n_2 > n_1 > 0$, тоді числа $\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1$ задовольняють рекурсивному правилу Паскаля та граничним умовам

$$\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1 = (\alpha_{(\mathbf{n}_1 - \mathbf{1}) \sqcup (\mathbf{n}_2 - \mathbf{1})} + 1) + (\alpha_{\mathbf{n}_1 \sqcup (\mathbf{n}_2 - \mathbf{1})} + 1), \tag{6.47}$$

$$\alpha_{\mathbf{0} \sqcup \mathbf{n}} = \alpha_{\mathbf{n}} = 0, \qquad \alpha_{\mathbf{n} \sqcup \mathbf{n}} = 2n. \tag{6.48}$$

(Друга гранична умова випливає з (6.46).)

Припустимо, що $n_2 > n_1$, та розподіл ймовірностей $\mathbf{P}r_{Min \mathbf{n}_1 \sqcup \mathbf{n}_2}$ на $Min \mathbf{n}_1 \sqcup \mathbf{n}_2 = \{(1,1), (1,2)\}$ задано за допомогою $\mathbf{P}r_{Min \mathbf{n}_1 \sqcup \mathbf{n}_2}(1, j) = p_j$, $j = 1, 2$ та $p_1 + p_2 = 1$. Тоді за індукцією $\mathbf{E}\tau^{m \mathbf{n}_1 \sqcup \mathbf{n}_2}$ можна записати як

$$1 + p_1^m \min \mathbf{E}\tau^{m \mathbf{n}_1 - \mathbf{1} \sqcup \mathbf{n}_2} + p_2^m \min \mathbf{E}\tau^{m \mathbf{n}_1 \sqcup \mathbf{n}_2 - \mathbf{1}} + (1 - p_1^m - p_2^m) \min \mathbf{E}\tau^{m \mathbf{n}_1 - \mathbf{1} \sqcup \mathbf{n}_2 - \mathbf{1}}.$$

Прибравши апріорно малі доданки, ми можемо переписати цей вираз як

$$\sim n_2 + \alpha_{n_1 - 1 n_2 - 1} \left(\frac{1}{n_2 - n_1 + 2} \right)^m + p_1^m + \alpha_{n_1 n_2 - 1} \left(\frac{1}{n_2 - n_1 + 1} \right)^m p_2^m.$$

Метод множників Лагранжа для $m \to \infty$ призводить до $p_1 = 1/(n_2 - n_1 + 2)$ та

$$\min \mathbf{E}\tau^{m\mathbf{n}_1 \sqcup \mathbf{n}_2} \sim n_2 + (1+\alpha_{n_1-1 n_2-1} + \alpha_{n_1 n_2-1})\left(\frac{1}{n_2-n_1+2}\right)^m .$$

Так ми отримуємо правило Паскаля (6.47).

Далі ми знаходимо генеруючу функцію для подвійної послідовності $\alpha_{\mathbf{n}_1 \sqcup \mathbf{n}_2} + 1$:

$$f(x,y) = \sum_{k=0}^{\infty}\sum_{n=k}^{\infty}(\alpha_{\mathbf{k}\sqcup\mathbf{n}}+1)x^k y^{n-k} = \frac{1+x}{(1-x)(1-x-y)}.$$

Цей явний вираз можна отримати шляхом спрощення $(1-x-y)f(x,y)$ використовуючи рекурентне співвідношення (6.47) і граничні умови (48).

Нарешті, отримуємо коефіцієнти $\alpha_{\mathbf{k}\sqcup\mathbf{n}}+1 = [x^k y^{n-k}]f(x,y)$ з

$$\sum_{n=0}^{\infty}\sum_{k=0}^{n}(\alpha_{\mathbf{k}\sqcup\mathbf{n}}+1)x^k y^{n-k} = (1+x)(1+x+x^2+\cdots)\left(1+(x+y)+(x+y)^2+\cdots\right). \qquad \square$$

Наступним кроком буде:

Проблема 1. Знайти асимптотичну формулу (6.41) для довільного кінцевого співдобутку (6.45) скінченних ланцюгів.

$$\begin{aligned}\min \quad & \mathbf{E}\tau^{\mathbf{1}\sqcup\mathbf{1}\sqcup\mathbf{2}} \\ & = 2x^m(3+3^{1-m}) + (1-2x)^m(2+3\cdot 2^m\cdot 3^{-m} - 3^{1-m} + 3^{1-m}2^{1-m}) + 3(2^m x^m - 2x^m) \\ & +2((1-x)^m - x^m - (1-2x)^m)(2+2^{1-m}) + ()\end{aligned}$$

Для кожної фіксованої частково впорядкованої множини N, можна розглянути n-ий спільний добуток $\coprod_{i\in\mathbf{n}} N$, а потім дослідити залежність часу поглинання $\tau^{m\coprod_{i\in\mathbf{n}} N}$ від кількості копій n та кількості обчислювачів m. Якщо N є сінглетоном, отримуємо випадкову величину τ^{mn} з Прикладу 7.

Гіпотеза 7. Для скінченної частково впорядкованої множини N, існує узагальнення функції $h(x)$ з Гіпотези 2, задане границею

$$h_N(x) := \lim_{\substack{m,n\to\infty \\ n/m \to x}} \min \mathbf{E}\tau^{m\coprod_{i\in\mathbf{n}} N} .$$

Ця функція має ряд властивостей, які узагальнюють властивості $h(x)$.

6.3.6 Практична реалізація процесу генерації дерев доведень

Для стабільного та ефективного функціонування сайдчейну необхідно, щоб були дотримані наступні умови:

– усі транзакції, які лідер блоку планує включити до виданого блоку, мають бути оброблені в межах часового інтервалу, тобто часу, відведеного на створення цього блоку, а відповідне дерево доведень має бути повністю побудоване;

– кількість цих транзакцій має бути максимально можливою, для якої ймовірність побудови відповідного дерева доведень близька до 1.

Перша умова необхідна для того, щоб мінімізувати або звести до нуля кількість доведень, які будуть створені, але не використані, тобто щоб праця обчислювачів не пройшла даремно. Друга умова необхідна для максимізації пропускної здатності сайдчейну.

Тому необхідно визначити, враховуючи параметри мережі (такі як довжина часового інтервалу та кількість активних доведень), таку максимальну кількість листків, щоб відповідне дерево доведень було повністю побудовано в межах часового інтервалу з ймовірністю принаймні $1-\varepsilon$ для досить малого $\varepsilon > 0$.

Ми припускаємо, що довжина часового інтервалу фіксована протягом усього життя сайдчейну. Ми також припускаємо, що час, необхідний для формування одного доведення, однаковий протягом усього життя сайдчейну для всіх майнерів. Цей час буде називатися тіком. Значення ділення тривалості часового інтервалу на тривалість тіка дорівнює кількості доведень, які кожен активний майнер може створити протягом одного часового інтервалу. Оскільки довжини часового інтервалу та тіку фіксовані, кількість таких доведень протягом інтервалу часу також фіксована. Однак кількість доведень може відрізнятися.

Завдання полягає в тому, щоб визначити максимальну кількість транзакцій у блоці для заданих значень k тіків у часовому інтервалі та m обчислювачів, для яких буде побудовано відповідне дерево доведень з імовірністю не менше $1-\varepsilon$.

Для вирішення цієї задачі скористаємося результатами підрозділу 3, а також зробимо наступні припущення.

Будемо вважати, що обчислювачі будують усі рівні дерева доведень послідовно, від листків до кореня. Спочатку обчислюємо ймовірності того, що відповідний рівень буде повністю побудований за $1, 2, 3, \ldots$ тіків (для заданого числа доведень та обчислювачів). Потім, використовуючи ці ймовірності, ми знаходимо кількість рівнів, які будуть побудовані з імовірністю у $\geqslant 1-\varepsilon$ за $\leqslant k$ тіків:

$$\mathbf{P}r(\tau^{mM_i} \leqslant k) \approx \sum_{\substack{k_1+\cdots+k_i \leqslant k^{1-r-i} \\ k_1,\ldots,k_i \geqslant 1}} \prod \mathbf{P}r(\tau^{m2^{r-1}} = k_r).$$

Якщо $\mathbf{P}r(\tau^{m2^{i'-1}} = 1) \approx 1$, ми можемо звести попередню формулу до:

$$\mathbf{P}r(\tau^{mM_\ell} \leqslant k) \approx \sum_{\substack{k_{i'+1}+\cdots+k_i \leqslant k-(i'-i'<r\leqslant i \\ k_{i'+1},\ldots,k_i \geqslant 1}} \prod \mathbf{P}r(\tau^{m2^{r-1}} = k_r).$$

Для вирішення нашої задачі може бути використана Таблиця 6.1, яка вказує на ймовірності побудови заданої кількості доведень для заданої кількості обчислювачів за задану кількість тіків.

Кожен рядок у Таблиці 6.1 відповідає певній фіксованій кількості доведень. Стовпці відповідають рівням дерева доведень, починаючи з другого рівня від кореня. Напр., в клітинці з координатами "512 обчислювачів, 32 доведення" є список з двох пар чисел: $\begin{smallmatrix}1;0{:}999997\\2;0.000003\end{smallmatrix}$. Це означає, що 512 обчислювачів побудують 32 доведення точно за 1 тік з ймовірністю 0.999997 та точно за 2 тіка з ймовірністю 0.000003. Імовірність побудови 32 доведень не більше, ніж за 2 тіки є нерозрізнювальною від 1.

Розраховуємо максимальну кількість транзакцій у блоці, яку 512 обчислювачів можуть обробити з ймовірністю не менше 0.95 за 9 тіків.

Таблиця 6.1 – Розподіл ймовірності для τ^{mn} з точністю до 10^{-6} та ймовірностями створення дерева за 9 тіків

$m \backslash n$	2	4	8	16	32	64	128	256	9 ticks
3	1; 0.750000 2; 0.250000	2; 0.810764 3; 0.187500 4; 0.001736	3; 0.346759 4; 0.598575 5; 0.054020 6; 0.000643 7; 0.000003						$\ell = 4$ 0.948934
4	1; 0.875000 2; 0.125000	1; 0.093750 2; 0.856554 3; 0.049624	2; 0.038452 3; 0.791998 4; 0.167602 5; 0.001946 6; 0.000002						$\ell = 4$ 0.998582
9	1; 0.996094 2; 0.003906	1; 0.711365 2; 0.288588 3; 0.000047	1; 0.010815 2; 0.928031 3; 0.061145 4; 0.000009	2; 0.006789 3; 0.824258 4; 0.168743 5; 0.000210					$\ell = 5$ 0.892535
10	1; 0.998047 2; 0.001953	1; 0.780602 2; 0.219387 3; 0.000011	1; 0.028163 2; 0.944047 3; 0.027789 4; 0.000001	2; 0.036465 3; 0.901558 4; 0.061960 5; 0.000017					$\ell = 5$ 0.951990
16	1; 0.999969 2; 0.000031	1; 0.960000 2; 0.040000	1; 0.306798 2; 0.693034 3; 0.000168	1; 0.000001 2; 0.720767 3; 0.279205 4; 0.000027	3; 0.323989 4; 0.673970 5; 0.002041				
32	1; 1.000000	1; 0.999598 2; 0.000402	1; 0.891278 2; 0.108722	1; 0.073443 2; 0.926430 3; 0.000127	2; 0.490645 3; 0.509350 4; 0.000005				$\ell = 6$ 0.948374
33	1; 1.000000	1; 0.999699 2; 0.000301	1; 0.904520 2; 0.095480	1; 0.089692 2; 0.910235 3; 0.000073	2; 0.561396 3; 0.438602 4; 0.000002				$\ell = 6$ 0.961682
64	1; 1.000000	1; 1.000000	1; 0.998446 2; 0.001554	1; 0.765182 2; 0.234818	1; 0.004182 2; 0.995734 3; 0.000084	2; 0.226404 3; 0.773595 4; 0.000001			
94	1; 1.000000	1; 1.000000	1; 0.999972 2; 0.000028	1; 0.963319 2; 0.036681	1; 0.163487 2; 0.836513	2; 0.969308 3; 0.030692			$\ell = 7$ 0.944377
95	1; 1.000000	1; 1.000000	1; 0.999975 2; 0.000025	1; 0.965585 2; 0.034415	1; 0.173944 2; 0.826056	2; 0.973714 3; 0.026286			$\ell = 7$ 0.950428
128	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.995870 2; 0.004130	1; 0.562887 2; 0.437113	1; 0.000013 2; 0.999930 3; 0.000057	2; 0.048095 3; 0.951905		
256	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999999 2; 0.000001	1; 0.990585 2; 0.009415	1; 0.304309 2; 0.695691	2; 0.999956 3; 0.000044		
451	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999981 2; 0.000019	1; 0.948528 2; 0.051472	1; 0.018313 2; 0.981687		$\ell = 8$ 0.949452
452	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999981 2; 0.000019	1; 0.949314 2; 0.050686	1; 0.018930 2; 0.981070		$\ell = 8$ 0.950256
512	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999997 2; 0.000003	1; 0.980019 2; 0.019981	1; 0.088899 2; 0.911101		
1024	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999994 2; 0.000006	1; 0.959185 2; 0.040815		
2175	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999995 2; 0.000005	1; 0.949825 2; 0.050175	$\ell = 9$ 0.949820
2176	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 1.000000	1; 0.999995 2; 0.000005	1; 0.950016 2; 0.049984	$\ell = 9$ 0.950011

Перші 5 рівнів (включаючи корінь) будуть оброблені кожен за 1 тік з ймовірністю, що майже дорівнює 1. Отже, ми маємо максимум 4 тіки, щоб побудувати ті, що залишились. Зверніть увагу, що восьмий рівень можна побудувати за 1 тік з дуже малою ймовірністю 0.088899, тому цей рівень вимагає двох тіків. Ймовірність побудувати його не більше ніж за два тіки становить $0.088899 + 0.911101$, що практично дорівнює 1. Отже, якщо дерево містить 8 рівнів, тоді 2 тіки залишається для побудови 6-го та 7-го рівнів, 1 тік на кожен

рівень. Згідно з результатами в таблиці 1, ймовірність побудови цих двох рівнів за 2 тіки становить $0.999997 \cdot 0.980019 = 0.980016$, що більше 0.95. Отже, блок з 128 транзакціями буде випущений з імовірністю принаймні 0.95 що задовольняє нашим вимогам.

Аналогічно можна показати, що ймовірність випуску блоку з 256 транзакціями значно менше 0.95. Отже, якщо є 512 активних обчислювачів, рекомендовано випускати блоки з 128 транзакціями.

На основі Таблиці 6.1 ми побудували Таблицю 6.2, яка показує рекомендовану кількість транзакцій у блоці для різної кількості доведень. Усі можливі значення кількості доведень розбиті тут на інтервали, відповідно до кількості транзакцій у блоці. Наприклад, 2176 обчислювачів побудують блок з 512 транзакціями з ймовірністю 0.95001, та 2175 обчислювачів з ймовірністю 0.949825. Отже, якщо кількість обчислювачів щонайменше 2176, тоді рекомендована кількість транзакцій у блоці становить 512, а якщо кількість обчислювачів від 998 до 2175, тоді рекомендована кількість транзакцій становить 256.

Таблиця 6.2 – Рекомендована кількість транзакцій у блоці $2^{\ell-1}$, відповідна ймовірність створення блоку $1-\varepsilon = 0.95$ (для різної кількості обчислювачів)

m	[1..3]	[4..9]	[10..32]	[33..94]	[95..451]	[452..2175]	$\geqslant$2176
$2^{\ell-1}$	4	8	16	32	64	128	256

Зауваження 6. Можна розв’язати (6.44) як рівняння щодо кількості доведень:

$$m \approx \frac{\ln n - \ln \varepsilon}{-\ln(1-1/n)}, \qquad n = 2^{\ell-1}, \quad \varepsilon = 1 - \mathbf{P}r(\tau^{mM_\ell} = \ell).$$

У нашому випадку $n = 256$ та $\varepsilon = 0.05$, і ми маємо $m \approx 2182$. Це збігається з останньою границею 2176 в Таблиці 6.2 з точністю до $(2182 - 2176) / 2176 \approx 0.3\%$.

6.4 Висновки до шостого розділу

У цьому розділі ми показали, як на базі сайдчейнів з Latus-консенсусом та zk-SNARK-доведеннями можна створити зручний децентралізований блокчейн, який дозволяє залучити багатьох незалежних користувачів до обробки та розповсюдження інформації у блокчейні. Для побудови такої конструкції ми суттєво використовували результати роботи[55], яку можна розглядати як обмежений прообраз нинішньої, і роботи[56], в яких вивчалися деякі аспекти теорії ігор, що виникають, коли обчислювачі встановлюють ціни на свої доведення. Усі статті із цієї серії присвячені деяким конкретним практичним проблемам, які можуть бути сформульовані в загальному вигляді як умови функціонування повністю децентралізованих сайдчейнів на основі протоколу консенсусу Latus, які дозволяють всім бажаючим учасникам обробляти та поширювати інформацію за певну винагороду. Ми частково вирішили ці проблеми, аналізуючи існуючі математичні моделі та методи та створюючи наші специфічні моделі, наприклад, розподіли ймовірностей на частково впорядкованих множинах, які найбільше підходять для сучасних цілей.

Особливістю цієї роботи є деякі гіпотези, які були сформульовані на основі великої кількості чисельних результатів, отриманих за допомогою обчислень нескінченної точності. На нашу думку, завдання доведення їх усіх видається досить нетривіальним. Чисельні результати, отримані в кінці роботи, дозволяють вибрати правильні значення деяких параметрів для досягнення стабільності та високої пропускної здатності в сайдчейнах.

В подальших дослідження, які будуть продовжувати цю серію, планується брати до уваги більш загальний, ефективніший і складніший підхід, коли серія блоків будується одночасно, що дозволяє обчислювачам створювати доведення для кількох послідовних блоків. Слід зазначити, що цей підхід дозволяє збільшувати пропускну здатність по суті без втрати рівня безпеки сайдчейну, а тому є корисним і цікавим.

---

[55] Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Models of distributed proof generation for zk-SNARKbased blockchains. In Theoretical and Applied Cryptography; Belarusian State University: Minsk, Belarus, 2020; pp. 112–120. http://conf.bsu.by/data/theoreticalandappliedcrypto/doc/TAC_2020_Proceedings.pdf.

[56] Bespalov, Y.; Garoffolo, A.; Kovalchuk, L.; Nelasa, H.; Oliynykov, R. Game-Theoretic View on Decentralized Proof Generation in zk-SNARK Based Sidechains. In Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021); 2021; Vol. 2923, - CEUR Workshop Proceedings, pp. 47–59. http://ceur-ws.org/Vol-2923/.

7 ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ З ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ ЗАПРОПОНОВАНИХ РІШЕНЬ ЯК ОСНОВИ ПЕРСПЕКТИВНОЇ СИСТЕМИ МОНІТОРИНГУ, ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА ІДЕНТИФІКАЦІЇ МЕРЕЖНИХ АТАК. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ ЧЕРЕЗ ІМПЛЕМЕНТАЦІЮ РОЗРОБЛЕНОЇ СИСТЕМИ МОНІТОРИНГУ, ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА ІДЕНТИФІКАЦІЇ АТАК У ДІЮЧІ ІНФОРМАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Система виявлення вторгнень (СВВ) на основі сигнатур намагаються ідентифікувати шкідливі дії в системі, порівнюючи спостерігаючу поведінку з відомими моделями атак. У системах такого типу база даних використовується для зберігання поведінки раніше відомих атак, які закодовані як сигнатури. Отже, ці системи здатні виявляти атаки, знаходячи схожі сигнатури в базі даних.

СВВ на основі сигнатур можуть працювати надійно, коли спостерігається вже відома схема атаки. В результаті у них дуже низький рівень помилкових спрацьовувань. Однак відсутність здатності виявляти невідомі атаки є основним недоліком систем такого типу, що робить його небажаним рішенням порівняно з іншими типами.

Розглянемо кілька прикладів та деяких методів, які можна використовувати для ідентифікації кожної сигнатури [121-124]:

– спроба підключення із зарезервованої IP-адреси – це легко визначити, перевіривши поле адреси джерела в заголовку IP;

– пакет із незаконною комбінацією прапорців TCP – це можна дізнатися, порівнявши прапорці, встановлені в заголовку TCP, з відомими гарними або поганими комбінаціями прапорців;

– електронна пошта, що містить певний вірус – СВВ може порівнювати тематику кожного електронного листа з темою, пов’язаною з електронною поштою, або може шукати вкладення з певним іменем;

– спроба переповнення буфера DNS, що міститься в корисному навантаженні запиту – розбираючи поля DNS і перевіряючи довжину кожного з них, СВВ може ідентифікувати спробу виконання переповнення буфера за допомогою поля DNS (іншим методом було б шукати використання послідовностей shellcode у корисному навантаженні);

– відмова від сервісної атаки на сервері POP3, викликана видачею однієї і тієї ж команди тисячі разів – одним підписом для цієї атаки було б відстежувати, скільки разів команда видається, і попереджувати, коли це число перевищує певний поріг;

– атака доступу до файлів на FTP-сервері шляхом видачі на нього команд файлів та каталогів без попереднього входу в систему – можливо, буде розроблений підпис відстеження стану, який відстежуватиме FTP-трафік для успішного входу та попереджатиме, якщо певні команди були видані до того, як користувач отримав автентифікацію належним чином.

Класифікація пакетів на основі корисного навантаження включає дослідження корисного навантаження пакетів, також відоме як «Глибока перевірка пакетів» (DPI). Правило (сигнатура) корисного навантаження використовується для класифікації пакетів, які можуть дати точні результати. Сигнатури – це окремі рядки в корисних навантаженнях пакетів, які можна використовувати для їхньої диференціації. Пакети можна класифікувати за відповідності сигнатур до вмісту корисних навантажень [125-128].

Глибокий аналіз пакетів (англ. Deep Packet Inspection - DPI) – технологія накопичення статистичних даних, перевірки і фільтрації мережних пакетів за їхнім вмістом. DPI аналізує не тільки заголовки пакетів, а й повний вміст трафіка з другого і вище рівнів моделі OSI. DPI здатне виявляти і блокувати віруси, фільтрувати інформацію, що не задовольняє заданим критеріям [129, 130].

DPI може приймати рішення не тільки за вмістом пакетів, але і за непрямими ознаками, властивим якимось певним мережним програмам і протоколам. Для цього може використовуватися статистичний аналіз (наприклад статистичний аналіз частоти зустрічі певних символів, довжини пакета і т. ін.).

DPI часто використовуються провайдерами для контролю трафіку, а іноді і для блокування деяких протоколів, таких як BitTorrent. За допомогою DPI

можна визначити, яка програма генерує або отримує дані, і на підставі цього зробити будь-яку дію. Крім блокування, DPI може збирати детальну статистику з'єднання кожного користувача окремо. Також, за допомогою quality of service DPI може управляти швидкістю передачі окремих пакетів, піднявши її або, навпаки, зменшивши, змінювати пріоритети передачі різних типів даних, наприклад, прискорюючи відкриття Інтернет сторінок за рахунок зменшення швидкості завантаження великих файлів. DPI використовується у великих корпораціях для запобігання випадкових витоків даних, а також для захисту від відправки по e-mail внутрішніх захищених файлів [131-134].

7.1 Результати моделювання роботи методу аналізу сигнатур заснованого на глибокому аналізі пакетів та рейтингуванні бази сигнатур

7.1.1 Опис СВВ на основі сигнатур Snort

Snort є найбільш популярною системою виявлення вторгнень, що заснована на сигнатурах. Snort реалізований так, що весь мережний трафік проходить через нього і застосовується політика безпеки щодо цього трафіка. Політика реалізується шляхом створення правил Snort, які відповідають змісту, який потрібно виявити. Якщо Snort використовується лише для мережних СВВ, то копія всього трафіку надсилається до Snort. Цей трафік аналізується Snort і відповідно генеруються результати. Зазвичай це використовується лише для оповіщення та статистики мережного трафіку, і це означає, що виявлення вторгнень не є профілактикою. Для СЗВ Snort реалізований таким чином, що весь трафік проходить через нього до досягнення пункту призначення. Сервер Snort розміщується таким чином, що весь трафік проходить через нього до досягнення внутрішньої мережі [135, 136].

Сервер Snort – це система, на якій встановлено та налаштовано Snort. Для їхньої реалізації два інтерфейси Ethernet створюються в межах Snort як мостова мережа. Весь трафік проходить через Snort, який виступає в якості першого інтерфейсу. Він обробляє мережний трафік згідно з правилами, які реалізуються,

і вживає відповідних дій. Якщо деякий трафік потрібно заблокувати, він скидає цей трафік і не дає йому пройти.

На рисунку 7.1 показано основні функціональні можливості Snort. Модуль захоплення пакетів (PCAP) використовується для зйомки вхідних пакетів трафіку. Далі декодер пакетів ідентифікує протокол і класифікує пакет відповідно до специфікації зв'язку пакета даних. Препроцесори (наприклад, препроцесор SMTP, препроцесор POP, препроцесор FTP/TELNET і препроцесор сеансу) готують пакети для обробки двигуном виявлення. По-перше, препроцесори збирають фрагменти Internet Protocol (IP) та потоки протоколу управління передачею (TCP). Потім вони перевіряють пакети на предмет будь-якого трафіку, який знаходиться поза сферою дії механізму виявлення. Препроцесори також можуть змінювати пакети, щоб двигуну виявлення було легше обробляти пакети. Наприклад, аномалії TCP, такі як дані, отримані поза вікном TCP, не можуть обробляти механізм виявлення. Препроцесор сеансу може виявити ці відсутні дані та змінити пакет, щоб повернути його у вікно TCP, щоб його можна було виявити. Двигун виявлення виявляє мережний трафік на основі набору визначених правил [137, 138]. Нарешті, звіти генеруються за допомогою вихідних плагінів.

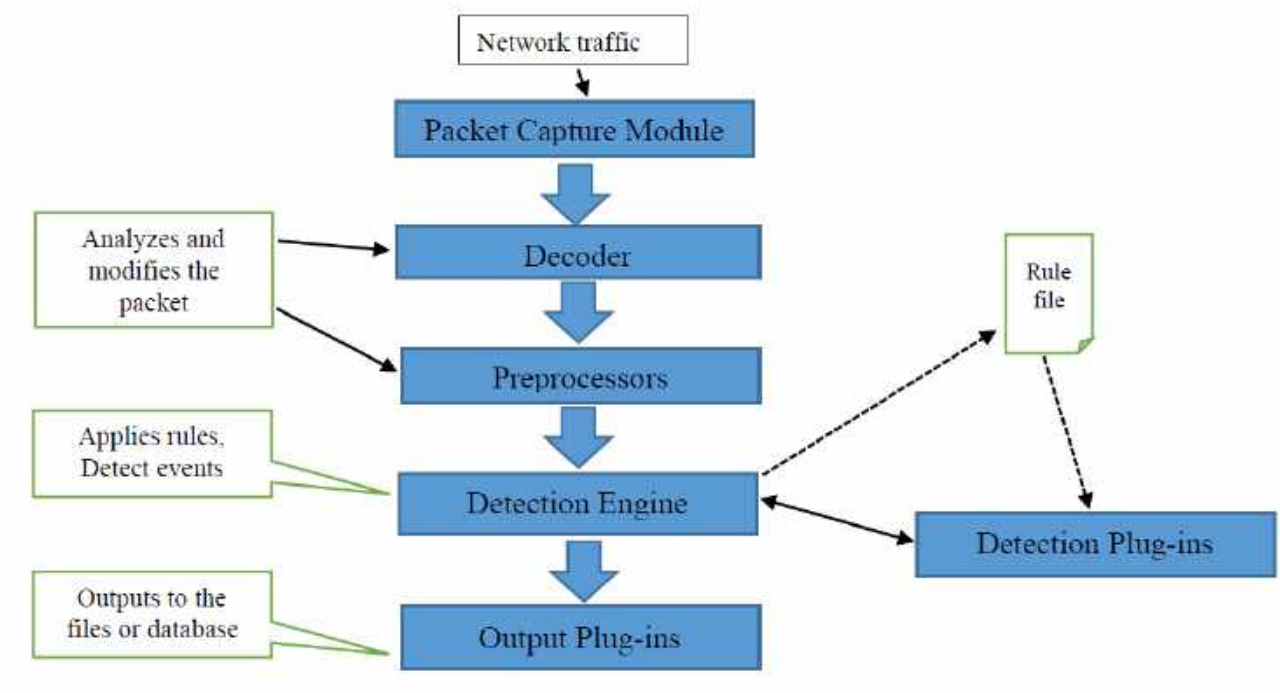


Рисунок 7.1 – Алгоритм функціонування Snort

В Snort реалізовано правило, а політика проводиться відповідно до цього правила. Snort застосовує відповідні дії, коли правило відповідає інтернет-трафіку. На рисунку 7.2 показана основна структура правила Snort, яка складається із заголовка і параметрів правила.

Заголовок Snort забезпечує дію, яку слід застосувати з адресою вказаного мережного трафіка. Правило задається протоколом, адресою джерела, IP-адресою джерела, напрямом потоку трафіку, IP-адресою пункту призначення та портом призначення [137]. На рисунку 7.2 показано зразок правила Snort. Заголовок правила містить інформацію, яка може надсилати попередження для пакету в потоці TCP, джерелом IP-адреси є 192.168.1.1 з будь-якою адресою порта джерела до будь-якого IP-адресата, що має номер порту 80. Параметри правила задають ім’я правила та ідентифікатор правила разом із вмістом, який потрібно виявити. Snort виконує встановлені дії, коли заголовок і параметри правил відповідають змісту пакета.

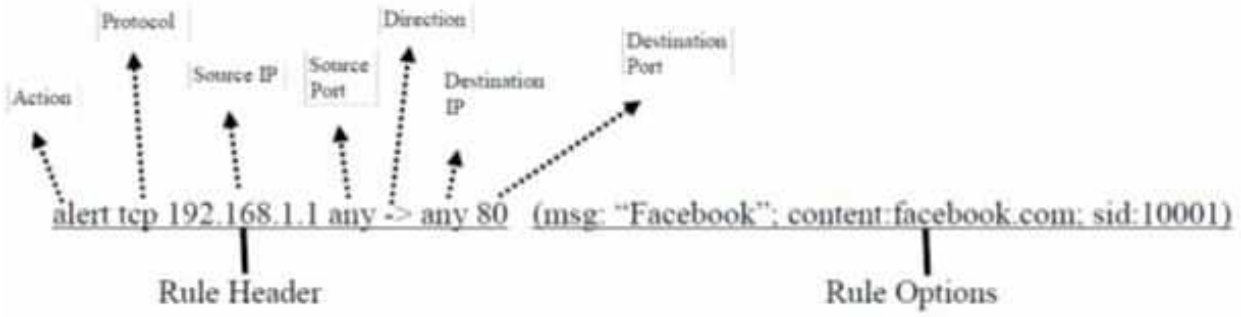


Рисунок 7.2 – Приклад правила в Snort

7.1.2 Практичне використання запропонованого методу.

Для проведення експериментів було обрано систему Snort, в яку підключався модуль роботи запропонованого алгоритму аналізу сигнатур з глибокою перевіркою пакетів і дешифруванням. Правила створюються для виявлення різних протоколів. Ці правила подають сповіщення, коли вони узгоджуються з трафіком, що проходить через Snort. Для створення правил потрібно збирати дані, фільтрувати та готувати дані. Ця методологія зображена

на діаграмі, показаній на рисунку 7.3, і детально розглядається нижче на прикладі.

Як вхідний трафік і атаки був узятий набір даних з датасетів [138, 139] які включають в себе набір записів з'єднань, в той час як кожне з'єднання складається з набору пакетів, переданих з певної вихідної IP-адреси на цільову IP-адресу для зазначеного протоколу за короткий проміжок часу. Навчальний набір і набір тестування складаються зі звичайних і атакуючих з'єднань.

Звичайні з'єднання складаються з різних протоколів, таких як TCP, UDP, ICMP і т.ін. Крім того, мають бути також включені різні види послуг, наприклад, FTP, Telnet і т.д. Різні типи атак випадковим чином синтезуються в звичайні потоки з'єднань відповідно до ймовірністі.

Рисунок 7.3 – Алгоритм роботи Snort для DPI

Всього в датасеті є сорок один параметр. Вони згруповані в чотири категорії: основні параметри, параметри контенту, параметри трафіка на основі часу і параметри трафіка на основі хоста. Ім'я та відповідний номер (#) для кожного параметра вказані в табл.7.1.

Основні параметри визначаються заголовками пакетів без необхідності перевірки DPI. Параметри контенту містять інформацію для перевірки вмісту

корисного навантаження в пакетах TCP, наприклад, кількість невдалих спроб входу в систему, знання інформації про домен і т. ін. Параметри трафіка на основі часу описують властивості в двосекундному часовому вікні, наприклад, кількість з'єднань з одним і тим самим хостом і т. д. Параметри трафіку на основі хоста використовуються для зображення атак у період W за кількістю з'єднань, а не в часовому інтервалі, наприклад, в кількості цільових хост-сервісів. У ході експерименту було зменшено кількість ознак в аналізованих параметрах.

Таблиця 7.1 – Опис ознак датасетів

Категорії	Найменування ознак
Основні ознаки	Duration, Protocol_type, Service, Flag, Src_bytes, Dst_bytes, Land, Wrong_frangment, Urgent
Ознаки контенту	Hot, Num_failed logins, Logged_in, Num_compromised, Root_shell, Su_attemped, Num_root, Num_file_creation, Num_shells, Num_access_files, Num_otbound_cmds, Is_hot_logins, Is_guest_login
Ознаки трафіка, засновані на часі	Count, Srv_count, error_rate, Srv_error_rate, Rerror_rate, Srv_rerror_rate, Same_srv_rate, Diff_srv_rate, Srv_diff_host_rate
Ознаки трафіка хоста	Dst_host_count, Dst_host_srv_count, Dst_host_same_srv_rate, Dst_host_diff_srv_rate, Dst_host_same_src_port_rate, Dst_host_srv_diff_host_rate, Dst_host_error_rate, Dst_host_srv_error_rate, Dst_host_rerror_rate, Dst_host_srv_rerror_rate

В таблиці 7.2 описані параметри, які прийняті як ознаки для виявлення вторгнень.

Таблиця 7.2 – Обрані ознаки

Категорії	Найменування ознак
Основні ознаки	Duration, Protocol_type, Service, Src_bytes, Dst_bytes, Num_failed logins, Logged_in, Root_shell, Num_root, Num_file_creation, Num_shells, Num_access_files, Num_otbound_cmds, Count, error_rate, Srv_rerror_rate, Same_srv_rate, Dst_host_srv_count, Dst_host_same_src_port_rate, Dst_host_rerror_rate

Перевірені правила реалізуються на мережному інтерфейсі для створення сповіщень про трафік у режимі реального часу. Snort аналізує вхід і вихід трафіка на мережний інтерфейс. Були створені правила для виявлення трафіка Facebook та Gmail. Snort налаштований на мережному інтерфейсі eth0. Проаналізувавши трафік Facebook та Gmail, Snort генерує результати. Snort працював 1 хвилину і 55 секунд і аналізував 37447 пакетів за хвилину. Загальна кількість отриманих

пакетів становить 37794, а Snort проаналізував 37448 цих пакетів, що становить 99,085%. Залишок з 346 пакетів Snort не аналізував через помилки в структурах пакетів. Ці пакети можна проаналізувати вручну.

На рисунку 7.4 наведено розбиття проаналізованого трафіка за протоколами. Це показує, що 99,997% аналізованих пакетів – це пакети IPv4, а 0,003% – пакети IPv6. Крім того, 94,686% аналізованого трафіку становить TCP, тоді як 5,285% – це UDP. На рисунках 7.5 та 7.6 показана статистика сповіщень, що генеруються в ході аналізу трафіка. Він також показує дії, які вчинив СВВ. Snort також створив файл журналу обробленого трафіка, який може бути використаний у ідентифікаторі відкритого додатка для обчислення пропускної здатності, використовуваної кожною веб-програмою. Ідентифікатор відкритого додатка містить деякі набори правил за замовчуванням для виявлення споживання пропускної здатності різних типів мережного трафіка. Його можна відключити, але в цьому випадку було ввімкнено виявити пропускну здатність, споживану кожною веб-програмою. Отримання статистики щодо кожного використовуваного веб-додатка є основною метою DPI. У цьому прикладі були створені правила для виявлення двох веб-додатків. У DPI правила можуть створюватися та оновлюватися для виявлення кожної веб-програми, щоб невідомий трафік можна було мінімізувати.

```
# Signatures to detect application
#Facebook Signatures
alert tcp any any -> any any (msg: "Facebook"; content: "facebook.com"; http_uri; fast_pattern; sid:10001; rev:1;)
alert tcp any any -> any any (msg: "Facebook"; pcre:"/.facebook.com|.facebook.net|.fb.com|.fbcdn.net|.fbsbx.com|.fb.me/i"; sid:10002; rev:1;)
#Gmail Signatures
alert tcp any any -> any any (msg: "Gmail"; content: "mail.google.com"; http_uri; fast_pattern; sid:10011; rev:1;)
alert tcp any any -> any any (msg: "Gmail"; pcre:"/mail.google.com|.Gmail.com/i"; sid:10012; rev:1;)
```

Рисунок 7.4 – Правила для детектування трафіка Facebook та Gmail

На наступному кроці створюються правила з метою безпеки, щоб уникнути заговору про тероризм. На рисунку 7.7 показано два правила, створені для виявлення вмісту, пов’язаного з тероризмом. Тобто сигнатурами виступають слова: робити бомбу, купувати пістолет і використовувати пістолет. Якщо хтось шукає цей вміст в Інтернеті, Snort DPI генерує попередження з датою, часом, адресою та джерелом IP-адреси. Ці ІС можуть бути додатково проаналізовані аналітиком з безпеки, щоб зменшити будь-які майбутні ризики.

```
===============================================================
Run time for packet processing was 115.127039 seconds
Snort processed 37447 packets.
Snort ran for 0 days 0 hours 1 minutes 55 seconds
   Pkts/min:        37447
   Pkts/sec:          325
===============================================================
Memory usage summary:
  Total non-mmapped bytes (arena):       75206656
  Bytes in mapped regions (hblkhd):      15835136
  Total allocated space (uordblks):      6579624
  Total free space (fordblks):           68627032
  Topmost releasable block (keepcost):   60536
===============================================================
Packet I/O Totals:
   Received:        37794
   Analyzed:        37448 ( 99.085%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:          346 (  0.915%)
   Injected:            0
===============================================================
```

Рисунок 7.5 – Пакети оброблені Snort

```
-------------------------------------------------------------
Action Stats:
     Alerts:            8 (  0.021%)
     Logged:            8 (  0.021%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            7
Verdicts:
      Allow:        37428 ( 99.032%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:           19 (  0.050%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
```

Рисунок 7.6 – Результати дій Snort

На рисунку 7.8 показано правило для сповіщень про пошук тероризму та попередження Gmail. На рисунку 7.9 показано правила, створені для блокування трафіка Facebook. Основна відмінність – слово drop замість попередження у правилі Snort, тому воно скине виявлений вміст. Результати для трафіку, заблокованого Snort, показані на рисунку 7.10. Дев’ять сповіщень були створені Snort, і Snort заблокував усі 3305 пов’язаних пакетів.

```
# Signatures to alert on content search for security reasons
alert tcp any any -> any any (msg: "Terrorism Content Search"; content: "terrorism"; sid:10021; rev:1;)
alert tcp any any -> any any (msg: "Terrorism Content Search"; pcre:"/make bomb|buy gun|buy pistol|use gun/i"; sid:10022; rev:1;)
```

Рисунок 7.7 – Правила для детектування контенту тероризма

```
saad@saad-VirtualBox:~$ sudo /usr/local/bin/snort -A console -q -c /etc/snort/snort.conf -i eth0
07/22-16:33:02.600637  [**] [1:10012:1] Gmail [**] [Priority: 0] {TCP} 216.58.193.101:443 -> 10.0.2.15:55738
07/22-16:33:25.905642  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.908641  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.908704  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.908736  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.908765  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.909622  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.909665  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
07/22-16:33:25.909695  [**] [1:10021:1] Terrorism Content Search [**] [Priority: 0] {TCP} 199.102.160.7:80 -> 10.0.2.15:52662
^C*** Caught Int-Signal
saad@saad-VirtualBox:~$
```

Рисунок 7.8 – Сповіщення створені Snort при детектуванні контенту тероризма

```
# Signatures to drop or block internet traffic
#Facebook drop
drop tcp any any -> any any (msg: "Facebook"; content: "facebook.com"; http_uri; fast_pattern; sid:11081; rev:1;)
drop tcp any any -> any any (msg: "Facebook"; pcre:"/.facebook.com|.facebook.net|.fb.com|.fbcdn.net|.fbsbx.com|.fb.me/i"; sid:11082; rev:1;)
```

Рисунок 7.9 – Правила блокування трафіка Facebook

```
======
Action Stats:
     Alerts:              9 (   0.272%)
     Logged:              9 (   0.272%)
     Passed:              0 (   0.000%)
Limits:
      Match:              0
      Queue:              0
        Log:              0
      Event:              0
      Alert:              9
Verdicts:
      Allow:              0 (   0.000%)
      Block:           3305 (100.000%)
    Replace:              0 (   0.000%)
  Whitelist:              0 (   0.000%)
  Blacklist:              0 (   0.000%)
     Ignore:              0 (   0.000%)
      Retry:              0 (   0.000%)
==================================================
```

Рисунок 7.10 – Трафік заблокований Snort

У таблиці 7.3 наведено показники якості ідентифікації атак запропонованого в даній дисертації методу аналізу сигнатур, заснованого на глибокому аналізі пакетів і часу порівняння пакетів із сигнатурами.

Таблиця 7.3 – Якість роботи методу аналізу сигнатур

	% знайдених атак	% невиявлених атак	% втрачених даних	% помилкових спрацьовувань	F1 міра	Час роботи у вікні W, мс
Snort	92,5	7,5	6,8	8,4	0,93	0,5
Стандартний аналіз сигнатур	93,01	6,9	6,2	7,9	0,93	0,53

Метод аналізу сигнатур, який використовує глибокий аналіз пакетів для аналізу вмісту трафіка ідентифікує 93% атак, також він має низьку кількість хибнопозитивних спрацьовувань (менше 8%).

7.2 Розробка комплексного методу виявлення вторгнень, який базується на використанні аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів

Кожен з методів детектування атак, заснований на поведінкових характеристиках та сигнатурах має як недоліки, так і переваги. Існують підходи, які пропонують комбіноване використання деяких методів для поліпшення ефективності детектування атак. Пропонується метод виявлення вторгнень на основі комплексного використання методів сигнатурного аналізу, аналізу аномалій та протоколів і навежено аналіз результатів його роботи [122, 136, 140].

В даному випадку мережна СВВ має множину детекторів і аналізатор трафіка. Якість роботи СВВ характеризується точністю метрик, рівнем виявлення (DR) і рівнем помилкових спрацьовувань (FPR), Точністю і Повнотою, F-мірою. Нехай показує ймовірність виявлення вторгнень під час

роботи методу поведінки [124]. В цьому випадку – функція залежить від показників, які характеризують СВВ:

$$P_b = f\left(Recall, Precision, F_\beta, DR, FPR\right).$$

Нехай $A_b^i, i = 1,2,3,...$ змінні, що позначають деякі порогові ймовірності виявлення вторгнень. Вибираючи потрібну функцію f і порогові значення виявлення вторгнень можна варіювати налаштування роботи СВВ (кількість правил тривоги, кількість спрацьовувань тривоги, рівень спрацьовувань тривоги, рівень блокування, реагування на атаку тощо).

У даній роботі було встановлено такі пороги: $A_b^1 = 0,9$, $A_b^2 = 0,7$, $A_b^3 = 0,5$. Це пов'язано з тим, що ймовірність виявлення вторгнень більше 90% є практично точною ідентифікацією наявності атаки, $A_b^2 = 0,7$ вказує на те, що необхідний додатковий аналіз трафіка. Якщо ж ймовірність виявлення менше 50%, то це з великою часткою ймовірності вказує на відсутність атаки [130, 133]. Схему роботи запропонованого комплексного методу наведено на рисунку 7.11. Розглянемо роботу комплексного методу більш докладно.

Попередня обробка трафіка. На вхід детекторів надходить трафік, який детектори захоплюють і відсилають на передобробку для зведення трафіка у зручний вид для обробки і аналізу.

Далі трафік аналізується, вибираються статистичні характеристики трафіка, ознаки, за якими трафік класифікуватиметься.

Метод поведінки. Далі трафік відсилається на аналіз методом поведінки за допомогою методів машинного навчання.

1. При $P_b \geq A_b^1$ метод поведінки відправляє трафік у підсистему реагування на атаки (або вилучає його) і записує дані про атаку в базу даних атак.

2. При $A_b^2 \leq P_b < A_b^1$ трафік відправляється на аналіз методом аналізу протоколів.

3. При $A_b^3 \leq P_b < A_b^2$ відправляється на аналіз методом сигнатурного аналізу, минаючи метод аналізу протоколів.

4. При $P_b < A_b^3$ трафік без будь-яких додаткових перевірок відправляється далі в мережу.

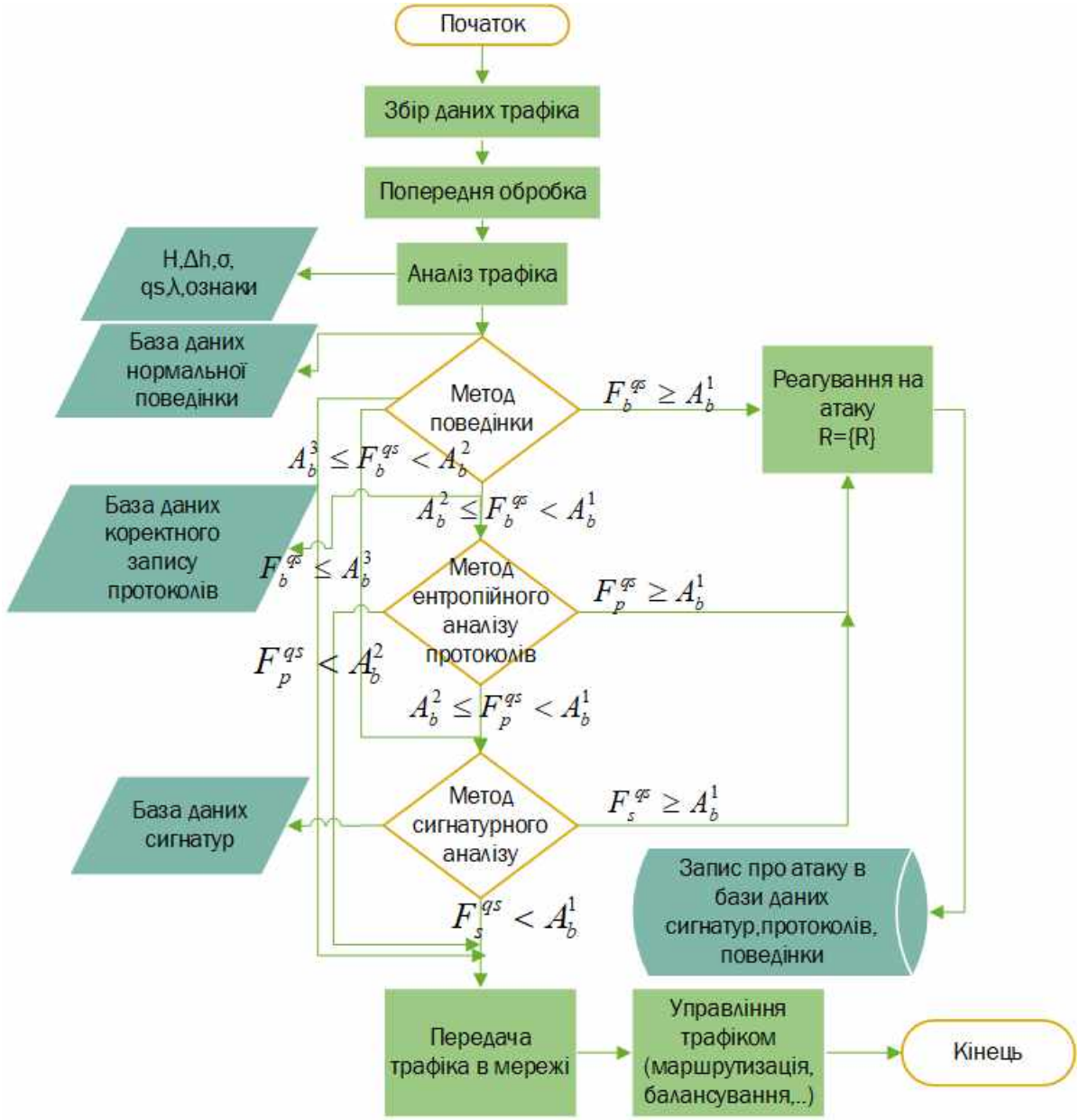


Рисунок 7.11 – Схема роботи комплексного методу виявлення вторгнень

Метод аналізу протоколів. Трафік, який був переданий на вхід методу аналізу протоколів, наприклад на основі ентропійного аналізу, проходить такі кроки:

1. При $P_b \geq A_b^1$ метод аналізу протоколів відправляє трафік у підсистему реагування на атаки (або вилучає його) і записує дані про цю атаку в базу даних атак.

2. При $A_b^2 \leq P_b < A_b^1$ трафік відправляється на аналіз методом сигнатурного аналізу.

3. При $P_b < A_b^2$ трафік без всяких додаткових перевірок відправляється далі в мережу.

Метод сигнатурного аналізу. Трафік, що надійшов на вхід методу сигнатурного аналізу, обробляється і порівнюється з існуючими сигнатурами атак.

1. При $P_b \geq A_b^1$ метод аналізу протоколів відправляє трафік у підсистему реагування на атаки (або вилучає його) і записує дані про цю атаку в базу даних атак.

2. При $P_b < A_b^1$ трафік без будь-яких додаткових перевірок відправляється далі в мережу.

Далі трафік передається всередині мережі відповідно до встановлених правил обробки і передачі.

Розроблено комплексний метод виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Для перевірки ефективності розробленого методу необхідно провести моделювання його роботи.

7.3 Результати моделювання роботи комплексного методу виявлення вторгнень

Результати роботи запропонованого комплексного методу показані в табл.7.4-7.7. Результати роботи кожного методу окремо і комплексного методу збігаються з результатами, отриманими іншими дослідниками [121, 123, 125, 126].

Для проведення експериментів в мережу відправлявся трафік кожні 8 мс. Далі цей самий трафік відправлявся збільшуючи інтенсивність, тобто кожні 4 мс, і далі кожну 1 мс. У таблиці 7.4 наведено показники ефективності роботи СВВ,

використовуючи які, можна проаналізувати запропоновані методи ідентифікації атак.

Таблиця 7.4 – Показники ефективності СВВ

Показники ефективності	Опис
отримані пакети	Кількість отриманих пакетів
проаналізовані пакети	Відсоток проаналізованих пакетів від загального числа отриманих пакетів
відкинуті пакети	Відсоток відкинутих пакетів від загального числа отриманих пакетів
відфільтровані пакети	Відсоток пакетів не показаних для СВВ
невиконані пакети	Відсоток пакетів, буферизованих в очікуванні обробки / або не оброблені

У таблиці 7.5 наведено результати роботи запропонованих у даній дисертації методів ідентифікації атак і існуючої СВВ Suricata в ході зміни інтенсивності трафіку. У таблиці 7.6 наведено показники якості ідентифікації атак запропонованих у даній дисертації методів. У таблиці 7.7 наведено результати роботи запропонованого комплексного методу і існуючих комплексних методів, запропонованих іншими дослідниками.

Таблиця 7.5 – Показники ефективності методів для різної інтенсівності трафіка

Трафік	Трива-лість переда-вання пакетів	Suricata	Метод поведінки	Метод ентропійного аналізу протоколів	Метод аналізу сигнатур	Комплекс-ний метод
Отримані пакети	8 мс	100%	100%	100%	100%	100%
	4 мс	100%	100%	100%	100%	100%
	1 мс	100%	100%	100%	100%	100%
Проаналізовані пакети, %	8 мс	99,99	100	97,78	98,86	100%
	4 мс	62,16	83,11	68,77	62,01	84,56
	1 мс	16,07	56,25	16,69	13,45	59,97
Відкинуті пакети, %	8 мс	0	0	0	0	0
	4 мс	27,45	14,46	25,78	27,94	24,25
	1 мс	45,63	38,83	44,05	46,02	40,44
Непроаналізовані пакети, ;%	8 мс	0,01	0	2,22	1,14	0
	4 мс	37,84	16,89	31,23	37,99	15,44
	1 мс	83,93	43,75	83,31	86,55	40,03

Таблиця 7.6 – Якість роботи комплексного алгоритму

	Метод поведінки	Метод ентропійного аналізу	Метод аналізу сигнатур	Комплексний метод
% виявлених атак	94,2	96,3	97,2	98
%* невиявлених атак	5,8	3,7	2,8	2
% втрачених даних	3,1	5,4	6,2	3,2
% помилкових спрацьовувань	2	15	0,7	0,5
F1 міра	0,87	0,94	0,96	0,98
Час роботи в період W, мс	0,41	0,48	0,5	0,47

Порівняльний аналіз роботи комплексного метода показав високу точність ідентифікації атак при різній інтенсивності трафіку. Комплексний метод показав більш високу точність ідентифікації атак (більше 98%) на відміну від існуючих. Залежно від необхідного рівня ідентифікації атак можна прискорити роботу комплексного методу шляхом зміни порогових значень виявлення.

Таблиця 7.7 – Якість роботи комплексного методу виявлення вторгнень

	Khan-2019	Shah-2018	Hu-2017	Запропонований комплексний метод
% виявлених атак	97	97	95	98
% невиявлених атак	0.3	0.3	0.5	0.2
% втрачених даних	7	3.2	9.8	3.2
% помилкових спрацьовувань	0.71	3.2	1.7	1.6
F1 міра	0.973	0.953	0.944	0.98

Для проведення порівняння запропонованих методів забезпечення безпеки (ЗМ) з існуючими (ІМ) було визначено набір параметрів, що характеризують забезпечення безпеки, якість обслуговування та врахування самоподібних властивостей трафіка. Також визначено низку параметрів, що уможливлюють оцінювання ефективності застосування методів виявлення вторгнень (кібератак). Результати порівняння наведено в табл.7.8, де позначка «+» означає, що даний метод враховує вказаний параметр, позначка «–» означає, що параметр не враховується.

Таблиця 7.8 – Результати дослідження існуючих методів забезпечення безпеки інформації під час її передачі та запропонованих

Методи		Ступінь утилізації каналів, %	Надійність, коефіцієнт готовності %	Затримки пакетів, мс	Джитер, мс	Втрати, %	Самоподібність трафіка	Конфіденційність	Цілісність	Доступність	Виявлення вторгнень, %	Заблокований атакований трафік, %
1		**2**	**3**	**4**		**5**	**6**	**7**	**8**	**9**	**10**	**11**
Метод балансування	ІМ	0,72	97	120	22	1,98	–	–	–	+	–	50
	ЗМ	0,6	99,9	100	18	0,98	+	–	–	+	+	99,5
Метод машрутизації	ІМ	0,7	97	67	28	1,5	–	+	–	+	–	1,2
	ЗМ	0,65	99,9	88	21	1,68	+	+	–	+	+	10
Метод балансування СВВ	ІМ	0,8	99	70	20	–	–	+	+	+	–	67
	ЗМ	0,7	99,9	50	17	–	+	+	+	+	–	81
Метод сигнатурного аналізу	ІМ	–	–	110	–	6,8	–	+	+	+	98	98
	ЗМ	–	–	96	–	6,2	–	+	+	+	97	97
Метод ентропійного аналізу протоколів	ІМ	–	–	48	–	–	–	+	+	+	87	87
	ЗМ	–	–	56	–	–	–	+	+	+	96	96
Метод машинного навчання	ІМ	–	–	51	–	–	–	+	+	+	94	94
	ЗМ	–	–	41	–	–	+	+	+	+	95	95
Комплексний метод виявлення вторгнень	ІМ	–	–	72	–	–	–	+	+	+	97	97
	ЗМ	–	–	68	–	–	+	+	+	+	99	99

Ґрунтуючись на результатах аналізу, наведених в табл. 7.8, можна зробити наступні висновки. Існуючі методи балансування навантаження та маршрутизації інформаційних потоків у комп’ютерних системах базуються на параметрах якості обслуговування, але не враховують параметри безпеки та виявлення вторгнень. Запропоновані методи безпечного балансування та безпечної маршрутизації враховують самоподібні властивості трафіка та параметри безпеки, за рахунок чого мають кращу якість обслуговування та забезпечують необхідний рівень безпеки. Запропоновані методи виявлення вторгнень використовують глибоку перевірку пакетів, ентропійний аналіз протоколів, методи машинного навчання та враховують самоподібні властивості інформаційних потоків, що призводить до більш ефективного виявлення вторгнень, ніж в існуючих методах.

7.4 Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак що базується на хмарному підході машинного навчання для умов низької продуктивності кінцевих пристроїв

Дублююча система оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини є розподіленою інформаційною системою та як і інші розподілені системи широко використовуються в системах збору інформації, моніторингу, розповсюдження інформації та управління. Невисокі вимоги щодо продуктивності пристроїв які об’єднані у цю систему дозволяють суттєво зменшити витрати на її впровадження та забезпечити їх автономність та великий час роботи. З іншого боку, широке їх використання та впровадження в багатьох сферах людського життя робить цю систему та кінцеві пристрої привабливими для різного роду атак. Це створює необхідність впровадження підсистеми захисту інформації у майбутню дублюючу систему оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини та є актуальним завданням, яке потребує негайного вирішення. Однією з складових системи захисту інформації є підсистема виявлення атак і аномалій трафіку.

У цих умовах низька продуктивність пристроїв не дозволяє повною мірою використовувати накопичений досвід захисту інформації, що використовується в комп’ютерних мережах і великих інформаційних системах. Викладене висуває вимоги щодо структури такої системи та розробки нових підходів і рішень для адаптації існуючих технологій захисту інформації в розподілених мережах, які б враховували особливості таких кінцевих пристроїв. Застосування методів машинного навчання для виявлення комп’ютерних атак активно обговорюється в останні роки, при цьому важливим аспектом досліджуваної предметної області є оцінка можливості практичної реалізації розроблених алгоритмів.

Запропонована архітектура складається з двох ключових рівнів, які взаємодіють через Інтернет (рис. 7.12): рівень хмарного сервісу, який контролює

керування моделями машинного навчання, що складають IDS, і рівень кінцевих пристроїв, який об’єднує кінцеві пристрої у керовані підмножини з однаковими IDS моделями.

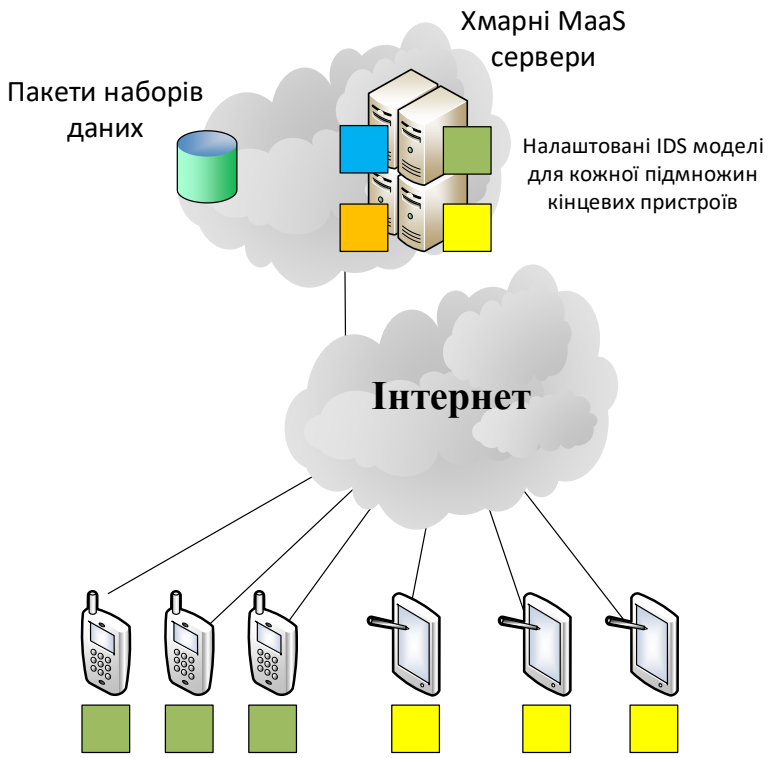


Рисунок 7.12 – Архітектура хмарної IDS

Хмарний сервіс, Model as a Service (MaaS), інтегрована в хмарний рівень для виконання важких завдань від імені кінцевих пристроїв, включаючи вибір ознак, створення моделі, навчання, тестування, та здійснює взаємодію з компонентами, що розміщуються на кінцевих пристроях дублюючої системи оповіщення населення про надзвичайні події у регіоні. Хмарний сервіс потенційно може адаптувати розроблені моделі, щоб найкраще відповідати робочим ресурсам кожного пристрою, шляхом оптимізації функцій навчання, встановлених у моделі пристроїв.

На рівні кінцевих пристроїв виконуються задачі з меншою обчислювальною складністю. До таких задач відносяться такі, як виділення атрибутів із мережевого трафіку та прогнозування аномалій трафіку за допомогою моделі IDS. Система групує кінцеві пристрої дублюючої системи

оповіщення населення про надзвичайні події у регіоні з однаковими ролями та ресурсами в підмножини для керування, щоб оптимізувати робоче навантаження хмарної служби. Аномалії, виявлені кінцевими пристроями дублюючої системи оповіщення населення про надзвичайні події у регіоні, передаються до хмарного рівня для оновлення навчального набору даних і для створення наборів зразків для розподілу на пристрої. Це забезпечує поетапне навчання.

Розглянемо ці рівні та їх взаємодію більш детально.

Рівень хмарного сервіси представляє ту частину хмари MaaS, яка використовує наявні хмарні сервіси SaaS (програмне забезпечення як послуга) для проектування та навчання моделей для кожної підмножини кінцевих пристроїв дублюючої системи оповіщення населення про надзвичайні події у регіоні. Сервіс збирає інформацію про випадки атак і аномалій від кінцевих пристроїв-учасників. Дублююча система оповіщення населення про надзвичайні події у регіоні передбачає велику кількість кінцевих пристроїв, що підключені до неї та різняться за своєю структурою та ролями. Останнє створює велике робоче навантаження на хмарний сервіс і вимагає використання великих ресурсів хмарних обчислень, необхідне для підтримки такого сервісу.

Роль MaaS може бути виділена одному або кільком хостам у хмарі. Це залежить від використання вузлів для призначених груп пристроїв і кількості пристроїв, що містяться в цих групах. Таким чином, численні вузли можуть розділяти комплекти обладнання один від одного для балансування навантаження. Хмарні вузли MaaS містять ряд функціональних елементів, показаних на рис. 7.13.

Модуль тестування пристроїв: контролює наявні ресурси (наприклад, пам’ять і центральний процесор) і середню інтенсивність трафіку для моделі IDS, що працює на граничних пристроях. Даний елемент встановлює тестовий агент на вибраний елемент пристрою з кожного набору пристроїв і збирає вимірювання агенту для виконання компонента зважування атрибутів.

Зважування атрибутів – призначає вагу всім значущим ознакам, які беруть участь у побудові моделі (базується на величинах необхідних обчислювальних

ресурсів та вимог до пам’яті). Ці коефіцієнти вказують на необхідну потужність для виявлення ознак на кінцевих пристроях і впливають на модель, створюється. Зважені ознаки спрямовуються в модуль калібрування моделі.

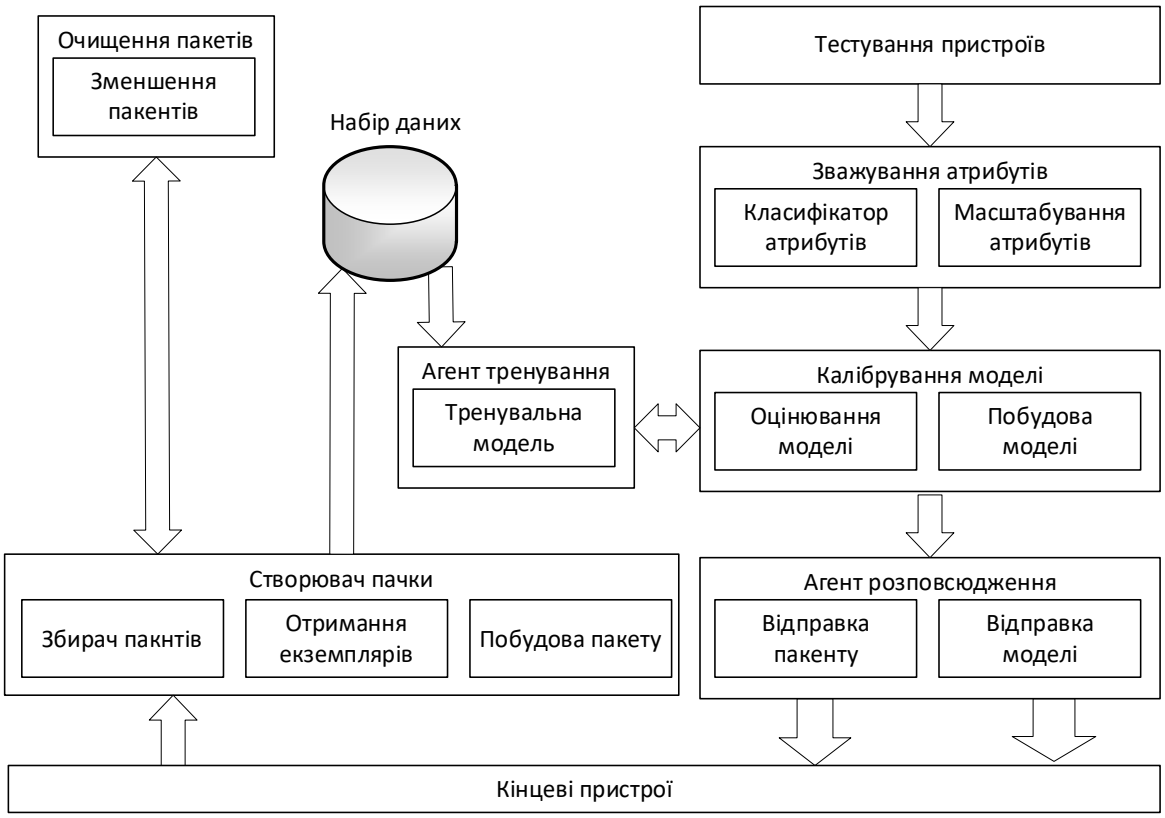


Рисунок 7.13 – Компоненти хмарної IDS

Модуль калібрування: переглядає обмеження моделі, створені для активних ваг критичних властивостей, і може ігнорувати виявлені критичні властивості, які перевантажують відповідні граничні пристрої та ініціюють помилку перевірки пакетів.

Створювач пакетів: - збирає відповідні зразки з пристроїв і об'єднує дані зразки в пакети для додаткового навчання.

Очищення пакетів: налаштуйте створені пакети для кожного визначеного пристрою. Це передбачає видалення вже повідомлених пристрою версій з відповідних пакетів, щоб уникнути дублювання на сторонніх пристроях.

Агент розповсюдження: цей елемент поширює шаблон на пристрої, які беруть участь у певній підмножині пристроїв, коли новий шаблон створюється для цього набору.

Агент тренування: готує нові моделі з відповідним зібраним і модернізованим набором даних, інакше він буде поступово навчати існуючу модель новими пакетами.

На рівні кінцевих пристроїв дублюючої системи оповіщення населення про надзвичайні події у регіоні пристрої групуються в групи з однаковими ролями, програмним та апаратним забезпеченням. Кінцеві пристрої наділений функціями обміну та оновлення параметрів моделі з хмарного сервісу. Модель, завантажена з хмарного сервісу, використовується для виявлення атак і аномалій. Якщо виявлено екземпляр атаки або аномалію трафіку, кінцевий пристрій повідомляє хмарний сервіс.

IDS, який запускається на кінцевих пристроях дублюючої системи оповіщення населення про надзвичайні події у регіоні, містить п’ять основних елементів, які можуть працювати в 2 режимах: на основі потоку або на основі пакетів (рис. 7.14).

Режим на основі потоку передбачає об'єднання пакетів, що передаються в одному напрямку і належать одному з'єднанню або сеансу, в один об'єкт для аналізу. Пакетний режим передбачає по-пакетний аналіз мережного трафіку, на основі якого робиться прогноз будь-яких аномалій у пакеті. Обидва режими вимагають набору навчальних даних, який їх підтримує. Функціональні елементи для обох режимів однакові.

Агент моніторингу: відповідає за перехоплення вхідних пакетів, передачу їх першому елементу аналізатора, генератору ознак, у вигляді окремого пакета або об’єднаних у набори потоків.

Формувач атрибутів – відповідає за вилучення атрибутів з окремих пакетів або наборів потоків і створення так званих «даних екземплярів» для обробки в моделях машинного навчання.

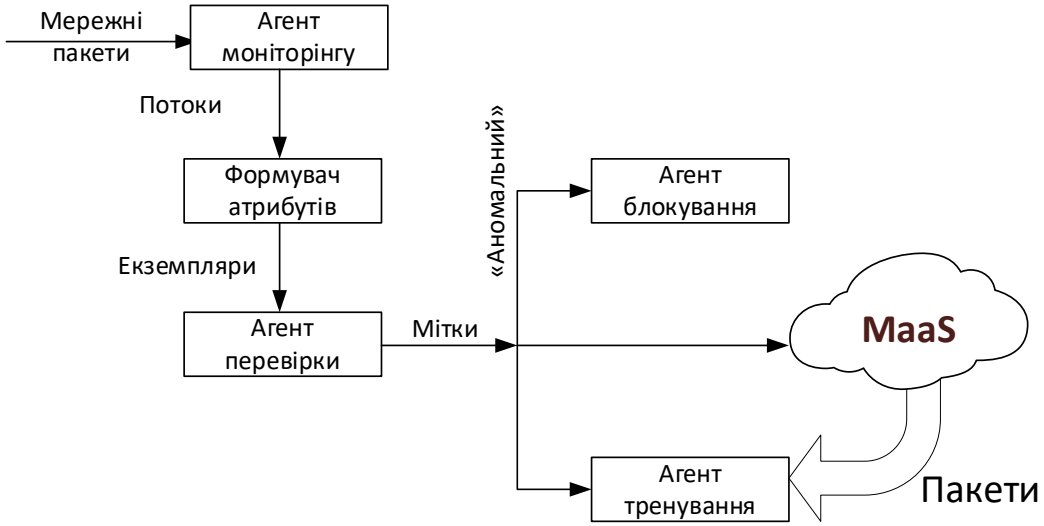


Рисунок 7.14 – IDS компонети кінцевого пристрою системи оповіщення

Агент перевірки – виявляє аномалії, передаючи дані кожного екземпляра до моделі машинного навчання. Коли в пристрої виявлено аномалію, спрацьовує сигнал тривоги, і джерело вхідного пакету/потоку блокується, в то час як пакет (у режимі пакету) скидається. Екземпляр, який ініціював сигнал тривоги, передається на хмарний вузол для обробки та оновлення моделей на інших кінцевих пристроях.

Агент тренування – навчає модель крок за кроком, використовуючи локально знайдені екземпляри, позначені як «аномалії», але спочатку збирає їх у пакети для оновлення моделі, коли пристрій не використовується. Цей агент також отримує позначені пакети екземплярів (крім прикладів, про які повідомляється пристроєм) від хмарного вузла до моделі тренування.

Агент блокування – блокує вхідний трафік із шкідливих джерел. Також можливе відправка брандмауеру повідомлення для відповідних дій або здійснити необхідні дії на самому пристрої.

7.5 Висновки до сьомого розділу

Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак, що базується на хмарному підході машинного навчання є складовою

дублюючої системи оповіщення населення про надзвичайні події у регіоні. Завдяки застосуванню хмарного рішення вдалось розв’язати завдання моніторингу, виявлення вторгнень та ідентифікації мережних атак для кінцевих пристроїв системи з обмеженими ресурсами. Хмарний компонент системи IDS використовується, щоб розвантажити кінцеві пристрої від необхідності виконувати складні обчислення моделі машинного навчання. Кінцеві пристрої отримують оновлену інформацію про параметри IDS від хмарного MaaS. У цьому випадку функції пристроїв нижнього рівня обмежуються виділення ознак мережевого трафіку та виявленням аномалій. Пристрої повідомляють хмарному сервісу про виявлені аномалії та передають їх параметри для аналізу та навчання моделі.

2. Набув подальшого розвитку метод виявлення вторгнень на основі аналізу сигнатур, який враховує дані глибокого аналізу пакетів та рейтингування бази сигнатур.

3. Метод аналізу сигнатур, який використовує глибокий аналіз пакетів для аналізу вмісту трафіка та ідентифікує 93% атак, має низьку кількість хибнопозитивних спрацьовувань (менше 8%).

4. Розроблено комплексний метод виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Це дозволяє підвищити як достовірність, так і точність виявлення вторгнень, та уможливлює раннє виявлення вторгнень в широкому діапазоні кібератак на систему.

5. Проведено порівняльний аналіз роботи комплексного методу, який показав високу точність ідентифікації атак при різній інтенсивності трафіка. Комплексний метод показав більш високу точність ідентифікації атак (більше 98%), на відміну від існуючих. Залежно від необхідного рівня ідентифікації атак можна прискорити роботу комплексного методу шляхом зміни порогових значень виявлення.

8 ОБҐРУНТУВАННЯ НАУКОВО-МЕТОДИЧНИХ РЕКОМЕНДАЦІЙ ЩОДО ПРАКТИЧНОГО ВПРОВАДЖЕННЯ РОЗРОБЛЕНИХ МОДЕЛЕЙ І МЕТОДІВ ЯК ОСНОВИ МАТЕМАТИЧНОГО ТА АЛГОРИТМІЧНО-ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ОНОВЛЕНИХ ПРОТОКОЛІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В СУЧАСНИХ ТА ПЕРСПЕКТИВНИХ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

8.1 Система загальних рекомендації щодо практичного використання запропонованих рішень в інфокомунікаційних мережах

Запропоновані математичні моделі та обчислювальні методи безпечної маршрутизації можуть знайти своє практичне застосування в сучасних та перспективних інфокомунікаційних мережах (ІКМ). Впровадження на практиці розроблених математичних моделей та методів маршрутизації має на меті підвищити ефективність ІКМ з точки зору показників мережної та кібербезпеки, а також, за необхідності, показників якості обслуговування.

Виконання рекомендацій щодо практичної реалізації розроблених моделей та методів спрямоване на створення сприятливих умов їх застосування та пов'язане з необхідністю проведення комплексу важливих організаційно-технічних заходів, що чіпають принципи структурно-топологічної, технологічної та алгоритмічно-програмної реалізації (рис. 8.1).

Рекомендації структурно-топологічного характеру спрямовані на використання сильнозв'язної структури ІКМ, що дозволить підвищити надійність та кіберстійкість мережі з точки зору реалізації багатошляхової маршрутизації з максимальним числом шляхів, які в залежності від використаного методу можуть або перетинатись, або не перетинатись. Від кількості подібних маршрутів, як показали результати дослідження, напряму залежать числові показники мережної безпеки, наприклад, ймовірність компрометації мережі та повідомлень (пакетів), показники якості

обслуговування (продуктивність, середі затримки та рівень втрат), а також показники надійності.

Використання сильнозв’язних топологій ІКМ дозволить мати необхідний канальний та кіберресурс для забезпечення реалізації схем захисту не тільки вузлів та каналів, але й маршрутів взагалі, що сприяє максимальному підвищенню рівня кіберстійкості мережі з точки зору розрахунку та використання множини основних та резервних маршрутів.

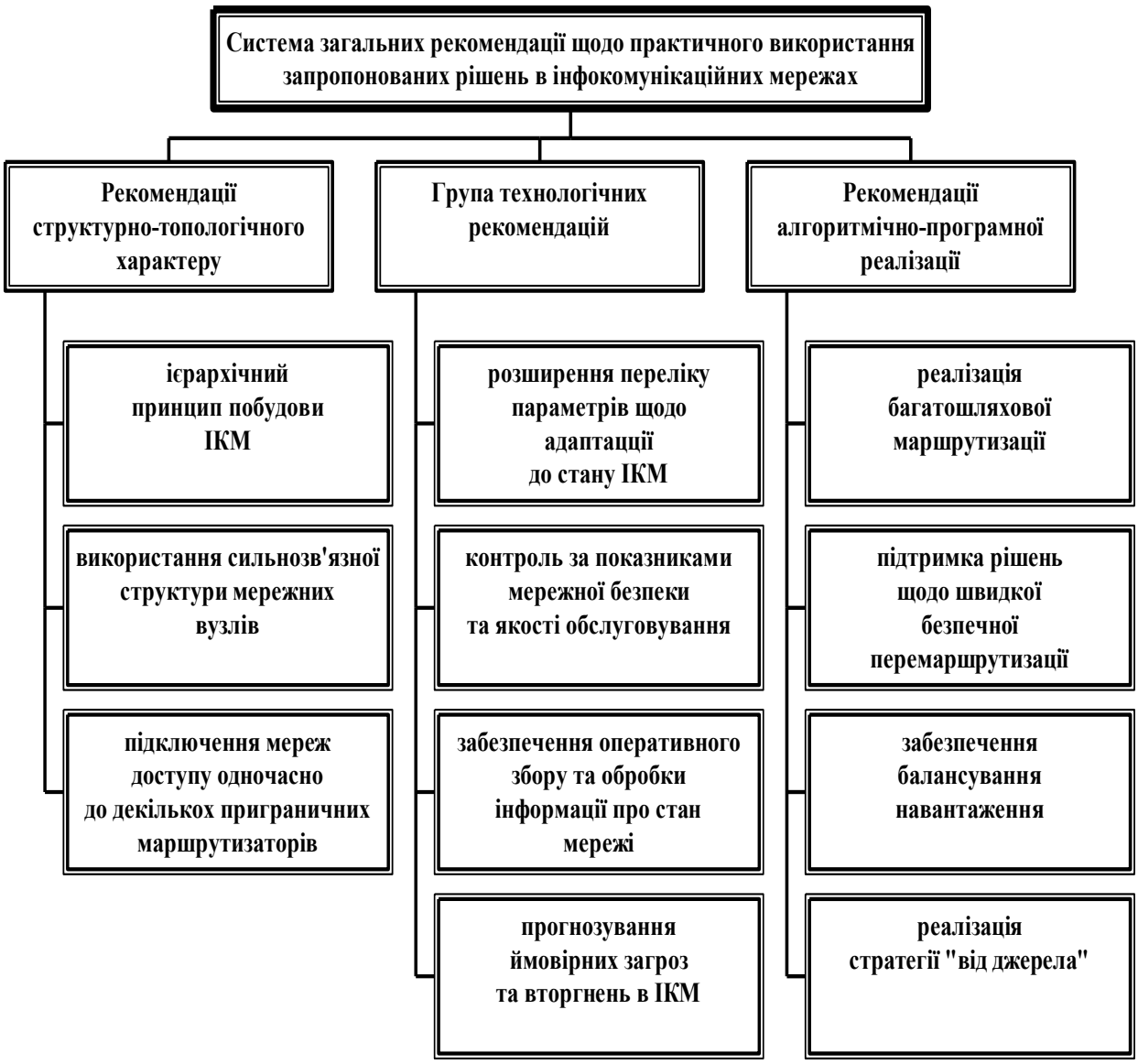


Рисунок 8.1 – Система рекомендацій щодо використання розроблених моделей та методів безпечної маршрутизації в ІКМ

Для забезпечення захисту приграничних маршрутизаторів, працездатність яких може бути порушена з причини перевантаження та/або порушення рівня мережної безпеки (компрометації), мережі доступу мають комутуватись одночасно до декількох подібних маршрутизаторів із балансуванням навантаження між ними та оперативним перемиканням потоків на резервні пристрої при виході з ладу основних.

Загальною вимогою до структури ІКМ є введення функціональної та топологічної ієрархії, що традиційно сприяє підвищенню масштабованості маршрутних рішень та мережі взагалі.

На технологічному рівні РСУ з метою якісного вирішення завдань безпечної маршрутизації має будуватися відповідно до вимог основних концепцій управління мережами, мережними ресурсами та інформаційним трафіком, забезпечення мережної безпеки, викладеними в рекомендаціях ITU-T M.3010 та NIST CVSS, ISO 17799 (BS7799), ISO 15408, COBIT, COSO [141-147]. У зв'язку з цим ІКМ повинна мати ефективні засоби збору, зберігання, обробки та передачі інформації про стан мережі та інформації управління в процесі вирішення задач безпечної маршрутизації. Пріоритетним має стати використання концепції оновлення маршрутів «за вимогою», що сприяє мінімізації службового трафіка та більш оперативному реагуванні на зміну стану мережі.

Система управління мережею має забезпечувати формування та активізацію завдань на збір виміряних значень мережних параметрів та робочих характеристик мережі з обчисленням мінімального та/або максимального значення параметра та/або комбінації значень цих параметрів. При цьому необхідно розширити перелік параметрів, за якими відбувається адаптація до умов функціонування ІКМ, що змінюються, тобто поряд з топологічною інформацією необхідно забезпечувати моніторинг, збір та аналіз даних:

– про номінальну пропускну здатність каналів зв’язку, їх завантаженість, рівень затримок пакетів та їх втрат;

– про рівень мережної безпеки комутаційного обладнання, наявні уразливості, ризики їх використання;

– про сценарії поточних та прогнозованих загроз та вторгнень в ІКМ;

– про характеристики трафіку користувачів що надходить на прикордонні маршрутизатори від мереж доступу або окремих груп абонентів: його інтенсивність, рівень вимог щодо мережної безпеки та якості обслуговування.

Особливості алгоритмічно-програмної реалізації запропонованих моделей та методів безпечної маршрутизації варто зазначити з прив’язкою до основних типів сучасних ІКМ.

8.2 Особливості практичного використання запропонованих рішень щодо безпечної маршрутизації у традиційних IP/MPLS-мережах

В традиційних IP/MPLS-мережах запропоновані моделі та методи мають стати основою математичного та алгоритмічно-програмного забезпечення маршрутизаторів та використовуватись при розрахунку та формуванні маршрутних таблиць. В залежності від топології мережі, її завантаженості та вимог щодо рівня якості обслуговування та мережної безпеки запропоновані рішення можуть базуватись на використанні маршрутних метрик або концепції Traffic Engineering. Для підвищення рівня кіберстійкості ІКМ в межах реалізації реактивного підходу запропоновані моделі та методи можуть бути використані для швидкої безпечної перемаршрутизації із реалізацією схем захисту вузла, каналу або маршруту.

Пріоритетним є використання стратегій маршрутизації «від джерела», коли рішення щодо подальшої маршрутизації приймає приграничний маршрутизатор, а транзитні маршрутизатори звільнені від функції корегування шляхів, що має знизити ймовірність створення петель (циклів). Інформацію про розраховані на приграничному маршрутизаторі безпечні шляхи в межах технології MPLS розповсюджується мережею за допомогою протоколу поширення міток LDP з формуванням і розсилкою відповідних таблиць

просування міток для кожного маршруту, що розраховується вздовж внутрішньодоменних LSR – маршрутизаторів комутації міток. Кінцевий прикордонний LER повинен буде лише зробити збірку пакетів вихідного трафіку, частини якого надійдутьдо нього за множиною розрахованих маршрутів. При цьому використовуючи звичайне хешування потоку CEF, усуваються можливі проблеми, пов'язані з нерівномірністю часу прибуття пакетів.

Окрім окремих особливостей практичної реалізації в IP та MPLS-мережах запропоновані в проєкті моделі та методи безпечної маршрутизації відповідають вимогам сучасних концепцій маршрутизації та управління трафіком – Constraint-Based Routing, QoS-Based Routing, Secure-Based Routing Load-Balance Routing та Traffic Engineering. Для підвищення оперативності реакції на зміни в стані ІКМ доцільно запровадити підтримку стратегії завчасної маршрутизації або маршрутизації з передрозрахунком шляхів – Precomputation Routing (PR). У ході PR на першому кроці завчасно розраховується множина шляхів (основних та резервних), а на другому кроці здійснюється їх вибір та розподіл потоків користувачів по цим шляхах з виділенням кожному з них необхідної пропускної здатності з метою забезпечення заданих показників якості обслуговування та мережної безпеки.

Реалізація переваг концепції PR для транспортних ІКМ дозволить забезпечити

по-перше, високу оперативність реалізації маршрутів, так як мітки створюються і узгоджуються між суміжними вузлами до початку надходження даних від користувача. Тому, якщо необхідний маршрут міститься в таблиці пересилання, йому вже присвоєно мітку, і потік пакетів, що надходить, може бути негайно переданий з цією міткою;

по-друге, високу масштабованість, оскільки кількість помічених маршрутів пропорційна до числа записів у таблиці пересилання, а не числу індивідуальних потоків;

по-третє, значне зменшення обсягу службового трафіку за постійної топології мережі, порівняно з класичною маршрутизацією. Встановлення та перерахунок маркованих маршрутів відбувається тільки при зміні топології мережі або отриманні відповідної інформації, що управляє, а не при надходженні на обслуговування кожного нового трафіку.

Запропонована у проєкті модель швидкої безпечної маршрутизації має на меті доповнити функціонал рішень щодо Faster IGP Convergence, IP Fast ReRouting та MPLS Fast ReRouting на основі більш повного врахування при розрахунку маршрутів характеристик потоків, параметрів мережної безпеки елементів ІКМ та ймовірних загроз, що проєктується на вибір тієї чи іншої схеми захисту, наприклад, найбільш схильного до компрометації вузла, каналу або маршруту взагалі.

Узагальнена архітектура маршрутизатора, який здійснює реалізацію безпечної швидкої перемаршрутизації (S-FRR) відповідно до запропонованої у проєкті моделі, представлено на рис. 8.2. До складу алгоритмічно-програмного забезпечення приграничного маршрутизатора повинен входити блок моніторингу та аналізу рівня мережної безпеки (ймовірності компрометації каналів зв’язку), а також блоку моніторингу топологічних характеристик ІКМ. Саме ці параметри мають аналізуватись блоком формування множини шляхів та блоком розрахунку ймовірності їх компрометації. Проактивний характер рішень обумовлений розрахунком метрик маршрутів, які враховують показники мережної безпеки комунікаційного обладнання.

В рамках запропонованого рішення S-FRR закладено можливість захисту вузла, каналу та шляху в цілому, за що відповідають окремі блоки (рис. 8.2). Далі інформація з цих блоків поступає до блоку оптимізації процесу безпечної швидкої перемаршрутизації. Цей блок відповідає за визначення множини основних і резервних шляхів, за якими передаються потоки пакетів в ІКМ з виконанням умов захисту елементів мережі. У випадку порушення вимог щодо рівня мережної безпеки основного маршруту потік пакетів буле автоматично перемкнуто на попередньо розрахований резервний шлях, який не містить небезпечний елемент мережі,

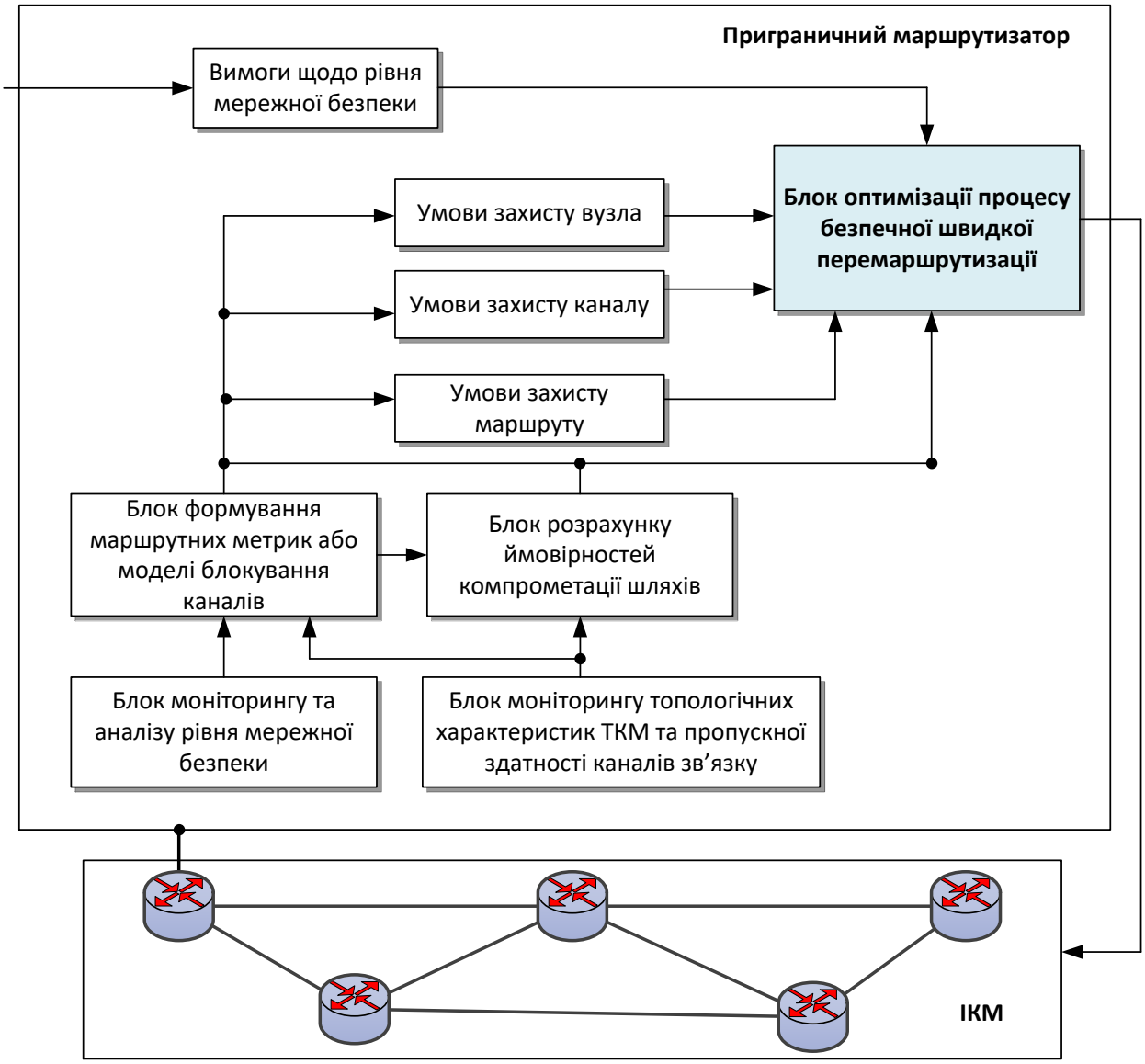


Рисунок 8.2 – Узагальнена архітектура маршрутизатора при реалізації безпечної швидкої перемаршрутизації

8.3 Особливості практичного впровадження запропонованих моделей та методів безпечної маршрутизації у програмно-конфігурованих мережах

Відмінною рисою програмно-конфігурованих мереж є передача більшості функцій щодо управління мережею, в тому числі і функцій розрахунку маршрутів, з маршрутизаторів мережі на SDN-контролери. Це дозволяє підвищити якість управління мережею, знизити вимоги щодо функціональності маршрутизаторів, їх обчислювальної потужності тощо. вартість На рис. 8.3

представлено архітектуру організації безпечної маршрутизації в SDN з централізованим управлінням. На рис. 8.3 виділяється дві функціональні площини: площина даних (інфраструктура ІКМ) та площина управління мережею, основою якої і є SDN-контролер.

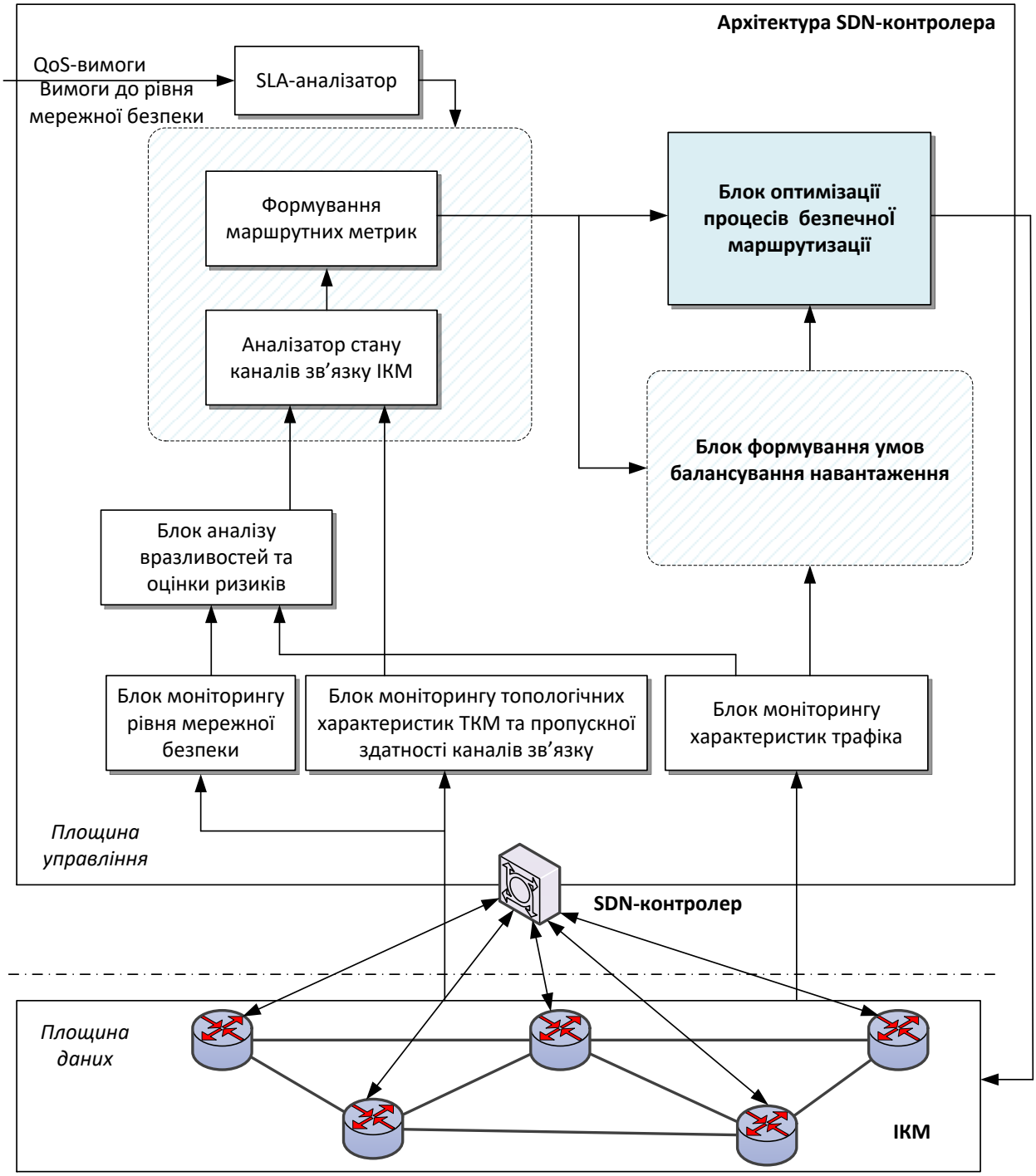


Рисунок 8.3 – Узагальнена архітектура організації безпечної маршрутизації в SDN

В архітектурі SDN-контролера блок SLA-аналізатора відповідає за аналіз - вимог щодо мережної безпеки та якості обслуговування (QoS) у мережі. Блоки моніторингу стану ІКМ – пропускної здатності та ймовірностей компрометації каналів зв'язку, а також характеристик трафіка передають відповідну інформацію на аналізатор стану мережі, де приймається рішення щодо формування маршрутних метрик та/або умов балансування навантаження. Блок оптимізації процесів безпечної маршрутизації здійснює розрахунок безпечних маршрутів. Після цього результати розрахунків, сформовані у вигляді відповідних маршрутних таблиць з SDN-контролера надсилаються у прощину даних, тобто маршрутизаторам ІКМ.

8.4 Особливості практичної реалізації впровадження запропонованих моделей та методів безпечної маршрутизації у мережах MANET

При реалізації запропонованих у межах проєкту моделей та методів безпечної маршрутизації в безпроводових мережах, які самоорганізуються (MANET), рішення можуть стати основою алгоритмічно-програмного забезпечення мережних вузлів, які в залежності від стану мережі виконуються функції термінального пристрою, точки доступу, маршрутизатора та/або сервера послуг. Запропоновані рішення в MANET можуть використовуватись як для безпечної маршрутизації трафіка користувачі, так і для передачі конфіденційних даних і секретів (ключів).

В MANET при використанні безпроводових технологій виникають додаткові ризики, пов'язані із компрометацією не тільки комунікаційного обладнання, але й радіоканалів. Тому особливо актуальним є завдання щодо адаптації ідей та принципів базового механізму SPREAD та запропонованих у проєкті його модифікацій в MANET, коли конфіденційні повідомлення передаються окремими фрагментами за множиною розрахованих найбільш безпечних шляхів, які можуть не перетинатись (оригінальна версія SPREAD), або є перетинатись (версія, що є розвитком SPREAD).

Загальна функціональна архітектура приграничного маршрутизатора MANET при організації безпечної маршрутизації конфіденційних повідомлень,

в основу якої покладено модифікований механізм SPREAD, запропонований у проєкті, представлено на рис. 8.4. Як і в MPLS-мережах за розрахунок маршрутів з попередньою реалізацією схеми Шаміра має відповідати лише приграничний вузол-маршрутизатор, який, аналізуючи стан мережі з точки зору ймовірних загроз та сигнально-завадової обстановки, також визначає тип реалізованої схеми – із надмірністю чи без неї, з обґрунтуванням параметрів (T, N). Транзитні вузли мають лише комутувати фрагменти конфіденційного повідомлення за попередньо розрахованому маршруту, що значно знижує вимоги до їх обчислювальної потужності.

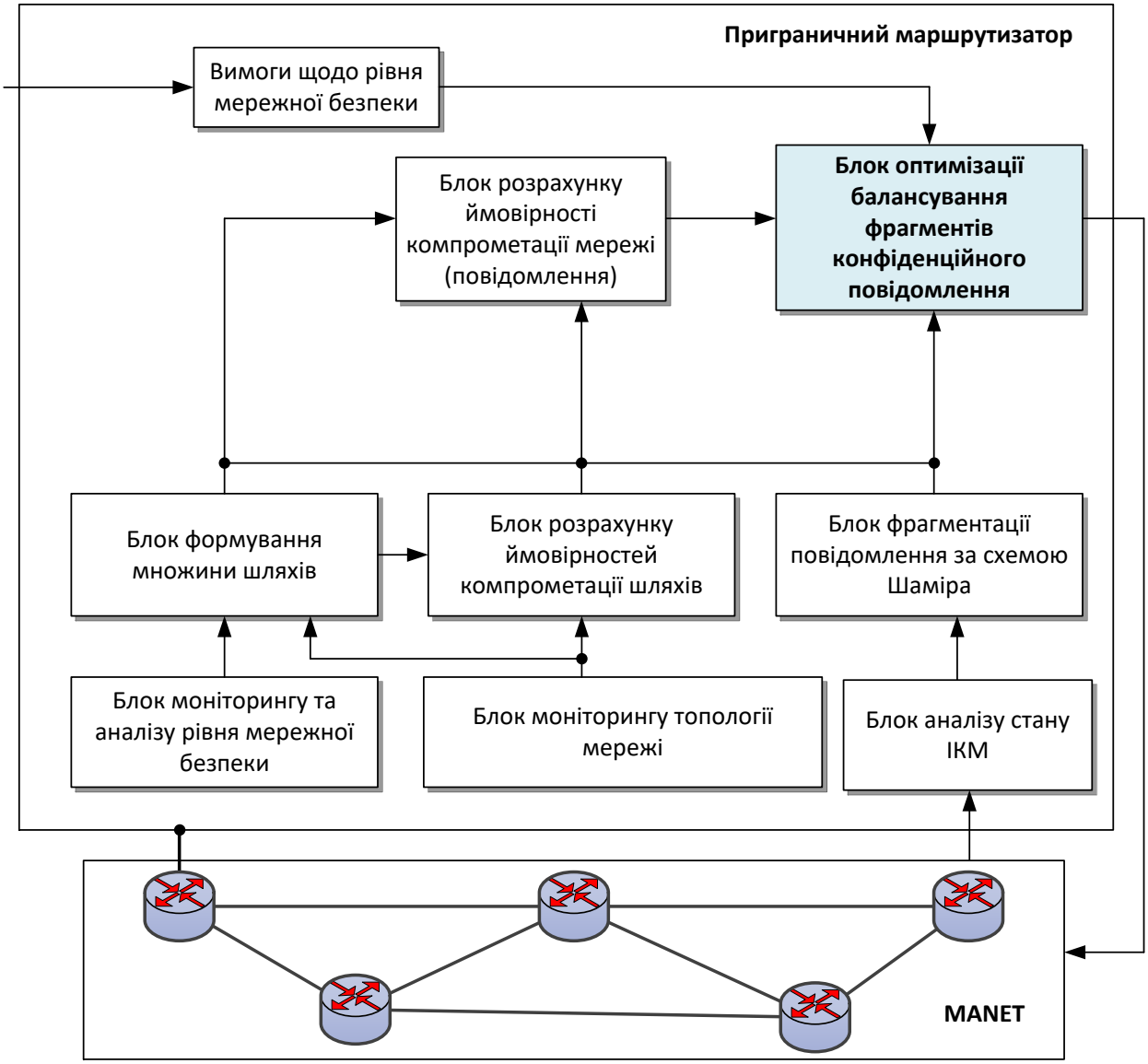


Рисунок 8.4 – Узагальнена архітектура маршрутизатора MANET при реалізації безпечної маршрутизації

8.5 Висновки до восьмого розділу

1. Розроблено рекомендації щодо практичної реалізації результатів проєкту, які стосуються впровадження запропонованих моделей та методів безпечної маршрутизації в ІКМ. Рекомендації базуються на результатах дослідження запропонованих рішень. Виконання рекомендацій передбачає проведення комплексу організаційно-технічних заходів, спрямованих на забезпечення ефективного функціонування ІКМ на основі запропонованих принципів структурно-топологічної, технологічної та алгоритмічно-програмної реалізації.

2. Запропоновані математичні моделі та обчислювальні методи безпечної маршрутизації можуть знайти своє практичне застосування в сучасних та перспективних інфокомунікаційних мережах (ІКМ). В традиційних IP/MPLS-мережах запропоновані моделі та методи мають стати основою математичного та алгоритмічно-програмного забезпечення маршрутизаторів та використовуватись при розрахунку та формуванні маршрутних таблиць. В залежності від топології мережі, її завантаженості та вимог щодо рівня якості обслуговування та мережної безпеки запропоновані рішення можуть базуватись на використанні маршрутних метрик, концепції Traffic Engineering. Для підвищення рівня кіберстійкості ІКМ в межах реалізації реактивного підходу запропоновані моделі та методи можуть бути використані для швидкої безпечної перемаршрутизації із реалізацією схем захисту вузла, каналу або маршруту.

3. При реалізації запропонованих рішень в програмно-конфігурованих мережах розроблені моделі та методи безпечної маршрутизації можуть стати основою алгоритмічно-програмного забезпечення SDN-контролерів, які здійснюють управління інформаційним обміном в межах певного мережного сегмента або домену.

4. При реалізації запропонованих у межах проєкту моделей та методів безпечної маршрутизації в безпроводових мережах, які самоорганізуються (MANET), рішення можуть стати основою алгоритмічно-програмного

забезпечення мережних вузлів, які в залежності від стану мережі виконуються функції термінального пристрою, точки доступу, маршрутизатора та/або сервера послуг. Запропоновані рішення в MANET можуть використовуватись як для безпечної маршрутизації трафіка користувачі, так і для передачі конфіденційних даних і секретів.

ВИСНОВКИ

Висновки за етапом № 1 (2020 року)

Опис наукових та науково-технічних результатів, отриманих в рамках виконання Проєкту (за окремими індикаторами виконання завдань).

1. Нові науково обґрунтовані знання з актуальних проблем побудови та впровадження моделей, методів та протоколів моніторингових систем запобігання поширення інфекційних захворювань в умовах децентралізованої взаємодії.

Розглянуто всі існуючі на сьогоднішній день способи та механізми, які використовуються у криптовалютних блокчейнах для забезпечення анонімності користувачів. Детально описано та ретельно проаналізовано кожен з цих способів та механізмів, виконано їх порівняльний аналіз. Визначено, які з них найбільше підходять для збереження конфіденційності певної приватної персональної інформації.

Проаналізовано способи та криптографічні примітиви, які застосовуються у блокчейн-технологіях таких найкрупніший за ринковою капіталізацією та "найприватніших" цифрових валют як Monero, Dash та ZCash. Крім того, саме ці криптовалюти є об’єктами пильної уваги та заборони багатьох спецслужб та фінансових організацій у світі. Ця увага свідчить про те, що вони дійсно є анонімними. При цьому тільки криптовалюта Monero є анонімною безумовно, а криптовалюти Dash та ZCash лише допускають вибір опції анонімності за бажанням користувача. Слід зазначити, що питання можливості використання цих валют, а також інших платіжних засобів для анонімного фінансування осіб у різних країнах суттєво залежить від того, про яку саме країну йдеться. В першу чергу це визначається законодавчою базою країни стосовно криптовалют взагалі та анонімних криптовалют зокрема. Тому остаточні висновки можна робити після вивчення законодавства конкретної країни або після вивчення справ, які, можливо, розглядались у судах цієї країни та які рішення по них були прийняті. Підводячи підсумки вивчення питання анонімного фінансування, можна

рекомендувати використання будь-якої анонімної валюти, такої як Monero, Dash або zCash (останні дві – з включеною опцією анонімності).

За результатами аналізу показано, як отримана інформація може бути використана при створенні мережі, яка буде функціонувати на основі блокчейну та зберігати, обробляти та передавати конфіденційну інформацію, ззбезпечуючи при цьому її анонімність. Відмічено, що використання так званих міксерів, на зразок тих, що використовує BTC або Dash, не є можливим при обробці інформації, оскільки персональну інформацію не можна розбити на меленькі частинки, на зразок монеток, та перемішувати однакові, оскільки персональна інформація є дуже особистою. Далі, використання різних специфічних платіжних систем, а також криптоматів, теж не вирішить це питання, оскільки обробка персональної інформації, її пересилання та отримання, внаслідок її специфічності та персоніфікованості, ніяк не можна порівнювати з обробкою та отриманням безособових криптовалют. Крім того, при обробці персональної інформації потрібно забезпечити різні рівні доступу до неї (наприклад, у користувача – повний доступ до його персональної інформації, у його лікарів – відповідно до спеціалізації, у роботодавця – довідка про дозволи та обмеження, які визначаються станом здоров’я кандидата на посаду, і т.д.).

Зроблено висновок, що для забезпечення заданого рівня анонімності при обробці, зберіганні, пересиланні та отриманні конфіденційної персональної інформації, можливо використовувати лише відповідний математичний апарат, на зразок кільцевих підписів (на зразок Monero) або SNARKів, на зразок zCash. Основна перевага таких способів забезпечення анонімності полягає у тому, що:

– математичний апарат, який застосовується на зазначених платформах для забезпечення анонімності, є повністю математично обґрунтованим та достатньо апробованим, що забезпечує достатній рівень довіри до нього;

– цей апарат тестувався та вдосконалювався протягом майже 10 років, в результаті чого підвищилась прозорість та зручність його використання;

– існує численна кількість наукових робіт, які пояснюють принципи роботи цього математичного апарату та обґрунтовує його стійкість, при цьому все

наукове та програмне забезпечення є повністю відкритим, та постійно обговорюється на різних форумах;

– інформація, яку можна обробляти з використанням цього математичного апарату, може бути будь-якою та мати довільну структуру, без якихось обмежень, внаслідок універсальності апарату;

– для забезпечення неможливості підміни інформації, не потрібно на локальних пристроях зберігати всю інформацію з усіма її перетвореннями, а достатньо зберігати лише останній варіант разом з доведенням коректності переходу між попередніми станами;

– саме доведення коректності переходу між станами є відносно коротким, його довжина не залежить від кількості інформації, яку воно підтверджує, тобто із зростанням кількості інформації об’єм пам’яті, необхідний для її захисту від підробки, не змінюється.

Розглянуто математичний апарат, необхідний для побудови доведення без розголошення знання певної інформації – так звані SNARK-доведення. На прикладі найбільш поширеного протоколу GRO-16 показано, як структурується інформація перед побудовою SNARK-доведення, як виконуються попередні обчислення (так звана церемонія, або Setup), як будується саме доведення та як перевіряється його коректність. Також показано, як будувати рекурсивні SNARK-доведення та для чого і в яких ситуаціях вони є необхідними. Крім того, були проаналізовані загрози, які виникають при некоректному використанні або некоректній побудові SNARK-доведення, та на що треба звернути увагу, щоб мінімізувати ці загрози.

Проведено аналіз, дослідження та обґрунтування можливості застосування різних інформаційних технологій (наприклад, Bluetooth, Wi-Fi, GPS, тощо) у засобах відстеження контактів як основної підсистеми глобального моніторингу населення. Зокрема, досліджено принципи побудови та можливості застосовування зазначених технологій для відстеження контактів, проаналізовано їх переваги та недоліки, потенційні атаки на додатки моніторингу, тощо. Проаналізувавши інформацію, що стосується реалізації

світових додатків, а також принципів функціонування типових протоколів для додатків відстеження контактів, варто відзначити декілька важливих висновків.

– для коректного функціонування додатків усі, без виключення, додатки використовують підключення до інтернету, зокрема Wi-Fi. Це пояснюється тим, що є необхідним передача анонімних ідентифікаторів до центрального серверу для подальшого аналізу та повідомлення потенційно заражених користувачів у випадку централізованої системи. У свою чергу у випадку децентралізованого підходу підключення до інтернету є необхідним для завантаження з центрального серверу ідентифікаторів захворівших людей та локального аналізу списку своїх контактів з метою виявлення контактів із зараженим. Також додаток StayHomeSafe використовує аналіз підключення пристрою до мереж Wi-Fi задля моніторингу ізоляції захворюваних;

– світова практика доводить, що більш ефективним є використання технології Bluetooth для обміну анонімними ідентифікаторами між користувачами. Зокрема використовується Bluetooth з низькою енергію, що дозволяє зменшити енерговживання та запобігти нераціональне використання живлення пристрою, а як наслідок зменшити негативне ставлення населення до функціонування додатків на їх пристроях.

– на даний момент, з використанням тільки технології GPS не працює жоден додаток. GPS використовується як додаткова функція для додатків з використанням Bluetooth з метою побудови карт місцевості із зазначенням районів захворювання, а також моніторингу ізоляції захворюваних. Відсутність додатків із використанням тільки технології GPS пояснюється тим, що технологія GPS не дозволяє коректно фіксувати місцезнаходження пристрою у всіх випадках. Наприклад, низькою є точність у рухомих та підземних середовищах, а також обмежена вертикальна точність, коли більшість мешканців або працівників однієї багатоповерхівки фіксуються у межах помилки, що особливо актуально в міських умовах та може призвести до помилкової підозри захворювання.

2. Моделі загроз, порушника та безпеки моніторингових систем відстеження контактів, деперсоналізації даних та побудови мережі в умовах децентралізованого середовища.

Проведено аналіз та дослідження моделей загроз, порушника та безпеки моніторингових систем відстеження контактів, деперсоналізації даних та побудови мережі в умовах децентралізованого середовища. За результатами досліджень встановлено переваги децентралізованих систем типу блокчейн, зокрема:

– блокчейн є однією з найпривабливіших моделей децентралізованого середовища, яке можна застосовувати для збереження, обробки та пересилання інформації, забезпечуючи при цьому максимальний рівень її деперсоналізації;

– отримані результати свідчать про надзвичайну роль криптології для забезпечення "життєдіяльності та життєздатності" децентралізованого середовища. Дійсно, сам блокчейн, як технологія, базується на таких криптографічних механізмах, як цифровий підпис та функція гешування. Ці криптографічні перетворення можна вважати базовими, оскільки вони забезпечують коректне функціонування будь-якого блокчейну, незалежно від його специфіки, додаткових властивостей та призначення.

Досліджено моделі порушника та відповідних атак, які спрямовано на застосовувані криптографічні перетворення. Встановлено, що досліджені криптографічні атаки залишаються загрозами для будь-якого блокчейну. Оскільки геш-функції та цифровий підпис використовуються у криптології вже не одне десятиріччя, то багато з таких моделей загроз є добре вивченими та дослідженими, при цьому описані та строго обґрунтовані необхідні та достатні умови успіху різних атак, розроблені методи оцінювання стійкості та побудови заздалегідь стійких криптографічних механізмів.

Досліджено та вивчено властивості нових типів атак, які виникли тільки після появи технології блокчейну, проаналізовано та досліджено різні способи захисту від них. Ці атаки направлені саме на спосіб функціонування блокчейну і не є атаками на криптографічні механізми, які його обслуговують. Деякі з атак

на блокчейн є загальними, тобто основну їх ідею можна застосовувати до будь-якого блокчейну, незалежно від протоколу консенсусу, який у ньому використовується. Інші атаки є спеціальними атаками, тобто суттєво залежать саме від типу протоколу консенсусу.

Досліджено та вивчено дві моделі загальних атак на блокчейн, оскільки, на відміну від атак на різні криптографічні примітиви, вони досліджені набагато менше. Крім огляду та порівняльного аналізу цих атак, також наведені основні способи протидії цим атакам, які суттєво використовують особливості функціонування та обслуговування блокчейну.

3. Обґрунтовані напрямки застосування криптографічних примітивів та протоколів взаємодії у децентралізованому середовищі.

Проведено аналіз сучасних методів та механізмів досягнення послуг безпеки – конфіденційності, цілісності, доступності, неспростовності, як користувачів децентралізованої системи, так й елементів/вузлів децентралізованої системи. Обґрунтовано перспективні напрямки застосування криптографічних примітивів та протоколів взаємодії у децентралізованому середовищі. За результатами дослідження встановлено наступне:

– відкритість транзакцій в децентралізованих системах, з одного боку, є плюсом для спільноти, а з іншого – з'являються ризики розкриття адреси суб'єкта, ідентифікувати особистість суб’єкта. Аналіз існуючих децентралізованих систем дозволяє зробити висновок, що на основі ланцюжка блоків можна ідентифікувати приналежність деяких адрес конкретним суб'єктам. Тому для здійснення транзакції в системі оптимальним є використання мультипідпису або смартконтрактів, гомоморфного шифрування, криптопротоколів для приховання персональної інформації суб’єкта без необхідності;

– протоколи доказу з нульовим розголошенням можна використовувати у протоколах конфіденційного обчислення, які дозволять деяким учасникам стверджувати, що інша сторона веде себе чесно;

– схема кільцевої підпису може забезпечити анонімність суб’єкту, що підписує, а також його незалежність від інших учасників, і при цьому забезпечити цілісність і автентичність відбитку, яким підписується повідомлення.

– гомоморфна властивість криптосистем може бути використана для створення безпечних систем голосування, хеш-функцій, стійких до колізії, закритої інформації пошукових систем та зробить широке розповсюдження публічних хмарних обчислень, гарантуючи конфіденційність даних, що оброблюються.

4. Нові науково обґрунтовані положення до теорії інформаційної та мережної безпеки, що представлені розробленими в проєкті моделями та методами моніторингу, виявлення вторгнень та ідентифікації мережних атак.

Проведено аналіз існуючих рішень в області моніторингу, швидкого та раннього виявлення вторгнень та ідентифікації мережних атак, виявлення фактів несанкціонованого доступу. Результати аналізу показали, що існуючі моделі та методи виявлення вторгнень в більшості направленні на виявлення інтенсивних атак, не враховують безпечність ресурсів комп’ютерних систем та властивості інформаційних потоків. Тобто, існують накладені обмеження на множину виявлених аномалій та структуру інформаційного потоку. Це обмежує можливість своєчасно виявити аномалії в комп’ютерних системах та інформаційних потоках. Новітні рішення в області моніторингу та виявлення вторгнень мають враховувати самоподібні та статистичні характеристики трафіку, глибокий аналіз пакетів та час, необхідний для обробки інформації.

Запропоновано метод виявлення вторгнень на основі аналізу ентропії пакетів. Новизною методу є розрахунок умовної ентропії та врахування статистичних характеристиках даних пакетів. Метод містить два етапи: вивчення базового розподілу та виявленні аномалій в спостережуваному трафіку. Запропонований метод був протестований на наборі реальних даних трафіку, в якому вимірювались статистичні властивості обраних полів в заголовках пакетів. Результати експерименту показали ефективність запропонованого методу

аналізу ентропії пакетів, щодо виявлення атак та ідентифікації їхнього типу, та показав високі значення точності виявлення атак і низькі помилковопозитивні значення.

Запропоновано метод виявлення вторгнень на основі аналізу сигнатур. Новизною методу є врахування даних глибокого аналізу пакетів та рейтингування бази сигнатур. Метод використовує глибоку перевірку пакетів в СВВ, в якій з'єднання між трафіком і сигнатурою аналізується з використанням розрахункового часу обслуговування пакетів. Метод аналізу сигнатур використовує різний час обробки в залежності від довжини пакета, специфікацій системи і кількості правил, визначених у системі і в першу чергу порівнює з найчастіше застосованими сигнатурами атак, що скорочує час обробки пакетів. Результати експериментів показали ефективність запропонованого методу, високі значення точності виявлення атак і низькі хибнопозитивні значення для різних типів атак.

Проведено аналіз існуючих моделей та методів моніторингу, обробки та аналізу трафіку в мережних системах виявлення вторгнень. Проведено аналіз властивостей трафіку та даних, що збираються на вузлах та в мережі. На основі проведеного аналізу обрано параметри трафіку, які буде використано в якості ознак для виявлення вторгнень.

5. Формування набору науково обґрунтованих ознак поведінки мережі та користувачів для їх використання в процесі раннього виявлення вторгнень та ідентифікації мережних атак засобами машинного навчання.

Проведено аналіз методів управління трафіком і системи виявлення вторгнень, який показав що вони належать важливій проблемі забезпечення мережної безпеки. Однією за задач якої є аналіз трафіку і стану мережі при використанні системи виявлення вторгнень шляхом розвитку засобів DPI / DCI. Проведено аналіз методів та критеріїв вибору ознак поведінки мережі для моніторингу, виявлення вторгнень та ідентифікації мережних атак. На основі проведеного аналізу обрано ознаки для перевірки ефективності розроблених методів моніторингу, виявлення вторгнень та ідентифікації атак.

Узагальнено методологію побудови, аналізу та застосування новітніх систем виявлення вторгнень, які можна розділити на два основних типи систем: на основі сигнатур і аномалій:

– системи виявлення вторгнень на основі аномалій створюють профіль, відстежуючи нормальну активність в системі. Цей профіль використовується, щоб знайти відхилення спостережуваних дій від нормальної поведінки системи і повідомити про них як про аномалії. У системах такого типу дуже важливо правильно визначити нормальний профіль системи в автономному режимі або в режимі онлайн;

– у системах виявлення вторгнень на основі статистичних даних здійснюється підтримка двох профілей для нормальної і поточної поведінки системи або мережі. У кожному з цих профілів поведінка системи моделюється шляхом розрахунку деяких статистичних показників, таких як середнє значення, стандартне відхилення, розподіл даних і т. ін.;

– у системах виявлення вторгнень на основі машинного навчання, система намагається вивчити шаблони даних і побудувати модель для класифікації аналізованих моделей. За результатами досліджень запропоновано використовувати низку кількісних характеристик рекурентних діаграм як ознак для класифікації часових рядів за допомогою машинного навчання.

6. Критерії та показники ефективності механізмів криптографічного захисту персональних даних користувачів та протоколів взаємодії, що забезпечують: оперативність; об'єктивність прийняття рішення; деперсоналізацію; узагальнену обробку, достовірності, доступності децентралізованого зберігання.

Проведено обґрунтування критеріїв та показників ефективності механізмів криптографічного захисту персональних даних користувачів та протоколів взаємодії, зокрема обґрунтування критеріїв та показників оперативності та об’єктивісті прийняття рішення; деперсоналізації; узагальненої обробки, достовірності, доступності децентралізованого зберігання, тощо. Узагальненим критерієм ефективності системи відстеженні контактів слід рахувати мінімум

кількості інфікованих, що приходяться на добу. Очевидно, що розглянуті критерії дозволять вирішити задачу збору інформації про стан захворюваності в найбільш об'єктивному вигляді. Зв'язок цього критерію з викладеними у розділі підлягає подальшому вивченню.

На основі досліджень проаналізовано та узагальнено критерії та показники ефективності механізмів криптографічного захисту персональних даних користувачів та протоколів взаємодії, що забезпечують: оперативність; об'єктивність прийняття рішення; деперсоналізацію; узагальнену обробку, достовірності, доступності децентралізованого зберігання. Зокрема, сформульовані критерії та показники для оцінки захищеності симетричних, та асиметричних перетворень, зокрема запропоновано використовувати ці критерії та показники для порівняльного аналізу різних методів криптографічної обробки персональних даних, які можуть бути вжиті в системі. Вони дозволяють оцінити механізми криптографічного захисту персональних даних користувачів та протоколів взаємодії, обґрунтовано використовуючи систему безумовних та умовних критеріїв.

7. Методика оцінки та порівняльних досліджень криптографічних примітивів та протоколів взаємодії в моніторингових системах запобігання поширенню інфекційних захворювань.

Розроблено та досліджено методики оцінки та порівняльних досліджень криптографічних примітивів та протоколів взаємодії в моніторингових системах запобігання поширенню інфекційних захворювань. Показано, що для коректного функціонування моніторингових систем, необхідним є комплексне застосування криптографічних механізмів таких, як блокові симетричні шифри, функції гешування, схеми електронного цифрового підпису, потокових шифрів та генераторів псевдовипадкових послідовностей:

– блокові симетричні шифри мають відповідати наступним показникам: високий рівень криптографічної стійкості, швидкодія та простота програмної і програмно-апаратної реалізації;

– функції гешування мають забезпечувати швидкість перетворення, оптимальний об’єм ключових даних, бути стійкими до першого прообразу, до другого прообразу, а також до мають забезпечувати стійкість до колізій.

– схеми електронного цифрового підпису має забезпечувати швидкодію з точки зору генерації параметрів та ключів, підписанні і перевірки підпису, об'єму ключових даних та результуючого підпису, а також мати надійну математичну базу та забезпечувати захист від відомих і потенційних атак;

– потокові шифри мають бути порівняні згідно довжини коротких пакетів, довгих пакетів, а також згідно критерію ініціалізації ключових параметрів. У випадку використання потокових шифрів у режимі генерації псевдовипадкових послідовностей та безпосередньо генераторів псевдовипадкових послідовностей, для визначення ефективності механізму, отримані послідовності мають бути досліджені щодо їх статистичних властивостей згідно описаної методики з використанням пакету статистичних тестів NIST STS.

За результатами досліджень отримані та строго обґрунтовані оцінки стійкості блокового алгоритму шифрування HadesMiMC та геш-функції Poseidon до лінійних та різницевих атак. Зазначимо, що побудова таких оцінок, особливо до лінійного криптоаналізу, вимагала доведення нетривіальних тверджень про властивості адитивних характерів скінченного поля:

– визначено конкретні параметри для алгоритму шифрування HadesMiMC та геш-функції Poseidon, які дозволяють їх застосовувати для рекурентних SNARK-доведень, що базуються на триплетах mnt-4 та mnt-6;

– показано, як краще обирати S-блоки для цих алгоритмів, щоб цей вибір був оптимальним і з точки зору стійкості, і з точки зору складності обчислень у SNARK-доведеннях;

– показано, яка кількість раундів є достатньою, щоб гарантувати стійкість алгоритмів при різних варіантах вибору параметрів.

– обчислено кількість констрейнтів на біт, для різних варіантів вибору параметрів, та показано, що вона є суттєво меншою, ніж для функції Педерсена, яка зараз використовується у криптовалюті ZCash.

8. Результати порівняльних досліджень та оцінки ефективності криптографічних примітивів та протоколів взаємодії, що потенційно можуть застосовуватись у моніторингових системах запобігання поширенню інфекційних захворювань.

Проведено порівняльні дослідження та оцінка ефективності криптографічних примітивів та протоколів взаємодії, що потенційно можуть застосовуватись у моніторингових системах запобігання поширенню інфекційних захворювань.

Розглянуто функціонування інформації, отриманої у моніторингових системах, у децентралізованому середовищі. Використання саме децентралізованого середовища дає незаперечні переваги, оскільки воно створює набагато більше можливостей для забезпечення об’єктивності у питаннях зберігання, обробки та передавання інформації різних типів, особливо персональних даних.

Досліджено та вивчено можливість переходу з блокчейну на більш загальну структуру, яка має додаткові можливості, але при цьому залишається стійкою до основних атак. В основному в якості нової структури розглядається блокграф (DAG), який має ті чи інші особливості. Пропонуються різні шляхи таких узагальнень та частковий аналіз їх властивостей:

– проаналізовано та досліджено низку протоколів консенсусу на блокграфах. Слід зазначити, що використання таких протоколів, хоч і призводить о значного збільшення швидкості обробки транзакцій, проте несе у собі певні ризики. На даний час для жодного з таких протоколів немає строгих доведень стійкості до основних атак, таких як атака подвійної витрати, атака розщеплення мережі, тощо. Побудова таких доведень вимагає подолання великих аналітичних складнощів, навіть якщо використовувати дуже спрощену математичну модель мережі;

– побудовано верхні оцінки для імовірності атаки подвійної витрати на протокол консенсусу SPECTRE. Для збільшення його захищеності запропоновано дещо нестандартний алгоритм прийняття транзакції вендором:

він повинен чекати, щоб певна кількість блоків підтвердження була створена, так би мовити, під його наглядом;

– наведено строго обґрунтовані формули для обчислення верхніх оцінок такої імовірності в залежності від параметрів мережі та кількості блоків підтвердження, які вендор має побачити до того, як вважатиме транзакцію незворотною. Для більшої наочності, також наведені відповідні чисельні результати.

9. Результати аналізу сучасного стану та дослідження існуючих рішень в області забезпечення мережної безпеки. Обґрунтовані напрямки розвитку та вдосконалення рішень щодо забезпечення мережної безпеки засобами управління трафіком та маршрутизації.

Проведено аналіз існуючих рішень в області забезпечення мережної безпеки та методів управління трафіком. Результати аналізу показали, що перспективними напрямками розвитку та вдосконалення рішень щодо забезпечення мережної безпеки є вдосконалення засобів управління трафіком та маршрутизації. Новітні рішення в області управління трафіком та маршрутизації мають враховувати не тільки параметри мережної продуктивності (пропускну здатність, затримки та рівень втрат пакетів), але й параметри мережної безпеки, що характеризують ефективність роботи задіяних в мережі систем виявлення вторгнень та аналізу вразливостей та ризиків.

Розроблено потокову модель безпечної маршрутизації з балансуванням навантаження відповідно до концепції Traffic Engineering. Новизною моделі є модифікація умов балансування навантаження, в яких крім пропускної здатності (показника якості обслуговування) також враховується ймовірність його компрометації (показник мережної безпеки). В межах цієї моделі задачу безпечної маршрутизації було представлено оптимізаційній формі, що дозволяє ефективно використати в процесі маршрутизації доступний мережний (канальний та буферний) ресурс. У процесі дослідження проаналізовано ряд варіантів формалізації рівня впливу ймовірності компрометації каналів на процес балансування навантаження. Запропоновано рекомендації щодо

використання запропонованої моделі безпечної маршрутизації для різних вихідних даних щодо загроз мережній безпеці. В ході порівняльного аналізу отриманих результатів встановлено, що в процесі балансування навантаження більш інтенсивніше завантажуються канали з меншою ймовірністю компрометації, розвантажуючи більш небезпечні з точки зору компрометації канали зв’язку.

Запропонована математична модель безпечної швидкої перемаршрутизації із захистом структурних елементів структурної мережі (каналу/вузла/маршруту) та її пропускної здатності. Новизною моделі є реалізація реактивного підходу до забезпечення мережної безпеки в мережі, коли при ймовірній компрометації елементу мережі всі потоки пакетів швидко перемикаються на попередньо розраховані резервні шляхи, які не проходять через скомпрометований вузол або канал. В рамках цієї моделі проблема безпечної швидкої перемаршрутизації сформульована у оптимізаційній формі. Модель налаштована на обчислення шляхів, що містять канали зв'язку з мінімальними значеннями ймовірності компрометації, що досягається використанням відповідних вагових коефіцієнтів (метрик) у цільовій функції, значення якої підлягало мінімізації. На числовому прикладі підтверджено адекватність та ефективність запропонованої моделі з точки зору реалізації обраних схем захисту (резервування).

Проведено аналіз існуючих моделей та методів моніторингу, обробки та аналізу трафіку в мережних системах виявлення вторгнень. Проведено аналіз властивостей трафіку та даних, що збираються на вузлах та в мережі. На основі проведеного аналізу обрано параметри трафіку, які буде використано в якості ознак для виявлення вторгнень.

Запропоновано модель системи виявлення вторгнень, яка враховує характеристики трафіка, правила його моніторинга, реагування на вторгнення та обробки, обмеження на параметри якості обслуговування. Модель налаштована на прискорення обробки трафіку в системах виявлення вторгнень та динамічний розподіл самоподібних інформаційних потоків навантаження між окремими датчиками. Новизною моделі є розрахунок середнього часу обслуговування

систем виявлення вторгнень з конфігурацією правил, для успішного визначення дозволу / заборони реагування на певний тип вторгнення. У порівнянні з моделями систем виявлення вторгнень для балансування навантаження на основі прийому пакетів, які зазвичай використовуються, модель, що використовує час обслуговування, збільшує кількість прийнятих і оброблюваних пакетів багатоядерними системами виявлення вторгнень, а також зменшує кількість пакетів, що відкидаються.

Обґрунтування переваг науково-технічної продукції у порівнянні з існуючими аналогами.

1. Запропоновано та досліджено новий протокол консенсусу, проведено його попередній аналіз стосовно переваг при забезпеченні функціонування блокчейну. Новий протокол консенсусу, описаний та проаналізований у цьому проєкті, має переваги у порівнянні з багатьма протоколами, які широко використовуються на сьогоднішній день. Ці переваги полягають як у потенційному збільшенні стійкості до описаних атак, так і у можливості досягнення більшої децентралізації.

2. Запропоновано та досліджено нові методи виявлення вторгнень та ідентифікації атак в перспективних системах виявлення вторгнень. Запропоновані методи мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані рішення щодо виявлення вторгнень та ідентифікації атак носять системний (комплексний) характер. Проактивність рішень забезпечується використанням методів виявлення вторгнень заснованих на статистичних характеристиках трафіка та поведінкових характеристиках трафіка та системи, що забезпечує комплексний аналіз даних як трафіка, так зміни в поведінці системи;

– в процесі виявлення вторгнень та атак, за допомогою запропонованого методу аналізу ентропії пакетів відносна ентропія класів пакетів в спостережуваному трафіку розраховується по відношенню до вихідного

розподілу трафіку. Це дозволяє не тільки виявити атаки, а також ідентифікувати їх тип;

– використання обраних ознак поведінки мережі й користувачів та застосування запропонованих методів виявлення вторгнень на основі ентропійного аналізу протоколів та аналізу сигнатур дозволяє виконати раннє виявлення вторгнень та ідентифікувати тип мережних атак.

2. Обґрунтовано суттєві переваги алгоритму блокового шифрування HadesMiMC та відповідної геш-функції Poseidon при використанні цих криптопримітивів у блокчейні як децентралізованому середовищі, додатковою функцією якого є забезпечення анонімності персональної інформації. Ці переваги полягають як у обґрунтованому рівні стійкості до відомих атак на криптопримітиви, так і у суттєвому підвищенні швидкодії (до 15 разів) при побудові відповідних SNARK-доведень, які є невід'ємною частиною механізмів забезпечення анонімності у блокчейні.

3. Обґрунтовано метод захисту від атаки на підміну блоку з інформацією, яка на певному етапі використовує цензурування. Протягом цієї атаки зловмисник не лише будує альтернативні підграфи, але й вибирає, які саме блоки він буде підтверджувати. Така атака є більш ефективною за кожен з цих методів окремо і її імовірність може бути значною. Також показано, що імовірність успіху цієї атаки можна суттєво знизити, якщо змінити правила прийняття транзакції. Важливими властивостями отриманих результатів є те, що, крім самої оцінки імовірності, можна також обчислити необхідну кількість блоків підтвердження, достатню для того, щоб гарантувати необоротність транзакції з імовірністю, як завгодно близькою до 1.

4. Запропоновано моделі безпечної маршрутизації, безпечної швидкої перемаршрутизації та системи виявлення вторгнень, які мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані рішення щодо безпечної маршрутизації носять системний (комплексний) характер. Проактивність рішень (до компрометації елементів мережі) забезпечується використанням моделі безпечної маршрутизації з

реалізацією принципів балансування навантаження відповідно до вимог концепції Traffic Engineering. Застосування принципів реактивного підходу (після компрометації елементів мережі) бачиться у використанні запропонованої моделі безпечної швидкої перемаршрутизації;

– в процесі балансування навантаження, реалізованого за допомогою запропонованої моделі безпечної маршрутизації, крім характеристик трафіка та пропускної здатності каналів зв'язку також враховуються показники мережної безпеки – ймовірності компрометації каналів зв'язку. Це дозволяє забезпечити в телекомунікаційній мережі комплексне та погоджене між собою покращення як показників якості обслуговування, так і мережної безпеки;

– при порушенні рівня мережної безпеки елементів мережі та пов'язаних з цим відмов в обслуговуванні застосування запропонованої моделі безпечної швидкої перемаршрутизації дозволить мінімізувати час та втрати пакетів шляхом перемикання трафіка на попередньо розраховані резервні шляхи, які не включають проблемні з точки зору мережної безпеки елементи (вузли та канали) телекомунікаційної мережі;

– при балансуванні навантаження легітимного та атакованого трафіку на датчики багатоядерної СВВ використання запропонованої модель системи виявлення вторгнень дозволить збільшити кількість прийнятих і оброблюваних пакетів та зменшити кількість пакетів, що відкидаються.

Практична цінність отриманих результатів реалізації Проєкту для економіки та суспільства.

1. Отримані результати з аналізу, дослідження та обґрунтування шляхів впровадження нових моделей, методів та протоколів захисту можуть використовуватися при створенні перспективних механізмів та систем захисту персональних даних користувачів в умовах децентралізованого середовища. Запропоновані рекомендації щодо застосування SNARKів дозволять забезпечити необхідний рівень анонімності у децентралізованій системі.

2. Отримані результати з аналізу, дослідження та умов застосування Bluetooth, Wi-Fi та GPS технологій у засобах відстеження контактів можуть

використовуватися при розробці моделей, методів та протоколів моніторингових систем запобігання поширення інфекційних захворювань в умовах децентралізованої взаємодії.

3. Отримані результати з аналізу та дослідження моделей загроз, порушника та безпеки моніторингових систем відстеження контактів, деперсоналізації даних та побудови мережі в умовах децентралізованого середовища мають практичну цінність, що полягає у:

– можливості захищеного зберігання приватної, персональної та конфіденційної інформації у децентралізованому середовищі;

– можливості її більш швидкої та більш захищеної обробки;

– можливості досягнення високого рівня анонімності як для клієнта, інформація якого обробляється, так і для особи, яка цю інформацію обробляє.

4. Отримані результати з обґрунтування перспективних напрямків застосування криптографічних примітивів та протоколів взаємодії у децентралізованому середовищі можуть використовуватися при розробці сучасних методів та механізмів досягнення послуг безпеки (конфіденційності, цілісності, доступності, неспростовності) моніторингових систем запобігання поширення інфекційних захворювань в умовах децентралізованої взаємодії.

5. Запропоновані методи виявлення вторгнень на основі ентропійного аналізу протоколів та аналізу сигнатур можуть бути використані в системах виявлення вторгнень інфокомунікаційних мереж та при виявленні різного роду аномалій. Їх застосування на практиці призведе до підвищення захищеності інформаційних ресурсів шляхом підвищення точності, швидкості та своєчасністі виявлення вторгнень та ідентифікації атак.

6. Отримані результати з обґрунтування критеріїв та показників ефективності механізмів криптографічного захисту персональних даних користувачів та протоколів взаємодії можуть застосовуватися на практиці для оцінки та при проведенні порівняльних досліджень різних алгоритмів та протоколів криптоперетворення як у моніторингових системах з

децентралізованою взаємодією, так і у інших прикладних додатках, зокрема, при розбудові національної системи з надання електронних довірчих послуг, тощо.

7. Отримані результати з розробки методики оцінки та порівняльних досліджень криптографічних примітивів та протоколів взаємодії можуть бути застосовані в моніторингових системах запобігання поширенню інфекційних захворювань, які функціонують у блокчейні як у децентралізованому середовищі. Зокрема, за результатами досліджень докладно розглянуто геш-функцію Poseidon і алгоритм блокового шифрування HadesMiMC, отримано строго обґрунтовані оцінки їх стійкості до лінійних та різницевих атак, визначено конкретні параметри для алгоритму шифрування HadesMiMC та геш-функції Poseidon, які дозволяють застосовувати їх для рекурентних SNARK-доведень. Ці примітиви особливо цікаві тим, що дуже добре підходять для використання в математичному апараті, який забезпечує повну анонімність оброблюваної інформації, що, зокрема, може бути ефективно застосовано для захисту персональної інформації пацієнтів в умовах пандемії. Отримані результати показали, що блоковий алгоритм шифрування HadesMiMC, що базується на операціях у простому скінченному полі, є стійким до лінійного та різницевого криптоаналізу, при правильному виборі параметрів цього алгоритму. Також, як наслідок, стійкою буде і геш-функція Poseidon, побудована з використанням конструкції SPONGE та перестановки HadesMiMC. Також було показано, як повинні бути вибрані параметри алгоритму, щоб гарантувати його заданий рівень стійкості. Крім того, обчислено кількість констрейнтів на біт інформації та показано, що алгоритм HadesMiMC та геш-функція Poseidon на сьогоднішній день не мають конкурентів при використанні у SNARK-доведеннях.

8. Отримані результати з проведення порівняльних досліджень та оцінки ефективності криптографічних примітивів та протоколів взаємодії дають можливість забезпечити швидку обробку інформації, яка поступає з моніторингових систем, а також гарантувати її цілісність, непідробність, конфіденційність та необхідний рівень анонімності.

9. Запропоновані моделі безпечної маршрутизації, безпечної швидкої перемаршрутизації та системи виявлення вторгнень можуть бути покладені в основу математичного та алгоритмічно-програмного забезпечення існуючих та перспективних маршрутизаторів IP/MPLS-мереж, серверів маршрутів та контролерів програмно-конфігурованих мереж. Їх застосування на практиці призведе по підвищення як рівня якості обслуговування за показниками мережної продуктивності, так і рівня мережної безпеки.

Опис шляхів та способів подальшого використання результатів виконання Проєкту в суспільній практиці.

1. Результати аналізу, дослідження та обґрунтування шляхів впровадження нових моделей, методів та протоколів захисту персональних даних можуть бути використані у суспільній практиці:

– для забезпечення цілісності, конфіденційності та анонімності інформації користувача або клієнта при її зберіганні, обробці та пересиланні в умовах децентралізованого середовища;

– для можливості створення багаторівневого доступу до приватної та персональної інформації, коли кожен, кому надано частковий доступ, може отримувати чиюсь персональну інформацію лише відповідно до свого статусу (лікар- доступ до медичної інформації, юрист – стосовно правопорушень, нотаріус – про майнову інформацію, роботодавець – інформацію про кваліфікації, тощо);

– для забезпечення анонімності того, хто буде обробляти відповідну персональну інформацію;

– для забезпечення неможливості підміни інформації;

– для гарантії невідмовності від існуючої у середовищі інформації.

2. Результати аналізу, дослідження та обґрунтування застосування Bluetooth, Wi-Fi та GPS технологій у засобах відстеження контактів можуть бути використані при обґрунтуванні компонентів моніторингових систем запобігання поширення інфекційних захворювань в умовах децентралізованої взаємодії.

3. Отримані результати з аналізу та дослідження моделей загроз, порушника та безпеки моніторингових систем відстеження контактів, деперсоналізації даних та побудови мережі в умовах децентралізованого середовища можуть бути використані:

– для створення захищеної децентралізованої системи зберігання, обробки та пересилання різної персональної, приватної, особистої та конфіденційної інформації;

– для створення електронного документообігу;

– для підвищення анонімності інформації, що зберігається, обробляється та пересилається, при чому анонімність забезпечується як для власника інформації, так і для особи, яка з нею працює;

– для забезпечення неспростовності, цілісності, конфіденційності інформації;

– для забезпечення розмежування доступу до різної персональної, приватної, особистої та конфіденційної інформації, що зберігається, обробляється та пересилається у децентралізованому середовищі.

4. Отримані результати з обґрунтування перспективних напрямків застосування криптографічних примітивів та протоколів взаємодії можуть бути використані при обґрунтуванні вимог та умов створення та практичного використання криптографічних моделей, методів та обчислювальних алгоритмів у децентралізованому середовищі як основних компонентів моніторингових систем запобігання поширення інфекційних захворювань.

5. Представлені методи моніторингу, швидкого та раннього виявлення вторгнень та ідентифікації мережних атак, виявлення фактів несанкціонованого доступу програмно реалізовані мовою Python та на рівні програмного прототипу можуть стати частиною систем виявлення вторгнень та систем виявлення аномалій. Область застосування запропонованих методів – інформаційні системи, які функціонують в умовах постійних загроз мережній безпеці. Це особливо важливо в умовах передачі конфіденційного трафіка або даних з обмеженим доступом.

6. Результати з обґрунтування критеріїв та показників ефективності механізмів криптографічного захисту персональних даних користувачів та протоколів взаємодії можуть бути безпосередньо використані у якості основного методичного напрацювання з методології дослідження та порівняльних оцінок різних сімейств криптоперетворень, в тому числі, в децентралізованих моніторингових систем, які будуються на основі технології блокчейн.

7. Отримані результати з розробки методики оцінки та порівняльних досліджень криптографічних примітивів та протоколів взаємодії можуть застосовуватися:

– при розробці та імплементації механізмів забезпечення анонімності оброблюваної інформації;

– для ефективного захисту персональної інформації пацієнтів в умовах пандемії;

– для підвищення швидкості обробки інформації в децентралізованому середовищі;

– для забезпечення анонімності як власника інформації, так і того, хто її обробляє;

– для забезпечення розмежування доступу або для багаторівневого доступу до різної персональної інформації в залежності від статусу того, хто має право на отримання відповідної інформації.

8. Отримані результати порівняльних досліджень та оцінки ефективності криптографічних примітивів та протоколів взаємодії можуть застосовуватись при побудові моніторингових систем запобігання поширенню інфекційних захворювань, що функціонують у децентралізованому середовищі із використанням протоколу консенсусу на блокграфах.

9. Представлені математичні моделі безпечної маршрутизації та безпечної швидкої перемаршрутизації програмно реалізовані в середовищі MATLAB та на рівні програмного прототипу можуть стати частиною перспективного протоколу маршрутизації. Математична модель системи виявлення вторгнень програмно реалізована на мові програмування Python для балансування навантаження

вузлів мережної системи виявлення вторгнень. Область застосування запропонованих моделей – телекомунікаційні мережі, які розгорнуті для взаємодії об’єктів критичної інфраструктури, що функціонують в умовах постійних загроз мережній безпеці. Це особливо важливо в умовах передачі конфіденційного трафіка або даних з обмеженим доступом.

Висновки за етапом № 1 (2021 року)

Опис наукових та науково-технічних результатів, отриманих в рамках виконання Проєкту (за окремими індикаторами виконання завдань).

1. Результати аналізу та класифікації моделей, методів та алгоритмів КЗІ та протоколів взаємодії для відстеження контактів у моніторингових системах.

Досліджено комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних без наявності будь-якої довіреної сторони, які надають можливість виконувати задану обробку виключно у зашифрованому вигляді з гарантією конфіденційності інформації та доступністю відповідного фрагменту оригінальних та/або перетворених даних виключно учаснику, який є власником відповідного фрагменту даних і при цьому не має довіри до решти учасників. Наведено моделі, алгоритми та протоколи КЗІ, які є необхідними при відстеженні контактів у моніторингових системах.

Проведено огляд та надано стислий опис існуючих додатків, призначених для відстеження контактів хворих на COVID-19. Зроблено висновок, що найкращими є додатки, які підтримують конфіденційність і не використовують місцезнаходження користувачів. З цієї точки зору, протокол, запропонований Google/Apple, видається найбільш перспективним для використання при розробці додатків для відстеження контактів COVID-хворих.

Наведено алгоритми та протоколи КЗІ, необхідні для коректної та повноцінної роботи таких додатків (алгоритми цифрового підпису, гешування та інкапсуляції ключів). Щодо кожного алгоритму та протоколу надано пояснення, чому він є необхідним для роботи додатку, які функції виконує та які властивості протоколів взаємодії він забезпечує.

2. Результати аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії для побудови однорангової системи обробки даних у децентралізованих системах.

Досліджено протоколи взаємодії для побудови системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров'я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань.

Наведено визначення однорангових систем обробки даних, проаналізовано переваги та недоліки таких систем, представлено результати критичного порівняння та аналізу існуючих протоколів консенсусу. Особливу увагу приділено такому найцікавішому та найпоширенішому випадку однорангової системи, як система, що базується на технології блокчейн.

Показано та обґрунтовано, які криптографічні алгоритми та протоколи потрібні для повноцінного функціонування таких систем.

Розглянуто недоліки таких систем, які є особливо критичними при обміні важливою та/або терміновою інформацією. Показано, як можна повністю або частково усунути ці недоліки, якщо скористатись новими методами, які з'явились у блокчейн технологіях. Використовуючи ці методи, можна побудувати деяку дворівневу структуру, яка складається з довільної кількості різних незалежних однорангових систем (за відповідною аналогією з криптовалютними блокчейнами, ми будемо їх називати сайдчейнами) з однією блокчейн мережею (MC – mainchain), єдиною задачею якої буде створення посилань на блоки сайдчейнів, для забезпечення їх стійкості та надійності. Мережа MC, з одного боку, ніяк не впливатиме на децентралізацію та самостійність окремих локальних однорангових систем, а з іншого – буде захищати ці системи від основних атак, спрямованих на протокол консенсусу блокчейну.

Після огляду загальної концепції побудови описаної дворівневої структури, детально описано її функціонування та вибір певних параметрів, які

визначають роботу цієї структури. Представлено компоненти децентралізованого протоколу з відповідними характеристиками, що дозволяє ефективну взаємодію десяткам мільйонів учасників для побудови децентралізованого розподіленого реєстру (або у приватному випадку - блокчейну). Зокрема, детально розглянуто протокол автентифікації, який також необхідний для коректності роботи однорангової системи. Наведено та проаналізовано дві версії цього протоколу, повну та вкорочену, та наведено пояснення, за яких умов їх використовувати. Крім того, "класичну" версію протоколу, яка розрахована на спілкування Сервер – Клієнт, адаптовано саме для випадку спілкування або двох вузлів однорангової мережі, або вузла однорангової мережі з вузлом мережі МС.

3. Вимоги та умови практичного застосування криптографічних примітивів протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань з урахуванням результатів досліджень.

Описано вимоги до забезпечення технічних та організаційних заходів, необхідних для забезпечення коректної роботи криптоалгоритмів та протоколів.

Досліджено вимоги та умови практичного застосування криптографічних примітивів та протоколів взаємодії для побудови системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань. Зокрема, визначено загальні показники стійкості криптосистем та задачі дискретного логарифмування.

Описано загальні та спеціальні методи дискретного логарифмування, що застосовуються у різних групах. Розглянуто різні атаки на визначені у розділах I та II алгоритми та протоколи, і, виходячи з працевитрат, необхідних для успішної реалізації атаки, визначено параметри, що забезпечують необхідний рівень стійкості, та область значень цих параметрів, за яких алгоритм чи протокол буде криптографічно стійким – звісно, за умови його коректного використання із виконанням всіх технічних та організаційних вимог.

4. Нові науково обґрунтовані положення в теорію інформаційної та мережної безпеки, які представлені розробленими в проєкті моделями та методами безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

Проведено аналіз існуючих рішень в області моніторингу мережі та виявлення вторгнень. Розглянуто проблеми моніторингу трафіка за різними підходами та пристроями. Проведено аналіз задач моніторинга, обробки та аналізу трафіку в мережних системах виявлення вторгнень. Розглянуто підходи щодо прискорення обробки трафіку в СВВ. З проведеного аналізу виникає важлива задача розробки методу моніторингу та аналізу трафіка в мережній СВВ, що враховує самоподібні властивості вхідного трафіку, час обслуговування та заснований на аналізі сигнатур.

Результати проведеного аналізу показали, що мережні СВВ-датчики можуть виявляти атаки, які датчикам на основі хоста не вдається виявити. Мережна СВВ перевіряє всі заголовки пакетів на наявність будь-якої шкідливої атаки. Багато DoS-атак (denial of service) заснованих на IP, таких як атака TCP SYN, фрагментована атака пакетів тощо, можна ідентифікувати лише за допомогою перегляду заголовків пакетів під час передачі в мережі. Таким чином, обрано мережну СВВ для проведення моніторингу та виявлення вторгнень.

Проведено аналіз існуючих атак в мережі та методів їх виявлення, який показав, що найбільш використовуваними та дієвими є методи машинного навчання та сигнатурні методи аналізу. Результати проведеного аналізу показали, що симбіотичне використання методів виявлення вторгнень повинне підвищити ймовірність та точність виявлення атак.

Розроблено модель системи моніторингу, до параметрів якої належать мультифрактальні характеристики трафіка, обмеження на час обслуговування різних класів трафіка, обмеження на кількість втрат, на час затримок. Модель моніторингу трафіка базується на розробленій раніше моделі мережної системи виявлення вторгнень, до параметрів якої належать мультифрактальні

характеристики трафіку, обмеження на час обслуговування різних класів трафіку.

Розроблена модель враховує параметри мережної безпеки, основним з яких виступала ймовірність виявлення вторгнень в мережу. Також розроблена модель враховує параметри завантаження ресурсів мережі. Це дозволяє розробити методи моніторингу трафіка детекторами виявлення вторгнень з урахуванням вимог якості обслуговування та параметрів безпеки.

Удосконалено метод моніторингу трафіка, який враховує його мультифрактальні та рекурентні характеристики. Розроблений метод застосовує модель моніторингу трафіка та враховує параметри безпеки розподілу трафіка, ймовірність виявлення вторгнень та атак. Для виявлення вторгнень формується база даних сигнатур, яка рейтингується в залежності від вимог моніторингу. Реалізація зазначеного методу дозволяє зменшити завантаженість ресурсів комп'ютерної системи за рахунок спрямування безпечних неоднорідних інформаційних потоків на безпечні та менш завантажені ресурси.

5. Результати дослідження запропонованих моделей, методів і протоколів безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

Встановлено, що основними вимогами, які висуваються до сучасних інфокомунікаційних систем і мереж, традиційно є забезпечення заданого рівня якості обслуговування та мережної безпеки. В умовах забезпечення мультисервісу в інфокомунікаційній мережі циркулює досить різний за своїми вимогами до QoS і NS інформаційних трафік, характеристики якого все частіше вдається описати за допомогою теорії фракталів і самоподібних процесів. Важливим науковим і практичним завданням є розробка математичних моделей, методів та у перспективі протоколів маршрутизації, які б забезпечували задані значення основних показників якості обслуговування самоподібного трафіка та орієнтували на підвищення рівня мережної безпеки.

Обрані для дослідження базові потокові математичні моделі маршрутизації, які адекватно описують мережний процес як у випадку

відсутності перевантаження, так і при ймовірному перевантаженні елементів (каналів і буферу черг) інфокомунікаційної мережі. Для формалізації умов забезпечення якості обслуговування за показниками пропускної здатності, середньої міжкінцевої затримки та ймовірності втрат пакетів використано апарат тензорного аналізу. Отримані QoS-умови можуть виступати як додаткові обмеження, що накладаються на маршрутні змінні.

З метою оптимізації процесів безпечної маршрутизації запропоновано критерій оптимальності та систему метрик безпечної маршрутизації в інфокомунікаційній мережі, які доцільно використовувати за умови різних сценаріїв компрометації мережного обладнання – маршрутизаторів і каналів зв’язку. Найпростіші метрики маршрутизації можуть ґрунтуватись на використанні ймовірностей компрометації маршрутизаторів і каналів ІКМ, а більш складні метрики безпечної маршрутизації отримуються на підставі оцінки ризику інформаційної безпеки мережних елементів ІКМ.

Результати дослідження підтвердили адекватність та ефективність запропонованих моделей і методів безпечної маршрутизації з погляду розрахунку найбільш безпечних маршрутів, які б додатково задовольняли вимогам щодо рівня якості обслуговування самоподібних потоків пакетів.

6. Результати досліджень математичних моделей криптографічного захисту персональних даних у засобах відстеження контактів.

Проведено дослідження математичних моделей криптографічного захисту персональних даних у засобах відстеження контактів. Зокрема, розглянуто різні підходи та абстрактні уявлення до формування моделей безпеки криптографічних систем: інформаційно-теоретична модель безпеки криптографічних систем, докази в якій виводяться з теорії інформації. Безпека в цій моделі повинна забезпечуватися навіть коли зловмисник володіє нескінченно великими обчислювальними ресурсами; стандартна модель, докази безпеки в якій виводяться на основі теорії складності, а завдання підбираються такими, щоб їх не можна було вирішити за поліноміальний час. Отже зловмисник для порушення безпеки повинен володіти досить великими обчислювальними

ресурсами, а для забезпечення потрібної безпеки такі ресурси повинні бути для зловмисника недосяжними; ігрові моделі, які розглядають криптографічний захист як гру із супротивником, тобто доведення в яких базується на певних припущеннях про можливості та дії гравців, а також на абстрактних уявленнях типу «випадковий оракул», тощо; моделі криптографічного захисту на фізичному рівні (наприклад, модель системи PLE), докази безпеки в якій враховують якість фізичних каналів між абонентами інформаційної взаємодії. Це більш практичний та ефективний підхід, який враховує можливість виникнення помилок при передачі повідомлень, а також можливість задання простору зашифрованого сигналу як безперервного векторного простору (що є більш реалістичним з погляду реальних систем та мереж передавання інформації); квантові та пост-квантові моделі безпеки, які враховують останні досягнення квантової механіки та докази в яких будуються із застосуванням формальних математичних моделей випадкових оракулів, квантових порушників, підробок, тощо.

Досліджено основні математичні моделі, які застосовуються при формальному описі та оцінці властивостей криптографічних примітивів та криптографічних систем, зокрема: детерміновані та ймовірності моделі відкритого тексту (символів, біграм, тощо), марківські моделі залежних символів тощо; математичні моделі шифрів та шифросистем: абстрактні моделі секретних систем (К. Шенона), методи їх комбінації та ймовірності моделі; математичні моделі криптопримітивів (шифр простої заміни, зсуву, афінного шифрування, заміни з кінцевим ключем, перестановки, тощо); ортогональні таблиці, досконалі шифри, математичні моделі шифру заміни з обмеженим і необмеженим ключем, випадкові і детерміновані генератори ключового потоку, тощо.

7. Результати досліджень криптографічних примітивів та протоколів взаємодії при збиранні, зберіганні та розповсюдженні даних про контакти.

Представлено результати з розробки та дослідження криптографічних примітивів та протоколів взаємодії при збиранні, зберіганні та розповсюдженні даних про контакти. Зокрема, розглянуто можливі альтернативи алгоритмів

цифрових підписів, асиметричного шифрування, хешування та генераторів псевдовипадкових послідовностей, що можуть бути використанні для реалізації у системах моніторингу контактів.

Особливістю застосування цифрового підпису в сучасних моніторингових системах є те, що такий підпис отримується за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується. Досліджено класифікації цифрових підписів, а також опис поширених алгоритмів цифрового підпису, що функціонують на сьогодні, а також принципово нові схеми пост-квантового рівня стійкості, зокрема, які будуються із застосуванням кодової криптографії. Розглянуто декілька варіантів побудови пост-квантово стійкого підпису та запропоновано альтернативну схему, що є перспективним напрямком в умовах розробки квантового комп'ютера, який здатен здійснити крипто аналіз систем на основі еліптичних кривих та факторизації. Альтернативна схема у своїй основі використовує гібридні кодові криптосистеми, ефективний алгоритм криптоаналізу для кого не відомо.

Досліджено асиметричні схеми шифрування, проведено їх класифікацію, типові варіанти використання, тощо. Зокрема докладно розглянуто напрямок пост-квантової криптографії, що заснований на застосуванні кодових криптосистем: класичних схем Мак-Еліса та Нідеррайтера і нової запропонованої схеми, що є гібридним використанням класичних схем, але при цьому із значно покращеними показниками ефективності, що доведено як з аналітичної, так і з практичної точки зору.

Досліджено різні схеми геш-функцій, що можуть бути використані як при реалізації блокчейн систем, так і на різних етапах функціонування систем моніторингу даних для ефективного зберігання, передачі даних та інше. На рівні з міжнародними алгоритмами досліджено стандартизований алгоритм хешування «Купина», ефективність та безпечність якого є доведеною низкою пошукових робіт, отже цей алгоритм може бути надійною альтернативою поширеним міжнародним схемам геш-функцій.

Досліджено генератори псевдовипадкових послідовностей, які необхідні для реалізації систем відстеження контактів, оскільки є складовою для генерації відкритих та секретних ключів, одноразових секретів тощо. Проаналізовано умови, що забезпечують використання генераторів, типову схему генератора, а також досліджено та запропоновано конкретні приклади пост-квантово стійких генераторів, що можуть бути застосовані.

8. Результати оцінки безпеки протоколів та криптографічних перетворень, які можуть застосовуватися при відстеженні контактів.

Проведено дослідження безпеки протоколів та криптографічних перетворень, які можуть застосовуватися при відстеженні контактів. Зокрема, представлено всебічне дослідження щодо відстеження контактів, що охоплює як традиційні, так і новітні технології цифрового відстеження контактів;

Висвітлено фундаментальний підхід та моделі відстеження контактів, і основна увага приділена до новітніх цифрових технологій відстеження контактів, із деталізацією різноманітних мобільних програм для відстеження контактів, які в даний час використовуються у багатьох країнах, разом із відповідними технологіями локалізації;

Висвітлено сучасні проблеми, з якими стикаються технології відстеження контактів, і кілька майбутніх тенденцій, передбачених для технологічного розвитку відстеження контактів у майбутньому. Враховуючи нестримну пандемію COVID-19, яку переживає світ, отримані результати дослідження є надзвичайно актуальними та значущими.

9. Результати досліджень запропонованих моделей, методів та технологій моніторингу, виявлення вторгнень та ідентифікації атак.

Проведено імітаційне моделювання розробленого методу моніторингу трафіка в системі виявлення вторгнень. Запропонований метод враховує параметри мультифрактальності трафіка та ймовірність виявлення вторгнень. При імітаційному моделюванні досліджувався вплив мультифрактальних властивостей трафіка на параметри якості обслуговування. Аналіз результатів імітаційного моделювання показав, що за низьких значень H та низької

неоднорідності моніторингова система приходить у стан рівноваги та продуктивність СВВ є задовільною, а час обробки пакетів має зменшується. За великих значень параметру Херста та великої неоднорідності, система моніторингу перебуває у нестабільному стані, а час обробки зростає, що призводить до максимального навантаження ресурсів, а отже, до значного збільшення кількості непроаналізованих пакетів і втрачених даних. Використання запропонованого методу моніторингу призводить до збільшення кількості проаналізованих пакетів на 23%, за рахунок чого відсоток виявлених атак збільшився на 16%, зменшується середній час очікування пакетів на 18% та зменшується кількість втрачених даних.

Розроблено симулятор атакованого трафіка, який дозволяє створювати модельну адитивну реалізацію трафіка і атаки, із заданими параметрами як трафіка, так і атаки. Реалізації атак відповідають відомим існуючим атакам різних типів. Отриманий штучним шляхом трафік атаки, разом з реальним трафіком з датасета, був використаний для проведення експериментів з методами машинного навчання.

Набули подальшого розвитку методи виявлення вторгнень на основі машинного навчання, які базуються на мультифрактальних та рекурентних характеристиках трафіка, що дозволяє скоротити час виявлення вторгнень і збільшує швидкість та точність виявлення вторгнень, уможливлює виявлення вторгнення при низькому рівні кібератак. Як методи класифікації обрано методи дерев рішень і нейронні мережі. Як ознаки використано статистичні, фрактальні і рекурентні характеристики трафіку.

Методи аналізу поведінки трафіку за допомогою машинного навчання показали високу точність ідентифікації різних атак при зміні інтенсивності атаки. Результати класифікації показали, що ймовірність виявлення атаки істотно залежить від фрактальних властивостей трафіка, рівня атаки по відношенню до трафіка і варіюється від 0,7 до 0,98: чим більша різниця фрактальних характеристик, тим більша ймовірність виявлення. Результати

показують, що методи класифікації, зокрема випадковий ліс, можуть бути успішно застосовані для виявлення DDoS-атак.

Проведено порівняльний аналіз бінарної класифікації фрактальних часових рядів методами машинного навчання. Розглянуто класифікацію на прикладі виявлення DDoS-атак у реалізаціях трафіка. Як методи класифікації були обрані випадковий ліс з деревами регресії і багатошаровий персептрон з періодичної нормалізацією. Реалізація трафіка з атаками була отримана шляхом підсумовування симульованого мультифрактального трафіка і реалізації DDoS-атаки. Результати класифікації показали, що ймовірність виявлення атаки істотно залежить від фрактальних властивостей нормального трафіка. Це пояснюється тим фактом, що зазвичай реалізації атак DDos мають велике значення показника Херста, і чим більше фрактальні властивості нормального трафіка і реалізацій атак відрізняються, тим легше виявити вторгнення. Чисельний експеримент показав, що виявлення атаки можливо на ранній стадії, коли коефіцієнт середньої атаки становить 15-20% від середнього трафіку. Ймовірність виявлення атаки залежить від рівня атаки по відношенню до трафіка і варіюється від 0,6 при 15% до 0,9 при рівні 20%. Метод випадкового лісу показав себе краще під час розпізнавання нормального трафіка, ніж нейронна мережа, але нейронні мережі мають великий потенціал для поліпшення.

Обґрунтування переваг науково-технічної продукції у порівнянні з існуючими аналогами.

1. Результати аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії для відстеження контактів у моніторингових системах мають наступні переваги у порівнянні з існуючими аналогами:

– вони орієнтовані саме на такі моделі, методи та алгоритми КЗІ, що є необхідними для роботи додатків, що відстежують контакти у моніторингових системах;

– аналіз моделей та методів виконувався саме з точки зору можливості та зручності їх застосування у моніторингових системах;

– запропоновані рішення щодо використання моделей, методів та алгоритмів КЗІ у моніторингових системах враховують специфіку таких систем. Використання запропонованих криптографічних примітивів дозволить виконувати ефективний моніторинг та, разом з тим, забезпечити достатній рівень анонімності.

2. Результати аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії для побудови однорангової системи обробки даних у децентралізованих системах мають наступні переваги у порівнянні з існуючими аналогами:

Показано, що децентралізовані системи, побудовані у вигляді блокчейну, мають додаткові переваги, а крім того, за рахунок певних надбудов, можуть бути удосконалені за такими напрямками:

– підвищення надійності та стабільності зберігання, обробки та передачі інформації;

– підвищення швидкості зберігання, обробки та передачі інформації;

– підвищення ефективності пошуку інформації, розміщеної у багатьох незалежних, автономних однорангових системах.

При цьому децентралізація системи не зменшується.

3. Результати з обґрунтування вимог та умов практичного застосування криптографічних примітивів та протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані рішення щодо вимог та умов практичного застосування криптографічних примітивів та протоколів, а також засобів КЗІ носять комплексний характер, вони враховують не тільки вимоги на параметри окремих алгоритмів та протоколів, а і повний комплект організаційних та технічних заходів;

– запропоновані вимоги та умови практичного застосування криптографічних примітивів та алгоритмів є повністю математично

обґрунтованими та оновленими відповідно до сьогоденних вимог до криптографічної стійкості таких примітивів та алгоритмів;

– для кожного криптографічного примітиву рівень його стійкості визначався індивідуально, відповідно до загальноприйнятого визначення, що дає можливість гарантувати загальну стійкість комплексу всіх криптографічних примітивів, що плануються до використання.

4. Запропоновані моделі моніторингу мережі та самоподібного трафіка мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані рішення щодо моніторингу трафіка носять системний (комплексний) характер. Проактивність рішень (до компрометації елементів мережі) забезпечується використанням моделі моніторингу мережі з реалізацією принципів балансування навантаження за рахунок врахування параметрів завантаженості ресурсів мережі. Застосування принципів реактивного підходу (після компрометації елементів мережі) бачиться у використанні методу моніторингу в системі виявлення вторгнень;

– в процесі моніторингу мережі, реалізованого за допомогою запропонованої моделі моніторингу, крім характеристик трафіка та пропускної здатності каналів зв’язку також враховуються показники мережної безпеки – ймовірності виявлення вторгнень та мультифрактальні властивості трафіка. Це дозволяє забезпечити в телекомунікаційній мережі комплексне та погоджене між собою покращення як показників якості обслуговування, так і мережної безпеки;

– при вторгненнях в мережу та реалізації атак застосування запропонованого методу моніторингу трафіка дозволить мінімізувати час та втрати пакетів шляхом блокування атакованого трафіка та вивільнення ресурсів для обробки легітимного трафіка.

5. Запропоновані моделі та методи безпечної маршрутизації в інфокомунікаційних мережах мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані рішення щодо безпечної маршрутизації враховують самоподібний характер більшості потоків пакетів, які циркулюють в

інфокомунікаційній мережі. Це дозволяє адекватно описати сучасний мережний трафік та забезпечити більш ефективне управління канальним та буферним ресурсом інфокомунікаційної мережі;

– отримані маршрутні рішення, завдяки застосуванню тензорної методології досліджень, орієнтують на забезпечення заданого рівня якості обслуговування за множиною показників: пропускною здатністю, середньою міжкінцевою затримкою та ймовірністю втрат пакетів. Запропоновані моделі та методи маршрутизації адекватно враховують характеристики потоків пакетів, дисципліни їх обслуговування на маршрутизаторах, а також параметри самої інфокомунікаційної мережі;

– оптимізаційна постановка задачі безпечної маршрутизації дозволяє максимізувати рівень мережної безпеки в інфокомунікаційній мережі на підставі використання системи метрик маршрутизації, які адекватно враховують ключові параметри мережної безпеки елементів ІКМ: ймовірності компрометації каналів та маршрутизаторів, перелік ймовірних вразливостей з оцінкою очікуваних збитків від їх реалізації з боку зловмисника.

6. Результати з дослідження математичних моделей криптографічного захисту персональних даних у засобах відстеження контактів мають переваги у порівнянні з існуючими аналогами, які полягають у комплексному врахуванні різних підходів до формалізованого опису моделей безпеки (інформаційно-теоретичних моделей, що будуються на базових положеннях теорії інформації; стандартної моделі, що будується на основі теорії складності; ігрових моделей, що застосовує певні припущення про можливості та дії гравців, абстрактні уявлення типу «випадковий оракул», тощо; моделей захисту на фізичному рівні (модель системи PLE), які враховують якість фізичних каналів між абонентами інформаційної взаємодії; квантові та пост-квантові моделі безпеки, які враховують останні досягнення квантової механіки із застосуванням формальних математичних моделей випадкових оракулів, квантових порушників, підробок, тощо), а також моделей криптографічних примітивів та криптографічних систем (детермінованих та ймовірнісних моделей відкритого

тексту (символів, біграм, тощо), марківських моделей залежних символів тощо; моделей шифрів та шифросистем (абстрактні моделі секретних систем, методи їх комбінації та ймовірності моделі); моделі криптопримітивів (шифр простої заміни, зсуву, афінного шифрування, заміни з кінцевим ключем, перестановки, тощо); ортогональні таблиці, досконалі шифри, математичні моделі шифру заміни з обмеженим і необмеженим ключем, випадкові і детерміновані генератори ключового потоку, тощо).

7. Результати з розробки та дослідження криптографічних примітивів та протоколів взаємодії при збиранні, зберіганні та розповсюдженні даних про контакти мають переваги у порівнянні з існуючими аналогами, які полягають у врахуванні останніх тенденцій та нових положень криптографічної науки у створенні квантово-стійких криптографічних механізмів та протоколів (цифрових підписів, асиметричного шифрування, хешування та генераторів псевдовипадкових послідовностей, тощо). Зокрема, при виконанні проєкту досліджено: декілька варіантів побудови пост-квантово стійкого цифрового підпису та запропоновано альтернативну схему, що є перспективним напрямком в умовах можливого застосуванні квантових обчислювачів (альтернативна схема використовує гібридні кодові криптосистеми, ефективний алгоритм криптоаналізу для кого не відомо); асиметричні схеми шифрування для пост-квантового застосування, в тому числі на кодових криптосистемах (класичних схем Мак-Еліса та Нідеррайтера і нової запропонованої схеми, що є гібридним використанням класичних схем, але при цьому із значно покращеними показниками ефективності); різні схеми геш-функцій, в тому числі новий алгоритм хешування «Купина» із підвищенням рівнем швидкості та безпеки; генератори псевдовипадкових послідовностей, що забезпечують пост-квантовий рівень стійкості, максимальний період формованих послідовностей та статистичну безпеку тощо.

8. Результати оцінки безпеки протоколів та криптографічних перетворень, які можуть застосовуватися при відстеженні контактів мають переваги у порівнянні з існуючими аналогами: обґрунтовано пропозиції та рекомендації

щодо створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини. Зокрема, проаналізовано та досліджено різні міжнародні методології загроз, запропоновано наступні контролі безпеки, за якими був зроблений подальший порівняльний аналіз: Конфіденційність; Цілісність; Існування механізму боротьби з проявом DOS атак; Обробка великого об'єму даних (випадок коли зловмисник може генерувати/відправляти великий об'єм даних); Уникання помилкового контакту (коли зловмисник може транслювати дані про позитивний тест іншим користувачам використовуючи потужні антени, створюючи масштабні фальшиві контакти; Справжня особистість (використання певних алгоритмів шифрування для захисту початкових ключів та псевдонімів); Авторизация; Невідречення. Досліджено реалізацію контролю приватності під час реалізації моніторингових рішень із забезпеченням наступних принципів: Права доступу; Мінімізація даних; Обмеження у зберіганні; Обмеження зберігання; Невідстежуваність; Захист інфікованих користувачів; Захист користувачів, які у зоні ризику; Захист інформації про взаємодію. Висвітлено сучасні проблеми, з якими стикаються технології відстеження контактів, і кілька майбутніх тенденцій, передбачених для технологічного розвитку відстеження контактів у майбутньому.

9. Запропоновані методи моніторингу та виявлення вторгнень та ідентифікації атак в системах виявлення вторгнень мають наступні переваги у порівнянні з існуючими аналогами:

– запропонований метод моніторингу трафіка в системах виявлення вторгнень, на відміну від існуючих, враховує мультифрактальні характеристики трафіка та ймовірність виявлення вторгнень;

– запропоновані рішення щодо виявлення вторгнень та ідентифікації атак носять системний (комплексний) характер. Проактивність рішень забезпечується використанням методів виявлення вторгнень заснованих на статистичних характеристиках трафіка та поведінкових характеристиках трафіка та системи, що забезпечує комплексний аналіз даних як трафіка, так зміни в поведінці системи;

– в процесі виявлення вторгнень та атак, за допомогою вдосконалених методів машинного навчання враховувались рекурентні та мультифрактальні характеристики трафіка. Це дозволяє не тільки виявити атаки, а також ідентифікувати їх тип;

– використання обраних ознак поведінки мережі й користувачів та застосування запропонованих методів виявлення вторгнень на основі методів машинного навчання дозволяє виконати раннє виявлення вторгнень та ідентифікувати тип мережних атак.

Практична цінність отриманих результатів реалізації Проєкту для економіки та суспільства.

1. За результатами аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії для відстеження контактів у моніторингових системах наведено основні застосування, які розроблені та використовуються різними країнами для відслідковування контактів під час пандемій. Після аналізу цих застосувань показано, які основні криптографічні алгоритми необхідні для кожного з них, щоб забезпечити, з одного боку, достатній рівень захисту персональної інформації, а з іншого – підтвердження авторства, цілісність повідомлення та оптимізацію процесу передавання конфіденційних даних. Так, розглянуті алгоритми гешування, цифрового підпису, гібридного шифрування та інкапсуляції ключа і для кожного з них була обґрунтована необхідність його застосування у моніторингових системах.

2. За результатами аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії для побудови однорангової системи обробки даних у децентралізованих системах:

– детально описано функціонування та параметри, які визначають роботу дворівневої структури, яка складається з довільної кількості різних незалежних однорангових систем (сайдчейнів) з однією блокчейн мережею (mainchain);

– представлено компоненти децентралізованого протоколу з відповідними характеристиками, що дозволяє ефективну взаємодію десяткам мільйонів учасників для побудови блокчейну, зокрема, наведено приклад протоколу

автентифікації, що використовується для обміну повідомленнями як між різними вузлами, так і між різними мережами, та забезпечує надійність обміну інформацією.

3. За результатами обґрунтування вимог та умов практичного застосування криптографічних примітивів протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань з урахуванням результатів досліджень:

– дана відповідь на важливе питання, яке стосується визначення вимог та умов практичного застосування симетричних та асиметричних криптографічних примітивів та протоколів взаємодії для побудови системи запобігання поширенню інфекційних захворювань з урахуванням результатів досліджень;

– показано, як повинні визначатись вимоги до організаційно-адміністративних та інженерно-технічних заходів безпеки, які забезпечують коректність використання та надійність засобів КЗІ, в яких реалізовано відповідні криптографічні алгоритми;

– розглянуті організаційно-адміністративні та інженерно-технічні заходи безпеки є складовою механізмів економічного стимулювання підключення до системи й активної взаємодії як звичайних громадян (що отримують інформацію у системі й розповсюджують її у визначених безпечних рамках), так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури. Механізми економічного стимулювання матимуть виключно добровільний характер з відсутністю будь-якої каральної складової. Кінцевою метою є охоплення системою переважної більшості суспільства із загальним позитивним сприянням;

– визначено, від яких саме параметрів цих симетричних та асиметричних алгоритмів залежить їх криптографічна стійкість, та сформулювали вимоги до області значень цих параметрів, за яких рівень стійкості алгоритмів є не нижче від заданого.

4. Запропоновані моделі моніторингу мережі та методу моніторингу трафіка в системі виявлення вторгнень можуть бути покладені в основу

математичного та алгоритмічно-програмного забезпечення існуючих та перспективних систем виявлення вторгнень, програмних моніторингових систем. Їх застосування на практиці призведе по підвищення як рівня якості обслуговування за показниками мережної продуктивності, так і рівня мережної безпеки.

5. Запропоновані моделі та методи безпечної маршрутизації можуть бути використані як для розв’язання задач аналізу стані інфокомунікаційних мереж щодо оцінки рівня якості обслуговування та мережної безпеки, так і задач синтезу – визначення порядку маршрутизації самоподібних потоків із забезпеченням заданих показників QoS та максимізацією рівня мережної безпеки. Отримані моделі та методи безпечної маршрутизації можуть бути використані при розробці та стандартизації перспективних протоколів маршрутизації як основа математичного та алгоритмічно-програмного забезпечення маршрутизаторів традиційних IP/MPLS-мереж, так і в серверів маршрутів або контролерів програмно-конфігурованих мереж (SDN).

6. Досліджені математичні моделі криптографічного захисту формально описують основні складові та основні застосовувані криптоперетворення з базовими криптографічними властивостями в залежності від параметрів та галузей їх практичного застосування. З цих базових моделей криптографічних примітивів будуються більш складні моделі, придатні для опису та дослідження сучасних криптографічних інструментів: шифрів, шифросистем, схем електронного цифрового підпису, криптографічних протоколів та систем правил, що регламентують використання криптографічних перетворень і алгоритмів в інформаційних процесах та інформаційно-комунікаційних системах. Отже, отримані результати дозволяють формалізувати процеси та вивчати певні характеристики криптографічного захисту інформації, в тому числі, персональних даних у засобах відстеження контактів. Їх практичне застосування дозволяє забезпечити фундаментальні властивості криптографічних примітивів, які в свою чергу використовуються для розробки більш складних об’єктів

(криптосистем та криптографічних протоколів) і які гарантують одне або декілька властивостей безпеки високого рівня.

7. Отримані результати з розробки та дослідження криптографічних примітивів та протоколів взаємодії при збиранні, зберіганні та розповсюдженні даних про контакти містять можливі альтернативи алгоритмів цифрових підписів, асиметричного шифрування, хешування та генераторів псевдовипадкових послідовностей, що можуть бути використанні для реалізації у системах моніторингу контактів. Для кожного з зазначених примітивів обґрунтовано застосування алгоритмів, які на сьогодні вважаються безпечними та ефективним. Крім того, для кожного з напрямків дослідження запропоновано нові схеми, що базуються на кодових криптосистемах, які вважаються стійкими до квантового криптоаналізу, оскільки їх безпечність спирається на складність вирішення NP-складної задачі синдромного декодування. Наведено результати порівняння ефективності запропонованих алгоритмів у порівнянні з відомими криптосистемами, які показують зазначені переваги за співвідношеннями стійкість/складність реалізації.

8. Отримані результати оцінки безпеки протоколів та криптографічних перетворень мають принципове значення для практичного розгортання моніторингових систем, систем оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини, сучасних та перспективних систем відстеженні контактів. Зокрема досліджено різні підходи до побудови подібних систем, заснованих як на централізованих так і на децентралізованих архітекторах. Централізовані системи засновані на обробці серверами додатків псевдонімів кожного користувача (унікальних псевдовипадкових ідентифікаторів), обробці та узагальненні інформації щодо анонімних ідентифікаторів, інформації про взаємодію, тощо. Однак централізовані архітектури мають суттєві недоліки з боку конфіденційності та можливостей централізованого відстеження контактів, що може бути використане для реінжинірингу особистої інформації про користувачів. У децентралізованих архітектурах користувачі мають більшу захищеність, зберігаючи особисту

інформацію, дані про контакти та зустрічі, які транслюють інші користувачі на мобільному пристрої, і завантажують ключі, які генерують анонімні ідентифікатори. Різні децентралізовані пропозиції мають приблизно схожі процеси, і конкретна відмінність відображається в різних алгоритмах створення анонімних ідентифікаторів. Отже практична цінність отриманих результатів виконання проєкту полягає в обґрунтуванні конкретних пропозицій та рекомендацій стосовно створення перспективних систем оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

9. Використання запропонованого методу моніторингу призводить до збільшення кількості проаналізованих пакетів за рахунок чого відсоток виявлених атак збільшується, зменшується середній час очікування пакетів на та зменшується кількість втрачених даних. Запропоновані методи виявлення вторгнень на основі машинного навчання можуть бути використані в системах виявлення вторгнень інфокомунікаційних мереж та при виявленні різного роду вторгнень. Їх застосування на практиці призведе до підвищення захищеності інформаційних ресурсів шляхом підвищення точності, швидкості та своєчасності виявлення вторгнень та ідентифікації атак.

Опис шляхів та способів подальшого використання результатів виконання Проєкту в суспільній практиці.

1. Отримані результати аналізу та класифікації відомих моделей, методів та алгоритмів КЗІ та протоколів взаємодії можуть бути використані при розробці моніторингових систем відстеження контактів в частині забезпечення конфіденційності, цілісності даних, підтвердження авторства тощо. та для побудови однорангової системи обробки даних у децентралізованих системах.

2. Застосування запропонованої дворівневої системи дозволить забезпечити безпечний обмін інформацією між локальними незалежними одноранговими системами, які організовані у блокчейни. Припустимо, що для зберігання локальної інформації (стосовно району, міста, області, тощо) використовуються багато різних незалежних однорангових систем, організованих у блокчейни. Ці блокчейни ми вважатимемо сайдчейнами з усіма

відповідними властивостями, зокрема з достатньо великою швидкістю виходу блоків. Щоб ці окремі децентралізовані системи могли безпечно взаємодіяти у плані обміну інформацією, над ними, вже на рівні держави, будується МС-блокчейн, єдиною функцією якого є створення своєчасних посилань на блоки всіх цих сайдчейнів. У такій моделі самостійність та децентралізованість локальних мереж не порушиться, а їхні блоки будуть вважатись стабільними при зазначених вище умовах.

3. Отримані результати обґрунтування вимог та умов практичного застосування криптографічних примітивів протоколів взаємодії можуть бути використані при розробці криптографічних складових системи запобігання поширенню інфекційних захворювань, механізмів економічного стимулювання підключення до системи й активної взаємодії звичайних громадян і повних вузлів.

4. Представлені математичні моделі моніторингу мережі та метод моніторингу трафіка програмно реалізовані мовою програмування Python та на рівні програмного прототипу можуть стати частиною перспективної системи моніторингу та системи виявлення вторгнень. Область застосування запропонованих моделей – телекомунікаційні мережі, які розгорнуті для взаємодії об’єктів критичної інфраструктури, що функціонують в умовах постійних загроз мережній безпеці. Це особливо важливо в умовах передачі конфіденційного трафіка або даних з обмеженим доступом.

5. Отримані в результаті виконання проєкту математичні моделі та методи безпечної маршрутизації, а такою їх програмні прототипи, виконані в середовищі MATLAB, доцільно використовувати при управлінні конфіденційним трафіком в умовах можливих загроз, вторгнень та реалізації вразливостей апаратно-програмного забезпечення комутаційного та серверного обладнання інфокомунікаційних мереж загального та спеціального призначення. Особливо це стосується мереж, які розгорнуті для забезпечення функціонування об’єктів критичної інфраструктури України, та мереж військового призначення.

6. Представлені математичні моделі криптографічного захисту в подальшому можуть бути застосовані як при проведенні пошукових досліджень з обґрунтування нових технологій криптографічного перетворення, механізмів та протоколів забезпечення безпеки персональних та інших даних, захист яких передбачено нормативно-правовими актами, так і для розробки навчально-методичних праць з викладення основних положень сучасної криптології. Зокрема, під час виконання проєкту дослідження окремі результати впроваджено впри викладенні навчальних курсів за дисциплінами: «Прикладна криптологія», «Теорія чисел, груп, полів, кілець», «Моделювання та оцінка ефективності засобів захисту інформації».

7. Отримані результати з розробки та дослідження криптографічних примітивів та протоколів взаємодії вже впроваджено при розробці та прототипуванні перспективних засобів криптографічного захисту інформації (акт впровадження в Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків). Зазначені результати будуть використані в подальшому при удосконаленні методів, моделей та механізмів криптографічного захисту інформації в інформаційних, комунікаційних та інформаційно-телекомунікаційних системах держави.

8. Отримані результати оцінки безпеки протоколів та криптографічних перетворень можуть бути використані в подальшому для практичного розгортання моніторингових систем, систем оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини, сучасних та перспективних систем відстеженні контактів.

9. Представлені методи моніторингу, швидкого та раннього виявлення вторгнень та ідентифікації мережних атак, виявлення фактів несанкціонованого доступу програмно реалізовані мовою Python та на рівні програмного прототипу можуть стати частиною систем виявлення вторгнень та систем виявлення аномалій. Область застосування запропонованих методів – інформаційні системи, які функціонують в умовах постійних загроз мережній безпеці. Це

особливо важливо в умовах передачі конфіденційного трафіка або даних з обмеженим доступом.

Висновки за заключним етапом

Опис наукових та науково-технічних результатів, отриманих в рамках виконання Проєкту (за окремими індикаторами виконання завдань).

1. Результати дослідження алгоритмів криптографічного захисту інформації та протоколів взаємодії в децентралізованому середовищі при побудові надійних та безпечних систем моніторингу запобігання поширення інфекційних захворювань.

Розглянуто основи функціонування симетричних криптосистем, базові перетворення, переваги та недоліки та способи реалізації у потокових та блочних перетвореннях. Можна зробити висновок, що блокові симетричні шифри знайшли широке застосування на практиці для вирішення задач забезпечення конфіденційності, цілісності, доступності, захисту від НСД тощо. Разом з тим, БСШ мають ряд недоліків, серед яких необхідно відмітити: достатньо велика складність перетворень при шифруванні, недостатня швидкодія прямих і зворотних криптоперетворень, можна говорити, що забезпечується середня швидкодія, складність, а в ряді випадків і неможливість розпараллелювання процесів крипто перетворень, всі блоки зашифровуються з використанням одного і того самого ключа тощо. Вирішення цього протиріччя покладається на потокові симетричні перетворення – потокові симетричні шифри. Необхідно відмітити, що зважаючи на вказані переваги потокових симетричних шифрів, на міжнародному рівні проведено та виконано ряд науково-практичних результативних проектів – Nessie, eSTREAM. І за результатами цього конкурсу визначено ряд алгоритмів, які можуть бути застосовані у практичних системах, у тому числі вони є ефективними при реалізації систем моніторингу контактів.

У той же час задля забезпечення конфіденційності, безпечності та інших функцій для користувачів систем моніторингу можуть бути застосовані асиметричні криптосистеми. Найбільшою особливістю асиметричних

перетворень є використання асиметричної пари ключів, які містить відкритий ключ, що відомий всім, та особистий ключ, що пов'язаний з відкритим ключем за допомогою певного математичного перетворення. При цьому вважається що обчислення особистого ключа, при знанні загальносистемних параметрів та відкритого ключа, повинно мати в гіршому випадку субекспоненційну складність, за умови коли обчислення відкритого ключа при формуванні асиметричної ключової пари – поліноміальну. Здійснено порівняння асиметричних та симетричних криптосистем з точки зору об'єму даних та безпечності, що вони забезпечують.

Досліджено криптографічні протоколи взаємодії, які можуть бути застосовані при взаємодії користувачів систем моніторингу. Особливістю криптопротоколів є те, що вони виконуються на основі застосування однієї або декількох криптосистем (криптоалгоритмів), відповідних ключових даних, параметрів і т. ін. В моделі взаємної недовіри взаємодіючі об'єкти та суб'єкти, які мають між собою інформаційні співвідношення мають бути захищені від обману, в тому числі, і юридично. Наведено рекомендації для реалізації різних протоколів автентифікації та розподілення таємниці з точки зору програмної імплементації та побудови систем моніторингу та інформування населення щодо епідеміологічної ситуації.

2. Концептуальні положення з розробки, аналізу та застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у системах моніторингу запобігання поширення інфекційних захворювань.

У розділі було розглянуто концептуальних положень стосовно застосування різних рішень щодо протоколів взаємодії та криптографічних перетворень у систем моніторингу запобігання поширення інфекційних захворювань.

Було запропоновано низка принципів:

– принцип контролю;
– принцип контролю обробки інформації;
– принцип мінімізації даних;

– принцип обмеження розкриття/доступу даних;
– принцип забезпечення точних цілей обробки;
– принцип встановлення жорстких обмежень на зберігання даних;
– принцип забезпечення даних;
– принцип забезпечення точності даних;
– принцип Залучення органів із захисту даних,

яким потрібно врахувати підчас розробки системи моніторингу інфекційних захворювань.

Було проаналізовані аспекти, які потрібно врахувати під час розробки подібної системи моніторингу, а саме – специфічні вразливості децентралізованого рішення на основі блокчейну, інструменти та методики для аналізу програмного коду; та запропоновані механізми захисту та інструменти/підходи моніторингу функціоналу рішення на основі блокчейну.

Також було розглянуто можливість створення дублюючої системи, як наступний крок після отримання досвіду створення децентралізованої системи на рівні держави дасть змогу виявити критичні місця та підготує базу для створення системи електронного голосування різних рівнів – від місцевих виборів до виборів президента України.

3. Науково-методичні рекомендації щодо практичного впровадження розроблених моделей, методів і протоколів безпечної маршрутизації конфіденційних повідомлень в сучасних та перспективних інфокомунікаційних мережах.

Проведено аналіз множини існуючих параметрів функціонування системи та мережі, який показав, що бажано зменшити кількість вхідних змінних як для зниження обчислювальної вартості моделі, так і для підвищення продуктивності моделі. Методи вибору функцій, засновані на статистиці, припускають оцінку зв’язку між кожною вхідною змінною та цільовою змінною за допомогою статистики і вибір тих вхідних змінних, які мають найтісніший зв’язок з цільовою змінною. Ці методи можуть бути швидкими і ефективними, хоча вибір статистичних заходів залежить від типу даних як вхідних, так і вихідних змінних.

Таким чином, при виборі функцій, заснованих на фільтрації, було обрано набір ознак для розробки методів моніторингу та виявлення вторгнень.

Оскільки в світі кіберзлочинів з'являються нові шаблони і класи атак, істотною вимогою є оновлення існуючих систем виявлення вторгнень згідно з новими шаблонами даних. Таке оновлення вимагає перепідготовки системи виявлення вторгнень з використанням нового набору даних поруч зі старим існуючим, які наведено в цій роботі. Наведено забезпечення своєчасного і економічно ефективного механізму поновлення, який зазначено як критичну вимогу під час розробки систем виявлення вторгнень.

Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак, що базується на хмарному підході є складовою дублюючої системи оповіщення населення про надзвичайні події у регіоні. Дані, які зібрано зберігаються та оброблюються в хмарному компоненті системи IDS, що дозволяє розвантажити кінцеві пристрої від необхідності виконувати складні обчислення. Функції пристроїв нижнього рівня обмежуються виділенням ознак мережного трафіку та виявленням аномалій. Пристрої повідомляють хмарному сервісу про виявлені аномалії та передають їх параметри для аналізу.

У розділі запропоновано та досліджено два методи безпечної маршрутизації, які можуть бути використані при фрагментованій передачі конфіденційних повідомлень в інфокомунікаційній мережі (ІКМ). Перший метод заснований на розрахунку та використанні шляхів, які не перетинаються, та є подальшим узагальненням механізму безпечної маршрутизації SPREAD. В основу запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, покладено послідовне розв'язання двох оптимізаційних задач:

- розрахунку маршрутів, що не перетинаються, в інфокомунікаційній мережі за допомогою моделі (4.1)-(4.8);
- безпечного балансування фрагментів конфіденційного повідомлення (4.9)-(4.14) за множиною попередньо розрахованих шляхів (4.1)-(4.8).

Модель (4.1)-(4.8) обрана для використання з причини її корисних властивостей щодо розрахунку максимальної кількості шляхів, що не перетинаються, із включенням у них каналів зв’язку з мінімальною ймовірністю компрометації. Модель (4.9)-(4.14) використана з метою забезпечення мінімально можливої ймовірності компрометації повідомлень (4.13), які фрагментовано передавались за попередньо розрахованою множиною шляхів, що не перетинались.

Результати проведеного дослідження на обраній мережній конфігурації (рис. 4.2) для трьох різних варіантів ймовірностей компрометації каналів зв’язку ІКМ (рис. 4.3 – рис. 4.5) підтвердили ефективність запропонованого методу безпечної маршрутизації та працездатність закладених в його основу оптимізаційних моделей щодо визначення множини шляхів, що не перетинались, та порядку безпечного балансування за ними фрагментів конфіденційного повідомлення (табл. 4.4). Використання запропонованої оптимізаційної моделі розрахунку шляхів, які не перетинаються, з врахуванням їх рівня мережної безпеки в межах запропонованого методу безпечної маршрутизації дозволила знизити ймовірність компрометації конфіденційних повідомлень в залежності від сценарію компрометації елементів мережі від 23-27% до 47-56%.

Запропоновано метод безпечної маршрутизації конфіденційних повідомлень, заснований на використанні шляхів, які можуть перетинатись. Це дозволяє більш повно використати наявний в мережі ресурс щодо пропускної здатності та кіберресурс. В межах даного методу ймовірність компрометації повідомлень розраховується за формулою повної ймовірності з врахуванням рівня мережної безпеки «містків» у структурі ІКМ. Метод не вимагає попереднього розрахунку множини шляхів, які не перетинаються, що спрощує його реалізацію на практиці.

Як показали результати дослідження запропонованого методу, найбільший виграш щодо значень ймовірність компрометації повідомлень (у середньому від 20-60%) вдалося отримати в умовах відносно невисокого рівня кіберзагроз у ІКМ, тобто коли ймовірність компрометації каналів (вузлів) зв’язку не

перевищувала 0,4. При збільшенні рівня загроз, коли ймовірність компрометації каналів (вузлів) зв'язку збільшувалась до 0,7, виграш щодо значень ймовірність компрометації повідомлень складав у середньому від 3-20%.

В межах запропонованих методів рівень мережної безпеки маршрутів, мережі та конфіденційних повідомлень взагалі оцінювався через ймовірність компрометації каналів зв'язку ІКМ. За необхідності врахування рівня мережної безпеки вузлів (маршрутизаторів) ІКМ вони можуть бути логічно представлені віртуальними каналами зв'язку, які мають вузлову ймовірність компрометації, без зміни змісту запропонованих методів безпечної маршрутизації конфіденційних повідомлень.

Представлені методи безпечної маршрутизації конфіденційних повідомлень отримали програмну реалізацію та представлені програмними прототипами протоколів безпечної маршрутизації у середовищі MATLAB та Python. Ці прототипи можу стати основою перспективних протоколів маршрутизації з підтримкою метрик мережної безпеки для подальшого застосування в традиційних IP/MPLS-мережах та програмно-конфігурованих мережах.

Перспективи подальших досліджень в області безпечної маршрутизації в інфокомунікаційній мережі пов'язані з урахуванням не тільки ймовірності компрометації каналів зв'язку, але й інших важливих показників мережної безпеки.

4. Обґрунтовані пропозиції з практичної реалізації запропонованих криптографічних примітивів та протоколів взаємодії для відомих застосувань і нових систем відстеження контактів, обробки деперсоналізації даних.

Наведено основну ідею стосовно використання кільцевих підписів та безпосередньої анонімної атестації для побудови протоколів моніторингу та інформування населення, які дозволяють максимально зберігати анонімність користувачів. Зокрема, було наведено огляд робіт стосовно кільцевого підпису та безпосередньої анонімної атестації, розглянуто кілька варіантів побудови алгоритмів кільцевого підпису та запропоновано новий, що має суттєві переваги.

На прикладах детально розглянуто, як працюють ці алгоритми для кожного варіанту підпису.

Встановлено, що на даний час основною проблемою, пов'язаною зі складністю використання кільцевих підписів, є їх довжина. Так, в загальному випадку вона є пропорційною розміру кільця. Тому кільцеві підписи не є ефективними для кільця великого розміру, що обмежує їх анонімність. Існують певні способи зменшення розміру кільцевого підпису, але вони можуть бути застосовані лише для окремих випадків. Тому актуальним на сьогодні є напрямок подальших досліджень, пов'язаний зі зменшенням довжини кільцевого підпису.

Показано, як наведені криптографічні механізми дозволяють підтверджувати валідність інформації стосовно певної особи, зберігаючи при цьому її анонімність та, за необхідності, не розкриваючи деталі цієї інформації.

5. Обґрунтовані пропозиції з практичної реалізації систем зберігання та поширення інформації у децентралізованих середовищах.

Показано, як на базі сайдчейнів з Latus-консенсусом та zk-SNARK-доведеннями можна створити зручний децентралізований блокчейн, який дозволяє залучити багатьох незалежних користувачів до обробки та розповсюдження інформації у блокчейні.

Удосконалено умови функціонування повністю децентралізованих сайдчейнів на основі протоколу консенсусу Latus, що дозволило частково вирішити існуючи проблеми та створити специфічні моделі, наприклад, розподіли ймовірностей на частково впорядкованих множинах, які найбільше підходять для сучасних цілей.

Особливістю цієї роботи є деякі гіпотези, які були сформульовані на основі великої кількості чисельних результатів, отриманих за допомогою обчислень нескінченної точності. Чисельні результати дозволяють вибрати правильні значення деяких параметрів для досягнення стабільності та високої пропускної здатності в сайдчейнах.

6. Розробка рекомендацій щодо створення інфраструктури системи моніторингу, раннього виявлення вторгнень та ідентифікації атак різного типу, виявлення фактів несанкціонованого доступу та несанкціонованих користувачів.

Підсистема моніторингу, виявлення вторгнень та ідентифікації мережних атак, що базується на хмарному підході машинного навчання є складовою дублюючої системи оповіщення населення про надзвичайні події у регіоні. Завдяки застосуванню хмарного рішення вдалось розв’язати завдання моніторингу, виявлення вторгнень та ідентифікації мережних атак для кінцевих пристроїв системи з обмеженими ресурсами. Хмарний компонент системи IDS використовується, щоб розвантажити кінцеві пристрої від необхідності виконувати складні обчислення моделі машинного навчання. Кінцеві пристрої отримують оновлену інформацію про параметри IDS від хмарного MaaS. У цьому випадку функції пристроїв нижнього рівня обмежуються виділення ознак мережевого трафіку та виявленням аномалій. Пристрої повідомляють хмарному сервісу про виявлені аномалії та передають їх параметри для аналізу та навчання моделі.

Набув подальшого розвитку метод виявлення вторгнень на основі аналізу сигнатур, який враховує дані глибокого аналізу пакетів та рейтингування бази сигнатур.

Метод аналізу сигнатур, який використовує глибокий аналіз пакетів для аналізу вмісту трафіка та ідентифікує 93% атак, має низьку кількість хибнопозитивних спрацьовувань (менше 8%).

Розроблено комплексний метод виявлення вторгнень, який базується на використанні алгоритму аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Це дозволяє підвищити як достовірність, так і точність виявлення вторгнень, та уможливлює раннє виявлення вторгнень в широкому діапазоні кібератак на систему.

Проведено порівняльний аналіз роботи комплексного методу, який показав високу точність ідентифікації атак при різній інтенсивності трафіка.

Комплексний метод показав більш високу точність ідентифікації атак (більше 98%), на відміну від існуючих. Залежно від необхідного рівня ідентифікації атак можна прискорити роботу комплексного методу шляхом зміни порогових значень виявлення.

7. Опис підходу щодо побудови прототипів протоколів безпечної маршрутизації конфіденційних повідомлень в інфокомунікаційних мережах.

Розроблено рекомендації щодо практичної реалізації результатів проєкту, які стосуються впровадження запропонованих моделей та методів безпечної маршрутизації в ІКМ. Рекомендації базуються на результатах дослідження запропонованих рішень. Виконання рекомендацій передбачає проведення комплексу організаційно-технічних заходів, спрямованих на забезпечення ефективного функціонування ІКМ на основі запропонованих принципів структурно-топологічної, технологічної та алгоритмічно-програмної реалізації.

Запропоновані математичні моделі та обчислювальні методи безпечної маршрутизації можуть знайти своє практичне застосування в сучасних та перспективних інфокомунікаційних мережах (ІКМ). В традиційних IP/MPLS-мережах запропоновані моделі та методи мають стати основою математичного та алгоритмічно-програмного забезпечення маршрутизаторів та використовуватись при розрахунку та формуванні маршрутних таблиць. В залежності від топології мережі, її завантаженості та вимог щодо рівня якості обслуговування та мережної безпеки запропоновані рішення можуть базуватись на використанні маршрутних метрик, концепції Traffic Engineering. Для підвищення рівня кіберстійкості ІКМ в межах реалізації реактивного підходу запропоновані моделі та методи можуть бути використані для швидкої безпечної перемаршрутизації із реалізацією схем захисту вузла, каналу або маршруту.

При реалізації запропонованих рішень в програмно-конфігурованих мережах розроблені моделі та методи безпечної маршрутизації можуть стати основою алгоритмічно-програмного забезпечення SDN-контролерів, які здійснюють управління інформаційним обміном в межах певного мережного сегмента або домену.

При реалізації запропонованих у межах проєкту моделей та методів безпечної маршрутизації в безпроводових мережах, які самоорганізуються (MANET), рішення можуть стати основою алгоритмічно-програмного забезпечення мережних вузлів, які в залежності від стану мережі виконуються функції термінального пристрою, точки доступу, маршрутизатора та/або сервера послуг. Запропоновані рішення в MANET можуть використовуватись як для безпечної маршрутизації трафіка користувачі, так і для передачі конфіденційних даних і секретів.

9. Серія наукових публікацій (із залученням молодих вчених) за результатами проведених досліджень в фахових наукових та міжнародних індексованих виданнях.

Результати досліджень авторського колективу за результатами виконання проєкту викладені в ряді монографій та наукових публікаціях наведених у Додатку А (підрозділи А.1 та А.2) до звіту.

10. Виступи (із залученням молодих вчених) на міжнародних наукових конференціях та семінарах (в тому числі англійською) з публікацією доповідей (в тому числі у індексованих виданнях).

Перелік тез доповідей авторського колективу за результатами виконання проєкту наведені у Додатку А (підрозділ А.3) до звіту.

11. Наукові, навчальні та методичні матеріали для впровадження отриманих результатів до начального процесу.

Перелік патентів України, наукових, навчальних та методичних матеріалів авторського колективу за результатами виконання проєкту наведені у Додатку А (підрозділи А.4 та А.5) до звіту.

12. Захист дисертаційних робіт на основі отриманих наукових результатів дослідження.

Перелік дисертаційних робіт, які були виконані авторами проекту або під їх керівництвом та у рамках виконання проєкту наведені у Додатку А (підрозділи А.7 та А.8) до звіту.

Обґрунтування переваг науково-технічної продукції у порівнянні з існуючими аналогами.

1. За результатами виконання Проєкту була отримана наступна науково-технічна продукція: програмно реалізовані мовою Python на рівні програмного прототипу методи обробки та вибору ознак трафіку, методи аналізу протоколів, що базуються на засобах машинного навчання та фрактального аналізу.

2. Запропоновані методи аналізу протоколів, вибору ознак, характеристик та оцінок систем виявлення вторгнень мають наступні переваги у порівнянні з існуючими аналогами:

– запропоновані характеристики систем виявлення вторгнень, на відміну від існуючих, мають враховують дані глибокого аналізу пакетів;

– запропоновані методи аналізу протоколів з відстеженням стану, на відміну від існуючих дозволяє датчику знаходити кореляції між різними подіями протягом сеансу, ідентифікуючи атаки з кількома компонентами;

– запропонований вибір оптимальної сукупності ознак оцінки інформаційної системи на відміну від існуючих дає найбільш ефективне і точне розпізнавання вторгнень;

– запропоновано єдину оцінку стану інформаційної системи на основі даних, що збираються в мережі, що надає можливість збору, аналізу та систематизації статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи.

3. Запропоновані методи безпечної маршрутизації конфіденційних повідомлень мають наступні переваги у порівнянні з існуючими аналогами:

– більш повно враховують особливості нерегулярної топології сучасних інфокомунікаційних мереж з точки зору визначення та використання як множини шляхів, які не перетинаються, так і множин шляхів, які перетинаються;

– забезпечують розрахунок множини найбільш ефективних з точки зору мережної безпеки шляхів, які не перетинаються, а не базуються на попередньо заданій подібній множині шляхів;

– забезпечують більш ефективне використання доступного мережного ресурсу з точки зору його пропускної здатності та кібернадійності каналів та вузлів зв’язку, які можуть входити до шляхів, які перетинаються.

4. Представлено новий алгоритм кільцевого підпису, який має наступні переваги:

– суттєво менша довжина підпису та час роботи алгоритму, у порівнянні з тими алгоритмами, що використовують функцію типу RSA;

– суттєво вища стійкість, у порівнянні з тими алгоритмами, що використовують функцію типу RSA;

– вдвічі менша довжина ключа та у стільки ж менший обсяг обчислень у порівнянні з іншими алгоритмами, що використовують операцію спарювання.

4. Протокол консенсусу Latus дозволяє всім зацікавленим сторонам одночасно брати участь у процесі генерації одного блоку. Це посилює децентралізацію, але й вимагає створення складніших протоколів взаємодії між лідером блоку та обчислювачами, а також вибору параметрів цих протоколів та обґрунтування їх коректності та надійності. Чисельні результати, отримані в роботі, дозволяють вибрати правильні значення деяких параметрів для досягнення стабільності та високої пропускної здатності в сайдчейнах.

5. За результатами виконання Проєкту була отримана наступна науково-технічна продукція: програмно реалізовані мовою Python на рівні програмного прототипу методи виявлення вторгнень на основі аналізу сигнатур, на основі аномалій в поведінці (зміні стану) мережі та на основі аналізу протоколів, що базуються на засобах машинного навчання та фрактального аналізу, комплексний метод виявлення вторгнень.

6. Запропоновані методи моніторингу та виявлення вторгнень та ідентифікації атак в системах виявлення вторгнень мають наступні переваги у порівнянні з існуючими аналогами:

– запропонований метод сигнатурного аналізу виявлення вторгнень, на відміну від існуючих, має модуль глибокого аналізу пакетів та рейтингування бази даних сигнатур;

– запропонований комплексний метод виявлення вторгнень та ідентифікації атак носять системний (комплексний) характер. Проактивність рішень забезпечується використанням методів виявлення вторгнень заснованих на статистичних характеристиках трафіка та поведінкових характеристиках трафіка та системи, що забезпечує комплексний аналіз даних як трафіка, так і зміни в поведінці системи;

– в процесі виявлення вторгнень та атак, за допомогою комплексного методу виявлення вторгнень враховувались статистичні, рекурентні та мультифрактальні характеристики трафіка. Це дозволяє виявити атаки нульового дня, аномалії в поведінці користувачів та мережі, ідентифікувати тип атак, а також збільшити ймовірність ефективного виявлення вторгнень, ніж в існуючих методах.

– використання обраних ознак поведінки мережі й користувачів та застосування запропонованих методів виявлення вторгнень на основі сигнатурного аналізу з глибоким аналізом пакетів та комплексного методу виявлення вторгнень дозволяє виконати раннє виявлення вторгнень та ідентифікувати тип мережних атак.

Практична цінність отриманих результатів реалізації Проєкту для економіки та суспільства.

1. Запропоновані методи збору, аналізу та систематизації статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи можуть бути використані в системах виявлення вторгнень інфокомунікаційних мереж та при виявленні різного роду вторгнень. Використання розроблених та запропонованих рішень щодо призведе до зменшення часу аналізу даних, середнього часу очікування системи, підвищення точності та продуктивності систем виявлення вторгнень. Сукупність запропонованих рішень знижує зловмисний інформаційний вплив на суспільство.

2. Результати проведеного дослідження для трьох різних варіантів ймовірностей компрометації каналів зв’язку ІКМ підтвердили ефективність

запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що не перетинаються, та працездатність закладених в його основу оптимізаційних моделей щодо визначення множини шляхів, що не перетинались, та порядку безпечного балансування за ними фрагментів конфіденційного повідомлення. Використання запропонованої оптимізаційної моделі розрахунку шляхів, які не перетинаються, з врахуванням їх рівня мережної безпеки в межах запропонованого методу безпечної маршрутизації дозволила знизити ймовірність компрометації конфіденційних повідомлень в залежності від сценарію компрометації елементів мережі від 23-27% до 47-56%.

3. Як показали результати дослідження запропонованого методу безпечної маршрутизації конфіденційних повідомлень за шляхами, що перетинаються, найбільший виграш щодо значень ймовірність компрометації повідомлень (у середньому від 20-60%) вдалося отримати в умовах відносно невисокого рівня кіберзагроз у ІКМ, тобто коли ймовірність компрометації каналів (вузлів) зв’язку не перевищувала 0,4. При збільшенні рівня загроз, коли ймовірність компрометації каналів (вузлів) зв’язку збільшувалась до 0,7, виграш щодо значень ймовірність компрометації повідомлень складав у середньому від 3-20%.

4. Запропоновані методи безпечної маршрутизації можуть бути покладені в основу математичного та алгоритмічно-програмного забезпечення існуючих та перспективних маршрутизаторів IP/MPLS-мереж, серверів маршрутів та контролерів програмно-конфігурованих мереж. Їх застосування на практиці призведе по підвищення як рівня мережної безпеки за ймовірністю компрометації повідомлень особливо в умовах сильно зв’язних структур інфокомунікаційних мереж.

5. Наводяться протоколи взаємодії для системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань.

6. Запропоновані протоколи взаємодії будуть забезпечувати максимальну децентралізацію системи, а механізми економічного стимулювання матимуть виключно добровільний характер з відсутністю будь-якої каральної складової.

7. Запропоновані методи виявлення вторгнень можуть бути використані в системах виявлення вторгнень інфокомунікаційних мереж та при виявленні різного роду вторгнень. Використання розроблених та запропонованих рішень щодо моніторингу, виявлення вторгнень та ідентифікації атак призведе до підвищення кількості, швидкості, точності та продуктивності систем раннього виявлення атак, зменшить середній час очікування пакетів та кількість втрачених даних та, як результат, збільшить захищеність інформаційних ресурсів та даних, що передаються інфокомунікаційними мережами. Останнє забезпечує безпечну життєдіяльність суспільства та унеможливлює зловмисний інформаційний вплив на нього, що є актуальним в умовах все більш глибокого та повсюдного впровадження інформаційних систем у життя людства та все зростаючих загроз інформаційній безпеці, зокрема зі сторони недружніх для України держав.

Опис шляхів та способів подальшого використання результатів виконання Проєкту в суспільній практиці.

1. Розроблені та запропоновані методи збору, аналізу та систематизації статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи можуть бути використані в системах моніторингу, виявлення вторгнень та ідентифікації атак, як частина дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини, на створення якої спрямований цей Проект, можуть використовуватися в складі підсистем виявлення та запобігання вторгнень інших інформаційних систем.

2. Представлені методи безпечної маршрутизації конфіденційних повідомлень отримали програмну реалізацію та представлені програмними прототипами протоколів безпечної маршрутизації у середовищі MATLAB та Python. Ці прототипи можу стати основою перспективних протоколів маршрутизації з підтримкою метрик мережної безпеки для подальшого

застосування в традиційних IP/MPLS-мережах та програмно-конфігурованих мережах.

3. Використовуючи наведені механізми кільцевих підписів та БАА, можна побудувати відповідні протоколи моніторингу епідеміологічної ситуації з максимальним забезпеченням анонімності, які дають можливість:

– надавати інформацію з підтвердженням відповідної обізнаності, але без розкриття особи, яка цю інформацію надає;

– підтверджувати валідність дій якоїсь особи, або підтверджувати дозволи, їй надані, без розкриття іншої інформації стосовно цієї особи.

У першому випадку застосовується алгоритм кільцевого підпису, у другому – механізми БАА.

4. Запропоновано протоколи взаємодії для використання у системах зберігання та поширення інформації у децентралізованих середовищах із застосуванням механізмів економічного стимулювання підключення до системи й протоколи активної взаємодії як звичайних громадян (що отримують інформацію у системі й розповсюджують її у визначених безпечних рамках), так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури.

5. Розроблені та запропоновані методи моніторингу, виявлення вторгнень та ідентифікації атак, як частина дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини, на створення якої спрямований цій Проект, можуть використовуватися в складі підсистем виявлення та запобігання вторгнень інших інформаційних систем, де циркулює конфіденційний трафік або дані з обмеженим доступом. Також запропоновані рішення з моніторингу, виявлення вторгнень та ідентифікації атак слід використовувати в мережах IoT, системах віддаленого управління, зокрема в системах, що відносяться до критичної інфраструктури, які функціонують в умовах постійних загроз мережній безпеці.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Блінов А. Вірус рецесії: чим обернеться епідемія COVID19 і хто постраждає найбільше. [Електронний ресурс] - URL: https://www.slovoidilo.ua/2020/03/18/pogljad/ekonomika/virus-recesiyi-chymobernetsya-epidemiya-covid-19-xto-postrazhdaye-najbilshe
2. А. Менезис, П. Ван Аршот, С. Ватсон. Руководство по прикладной криптографии CRC Press, 1997, электронная копия, 662 с
3. Брюс Шнайер. Прикладная криптография. М., изд. Триумф. 2002 г., -797 с.
4. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , -593с.
5. Іванов М.А., Чугунков І.В. Криптографічні методи захисту інформації в комп'ютерних системах та мережах. – М.: НИЯУ МИФИ, 2012. – 400 с.
6. Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg.–245 p.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.
8. Bellare M. Symmetric encryption. [Електронний ресурс] - URL: https://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf (last accessed: 18.11.2018).
9. Олійников Р.В. Методи аналізу і синтезу перспективних симетричних криптографічних перетворень. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – ЗАХИСТ ІНФОРМАЦІЇ, ТОМ 17, №2, КВІТЕНЬ-ЧЕРВЕНЬ 2015 154 Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2014.
10. New European Schemes for Signatures, Integrity, and Encryption (NESSIE), IST-1999-12324. [Електронний ресурс] - URL: https://www.cosic.esat.kuleuven.be/nessie.
11. Мао, В. Современная криптография: теория и практика. : Пер. с английского. М.: Издательский дом «Вильямс», 2005. — 768 с.

12. Горбенко, Іван Дмитрович. Прикладна криптологія: Монографія / Горбенко І.Д., Горбенко Ю.І.: видання 2-ге. - Харків : Форт, 2012. - 868 с.
13. Горбенко, Юрій Іванович Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія / Горбенко Юрій Іванович ; за заг. ред. д-ра техн. наук, проф. Горбенка Івана Дмитровича ; Харків. нац. ун-т ім. В. Н. Каразіна, Приват. т-во "Ін-т інформ. технологій". - Харків : Форт, 2015.
14. Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems (англ.) // Commun. ACM — NYC, USA: ACM, 1978. — Vol. 21, Iss. 2. — P. 120—126.
15. Горбенко Ю. І. Сутність та необхідність виконання додаткових вимог відносно надання довірчих послуг в ЄС та Україні в період 2015 – 2030 рр. / Ю. І. Горбенко // Радиотехника. - 2014. - Вип. 176. - С. 145-152. - Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2014_176_22
16. Schnorr C.P. Efficient Signature Generation by Smart Cards. — J. Cryptology, 1991. — С. 161—174.
17. Schnorr C.P. Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO’89. Lecture Notes in Computer Science 435. - 1990. - С. 239-252.
18. Шнайер Б. 23.2 Алгоритмы разделения секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 588—591. — 816 с.
19. Pasailă D., Alexa V., Iftene S. Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes (англ.) // International Journal of Computing — 2010. — Vol. 9, Iss. 2. — P. 107—117.
20. Закон України про захист персональних даних https://zakon.rada.gov.ua/laws/show/2297-17#Text
21. General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
22. PEPP-PT License. GitHub. 2020-04-19. Retrieved 2020-04-22.

23. Smartphone Market Share https://www.idc.com/promo/smartphone-market-share
24. Google can't fix the Android update problem https://www.theverge.com/2019/9/4/20847758/google-android-update-problem-pie-q-treble-mainline
25. The eHealth network was set up by the European Commission under article 14 of Directive 2011/24/EU. https://ec.europa.eu/commission/presscorner/detail/en/IP_11_1589
26. EN ENEUROPEAN COMMISSION Brussels, 8.4.2020 RECOMMENDATION https://ec.europa.eu/info/sites/default/files/recommendation_on_apps_for_contact_tracing_4.pdf
27. European Commission recommendation of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data.
28. European Commission guidance of 16 April 2020 on apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN
29. European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (P9_TA(2020)0054) https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html
30. . Alharby, A. Aldweesh, and A. v. Moorsel. 2018. Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018). In 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB).
31. Proof-of-Work» Proves Not to Work, 2004 «If we try to make it uneconomic to send spam then we must restrict senders to 1,750 messages a day» https://www.cl.cam.ac.uk/~rnc1/proofwork.pdf

32. «Proof-of-Stake Algorithmic Methods: A Comparative Summary». Social Science Research Network (SSRN). 11-03-2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131897
33. Rüdiger Schollmeier, A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications, Proceedings of the First International Conference on Peer-to-Peer Computing, IEEE (2002).
34. Offner, Carl. "Notes on Graph Algorithms Used in Optimizing Compilers" (PDF). Retrieved 13 April 2018.
35. Milewski, Robert; Govindaraju, Venu (31 March 2008). "Binarization and cleanup of handwritten text from carbon copy medical form images". Pattern Recognition. 41 (4): 1308–1315. doi:10.1016/j.patcog.2007.08.018. Archived from the original on 10 September 2020.
36. IoT - Smart Contract Rule Based Secure Communication Scheme for Healthcare System. EasyChair Preprint №1802. October 31, 2019
37. Harrand, Nicolas; Soto-Valero, Cesar; Monperrus, Martin; Baudry, Benoit (2019). "The Strengths and Behavioral Quirks of Java Bytecode Decompilers". 19th International Working Conference on Source Code Analysis and Manipulation (SCAM). IEEE: 92–102. arXiv:1908.06895. Bibcode:2019arXiv190806895H. doi:10.1109/SCAM.2019.00019. ISBN 978-1-7281-4937-0. S2CID 201070711.
38. Reverse Compilation Techniques (PDF) (PhD thesis). Queensland University of Technology. Archived (PDF) from the original on 2016-11-22. Retrieved 2019-12-21.)
39. Fuzz Testing of Application Reliability". University of Wisconsin-Madison. Retrieved 2020-12-30.
40. New Directions in Cryptography W. Diffie and M. E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644—654.
41. Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A.A. (2018). A Detailed Analysis of the CICIDS2017 Data Set. ICISSP.
42. Intrusion Detection Evaluation Dataset (CIC-IDS2017) URL: https://www.unb.ca/cic/datasets/ids-2017.html

43. UGR'16: A New Dataset for the Evaluation of Cyclostationarity-Based Network CBBs. [online]. Режим доступу: https://nesg.ugr.es/nesg-ugr16/

44. Özgür A., Erdem H. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ PrePrints. 2016. Vol. 4. P. e1954v1. DOI:10.7287/peerj.preprints.1954v1

45. Al-Kasassbeh M., Al-Naymat G., Al-Hawari E. Towards generating realistic SNMP-MIB dataset for network anomaly detection. International Journal of Computer Science and Information Security. 2016. Vol. 14, No. 9. P.1162–1185.

46. Ageyev D., Mohsin A., Radivilova T., Kirichenko L. Infocommunication Networks Design with Self-Similar Traffic. The Experience of Designing and Application of CAD Systems (CADSM): Proceedings of 2019 IEEE 15th International Conference, 2019, Polyana, Ukraine. IEEE, 2019. P. 24–27. DOI: 10.1109/CADSM.2019.8779314.

47. Ageyev D., Bondarenko O., Radivilova T., Alfroukh W. Classification of existing virtualization methods used in telecommunication networks. Dependable Systems, Services and Technologies (DESSERT): Proceedings of 2018 IEEE 9th International Conference, Kiev, Ukraine. IEEE, 2018. P. 83–86. DOI: 10.1109/DESSERT.2018.8409104.

48. Stojanović B., Hofer-Schmitz K., Kleb U. APT datasets and attack modeling for automated detection methods: A review. Computers & Security, Volume 92, 2020, 101734. Doi: https://doi.org/10.1016/j.cose.2020.101734.

49. T. Radivilova, K. Lyudmyla, O. Lemeshko, D. Ageyev, M. Tawalbeh and A. Ilkov, "Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 819-822, doi: 10.1109/PICST51311.2020.9467973.

50. V. Chandola, A. Banerjee, V. Kumar, “Anomaly Detection: A Survey,” ACM Computing Survey, vol. 41, pp.1–58, 2009.

51. K. Sheridan, T. G. Puranik, E. Mangortey, O. J. Pinon-Fischer, M. Kirby, D.N. Mavris, “An application of dbscan clustering for flight anomaly detection during

the approach phase," Scitech 2020 Forum (AIAA), 2020, pp. 1851. https://doi.org/10.2514/6.2020-1851

52. D. Ageyev, T. Radivilova and O. Mohammed, "Traffic Monitoring and Abnormality Detection Methods Analysis," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 823-826, doi: 10.1109/PICST51311.2020.9468103.
53. Kirichenko L., Radivilova T., Bulakh V. Machine Learning in Classification Time Series with Fractal Properties. Data. 2019. Vol. 4, iss. 1, 5. P. 1–13. DOI:10.3390/data4010005 8632010.
54. Mulesa, O., Povkhan, I., Radivilova, T., Baranovskyi, O. (2021). Development of the method of construction of the optimal model of time series forecasting on the basis of the principle of competition. Eastern-European Journal of Enter-prise Technologies, 5 (4 (113)), 6–11. doi: https://doi.org/10.15587/1729-4061.2021.240847
55. Kumar, V., Sinha, D. A robust intelligent zero-day cyber-attack detection technique. Complex Intell. Syst. 7, 2211–2234 (2021). https://doi.org/10.1007/s40747-021-00396-9
56. Lyudmyla Kirichenko, Abed Saif Ahmed Alghawli, Tamara Radivilova. Generalized Approach to Analysis of Multifractal Properties from Short Time Series. International Journal of Advanced Computer Science and Applications(IJACSA), Volume 11 Issue 5, 2020. P.183-198. doi: 10.14569/IJACSA.2020.0110527
57. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(11), 2021, 183-194. https://doi.org/10.28925/2663-4023.2021.11.183194.
58. Ageyev, D., Radivilova, T. Traffic monitoring and abnormality detection methods for decentralized distributed networks, CEUR Proceedings Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Vol. 2923, 2021, pp. 283–288

59. Khan M. A., Karim M. R., Kim Y. A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network. Symmetry. 2019. Vol. 11, P. 581-585. DOI: 10.3390/sym11040583
60. Sharafaldin, I., Habibi Lashkari, A., Hakak, S., & Ghorbani, A.A. (2019). Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. 2019 International Carnahan Conference on Security Technology (ICCST), 1-8.
61. Kaur R., Kashmira P., Meena K., Mohapatra A. K. Survey on Different Techniques of Threshold Cryptography. Journal of Electronics and Communication Engineering (IOSR-JECE). 2017. P. 114–119.
62. Venukumar V., Pathari V. A survey of applications of threshold cryptography – proposed and practiced. Information Security Journal: A Global Perspective. 2016. Vol. 25, No. 4–6. P. 180–190. DOI: 10.1080/19393555.2016.1251996.
63. Sarma K.S., Lamkuche H.S., Umamaheswari S. A Review of Secret Sharing Schemes. Research Journal of Information Technology. 2013. Vol. 5. P. 67–72. DOI: 10.3923/rjit.2013.67.72.
64. Lou W., Kwon Y. H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks. IEEE Transactions on Vehicular Technology. 2006. Vol. 55, No. 4. P. 1320–1330. DOI: 10.1109/TVT.2006.877707.
65. Lou W., Liu W., Fang Y. SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks. INFOCOM 2004: Proceedings of the Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies. Hong Kong, China, 7–11 March, 2004. IEEE, 2004. P. 2404–2413. DOI: 10.1109/INFCOM.2004.1354662.
66. Gupta D., Segal A., Panda A., Segev G., Schapira M., Feigenbaum J., Rexford J., Shenker S. A new approach to interdomain routing based on secure multi-party computation. Hot Topics in Networks: Proceedings of the 11th ACM Workshop. October, 2012. ACM, 2012. P. 37–42. DOI: 10.1145/2390231.2390238.

67. Gharib, M., Yousefizadeh, H., Movaghar, A. (2018), “Secure Overlay Routing for Large Scale Networks”, IEEE Transactions on Network Science and Engineering, No. 1, P. 1-12. DOI: https://doi.org/10.1109/TNSE.2018.2812830
68. Лемешко, О. В., Єременко, О. С., Невзорова, О. С. (2020), Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість, Харків: ХНУРЕ, 308 с.
69. Євдокименко, М. О., Шаповалова, А. С., Шаповал, М. М. (2020), “Потокова модель маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей”, Проблеми телекомунікацій, No. 1(26), С. 48-62. Режим доступу: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf
70. Снегуров А.В., Чакрян В.Х. Метод формирования метрик маршрутизации, основанный на рисках информационной безопасности. Системи управління, навігації та зв’язку. 2012. № 4(24). С. 105–110.
71. Snihurov, A., Chakrian, V. (2015), “Improvement of EIGRP Protocol Routing Algorithm with the Consideration of Information Security Risk Parameters”, Scholars Journal of Engineering and Technology, No. 3(8), P. 707-714.
72. Lemeshko, O., Yeremenko, O., Persikov, A., Vavenko, T. (2018), “Mathematical Model of Calculating the Maximum Number of Disjoint Paths in Secure Routing”, Proceedings of the 2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, Ukraine, 10-14 September, P. 1–4. DOI: https://doi.org/10.1109/UkrMiCo43733.2018.9047581
73. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B. (2019), “Enhanced Solution of the Disjoint Paths Set Calculation for Secure QoS Routing”, Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 18-20 December, P. 210-213. DOI: https://doi.org/10.1109/ATIT49449.2019.9030520
74. Lemeshko, O., Yeremenko, O., Sleiman, B., Yevdokymenko, M. (2020), “Fast ReRoute Model with Realization of Path and Bandwidth Protection Scheme in

SDN”, Advances In Electrical And Electronic Engineering, No. 18(1), P. 23-30. DOI: https://doi.org/10.15598/aeee.v18i1.3548

75. Лемешко, А. В., Еременко, А. С. (2015), “Усовершенствование модели безопасной маршрутизации сообщения с оптимальной балансировкой числа его фрагментов по непересекающимся маршрутам”, Захист інформації, No. 17(2), С. 135-142. DOI: https://doi.org/10.18372/2410-7840.17.8776
76. Yeremenko O.S., Ali S.A. Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET. Radioelectronics and Informatics. 2015. № 1(68). С. 26–29.
77. Yeremenko O., Yevdokymenko M., Persikov A. Flow-aware approach of evaluating probability of compromise in combined structure network. Advanced Information and Communication Technologies (AICT): Proceedings of the 2nd International Conference, Lviv, Ukraine, 4–7 July, 2017. IEEE, 2017. P. 258–261. DOI: 10.1109/AIACT.2017.8020114.
78. Yeremenko, O., Lemeshko, O., Persikov, A. (2017), “Enhanced Method of Calculating the Probability of Message Compromising Using Overlapping Routes in Communication Network”, Proceedings of the 2017 12th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), Lviv, Ukraine, 5-8 September, P. 87-90. DOI: https://doi.org/10.1109/STC-CSIT.2017.8098743
79. Yeremenko, O., Lemeshko, O., Persikov, A. (2018), “Secure Routing in Reliable Networks: Proactive and Reactive Approach”, Advances in Intelligent Systems and Computing II, CSIT 2017, Advances in Intelligent Systems and Computing, No. 689, Springer, Cham, P. 631–655. DOI: https://doi.org/10.1007/978-3-319-70581-1_44
80. Рябинин И.А., Черкесов Г.Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. М.: Радио и связь, 1981. - 264 с.
81. R.L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In Asiacrypt 2001. Full version available at http://www.mit.edu/~tauman and to appear in Essays in Theoretical Computer Science: in Memory of Shimon Even.

82. E. Bresson, J. Stern, and M. Szydlo. Threshold ring signatures and applications to ad-hoc groups. In Advances in Cryptology – Crypto 2002.
83. M. Naor. Deniable ring authentication. In Advances in Cryptology – Crypto 2002.
84. M. Abe, M. Ohkubo, and K. Suzuki. 1-out-of-n signatures from a variety of keys. In Advances in Cryptology – Asiacrypt 2002.
85. F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In Advances in Cryptology – Asiacrypt 2002.
86. J. Herranz and G. S´aez. Forking lemmas for ring signature schemes. In Progress in Cryptology – Indocrypt 2003.
87. Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup. Anonymous identification in ad-hoc groups. In Advances in Cryptology – Eurocrypt 2002.
88. J. Xu, Z. Zhang, and D. Feng. A ring signature scheme using bilinear pairings. In Workshop on Information Security Applications (WISA), 2004.
89. J.K. Liu, V.K. Wei, and D.S. Wong. Linkable spontaneous anonymous group signatures for ad hoc groups. In ACISP 2004.
90. B. Adida, S. Hohenberger, and R.L. Rivest. Ad-hoc-group signatures from hijacked keypairs. Available at http://theory.lcs.mit.edu/~srhohen/papers/AHR.pdf, 2005.
91. D. Chaum and E. van Heyst. Group signatures. In Advances in Cryptology – Eurocrypt ’91.
92. M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In Advances in Cryptology – Eurocrypt ’96.
93. L. Chen, C. Kudla, and K.G. Patterson. Concurrent signatures. In Advances in Cryptology – Eurocrypt 2004.
94. Bender, A. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles / Adam Bender, Jonathan Katz, Ruggero Morselli, TCC 2006. Cryptology ePrint Archive, 2005. https://eprint.iacr.org/2005/304.pdf
95. Zero-to-Monero 2-0-0, https://web.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
96. J. Xu, Z. Zhang, and D. Feng. A ring signature scheme using bilinear pairings. In Workshop on Information Security Applications (WISA), LNCS, 2004

https://www.researchgate.net/publication/221239543_A_Ring_Signature_Scheme_Using_Bilinear_Pairings

97. Kovalchuk L.V. Davydoff O.A. New efficient ring signature algorithm for provision of information by authorized people. Збірник тез VII Міжнародного науково-практичного семінару «Актуальні питання забезпечення кіберзахисту та захисту інформації», 24-27 лютого 2021 року, с. Верхнє Студене.
98. Trusted Computing Group. Trusted computing platform alliance (TCPA) main specification, version 1.1a. Republished as Trusted Computing Group (TCG) main specifcation, Version 1.1b, Available at www.trustedcomputinggroup.org, 2001.
99. E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In Proc. 11th ACM Conference on Computer and Communications Security, pages 225–234. acm press, 2004.
100. Camenisch, Jan, Manu Drijvers, and Anja Lehmann. Anonymous Attestation Using the Strong Diffie Hellman Assumption Revisited. Cryptology ePrint Archive: Report 2016/663. Available at: https://eprint.iacr.org/2016/663.pdf
101. Rootstock: smart contracts on Bitcoin network, 2018. https://www.rsk.co/.
102. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.;Wuille, P. Enabling blockchain innovations with pegged sidechains, 2014. https://blockstream.com/sidechains.pdf.
103. Kiayias, A.; Zindros, D. Proof-of-work sidechains, 2018. https://ia.cr/2018/1048.
104. Garoffolo, A.; Kaidalov, D.; Oliynykov, R. Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains, 2020. arXiv:2002.01847.
105. Pass, R.; Shi, E. FruitChains: A Fair Blockchain. Cryptology ePrint Archive, Report 2016/916, 2016. https://ia.cr/2016/916.
106. VeriBlock Inc.. Proof-of-Proof and VeriBlock Blockchain Protocol Consensus Algorithm and Economic Incentivization Specifications, 2019. http://bit.ly/vbk-wp-pop.

107. Gaži, P.; Kiayias, A.; Russell, A. Tight consistency bounds for bitcoin. Proceedings of the 2020 ACM SIGSAC Conference on Compute and Communications Security, 2020, pp. 819–838. https://doi.org/10.1145/3372297.3423365.
108. Karpinski, M.; Kovalchuk, L.; Kochan, R.; Oliynykov, R.; Rodinko, M.; Wieclaw, L. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. Sensors 2021, 121, 75–81. https://www.mdpi.com/1424-8220/21/19/6408 https://doi.org/10.3390/s21196408.
109. Kovalchuk, L.; Kaidalov, D.; Nastenko, A.; Rodinko, M.; Oliynykov, R. Probability of double spend attack for network with non-zero synchronization time. 21th Central European Conference on Cryptology (CECC 2021), 2021, pp. 52–54. https: //web.math.pmf.unizg.hr/~duje/cecc2020/.
110. Kovalchuk, L.; Kaidalov, D.; Nastenko, A.; Rodinko, M.; Shevtsov, O.; Oliynykov, R. Decreasing security threshold against double spend attack in networks with slow synchronization. Computer Communications 2020, 154, 75–81. https://doi.org/10.1016/j.comcom.2020.01.079.
111. Garoffolo, A.; Viglione, R. Sidechains: Decoupled Consensus Between Chains, 2018. arXiv:1812.05441.
112. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In CRYPTO 2017, Part I; - Lecture Notes in Computer Science, vol. 10401, Springer, Heidelberg, 2017; pp. 357–388. https: //doi.org/10.1007/978-3-319-63688-7_12.
113. Garay, J.; Kiayias, A.; Leonardos, N. The bitcoin backbone protocol: Analysis and applications. In Advances in Cryptology - EUROCRYPT 2015, Part II; - Lecture Notes in Computer Science, vol. 9057, Springer, Berlin, Heidelberg, 2015; pp. 281–310. https://doi.org/10.1007/978-3-662-46803-6_10.
114. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Succinct non-interactive zero knowledge for a von Neumann architecture, 2013. https://ia.cr/2013/879.
115. Bowe, S.; Gabizon, A. Making Groth's zk-SNARK simulation extractable in the random oracle model, 2018. https://ia.cr/2018/187.

116. Reitwiessner, C. zkSNARKs in a nutshell, 2016. https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/.
117. Bitansky, N.; Canetti, R.; Chiesa, A.; Tromer, E. From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again. Cryptology ePrint Archive, Report 2011/443, 2011. https://ia.cr/2011/443.
118. Groth, J. Short pairing-based non-interactive zero-knowledge arguments. In ASIACRYPT 2010; Abe, M., Ed.; Springer-Verlag, 2010; Vol. 6477, - Lecture Notes in Computer Science, pp. 321–340. https://doi.org/10.1007/978-3-642-17373-8_20.
119. Gennaro, R.; Gentry, C.; Parno, B.; Raykova, M. Quadratic Span Programs and Succinct NIZKs without PCPs. Cryptology ePrint Archive, Report 2012/215, 2012. https://ia.cr/2012/215.
120. Parno, B.; Gentry, C.; Howell, J.; Raykova, M. Pinocchio: Nearly Practical Verifiable Computation. Cryptology ePrint Archive, Report 2013/279, 2013. https://ia.cr/2013/279.
121. Z. Hu, S. Gnatyuk, B. Akhmetov, V. Simakhin, D. Ospanova, N. Akatayev, “Method for Cyber Threats Detection and Identification in Modern Cloud Services,” In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham, pp.326-346, 2021. https://doi.org/10.1007/978-3-030-80472-5_28
122. T. Radivilova, K. Lyudmyla, O. Lemeshko, D. Ageyev, M. Tawalbeh and A. Ilkov, "Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 819-822, doi: 10.1109/PICST51311.2020.9467973.
123. V. Chandola, A. Banerjee, V. Kumar, “Anomaly Detection: A Survey,” ACM Computing Survey, vol. 41, pp.1–58, 2009.
124. K. Sheridan, T. G. Puranik, E. Mangortey, O. J. Pinon-Fischer, M. Kirby, D.N. Mavris, “An application of dbscan clustering for flight anomaly detection during

the approach phase," Scitech 2020 Forum (AIAA), 2020, pp. 1851. https://doi.org/10.2514/6.2020-1851

125. D. Ageyev, T. Radivilova and O. Mohammed, "Traffic Monitoring and Abnormality Detection Methods Analysis," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 823-826, doi: 10.1109/PICST51311.2020.9468103.
126. Shitong Zhu, Shasha Li, Zhongjie Wang, Xun Chen, Zhiyun Qian, Srikanth V. Krishnamurthy, Kevin S. Chan, and Ananthram Swami. 2020. You do (not) belong here: de-tecting DPI evasion attacks with context learning. In Proceedings of the 16th Interna-tional Conference on emerging Networking EXperiments and Technologies (CoNEXT '20). Association for Computing Machinery, New York, NY, USA, 183–197. DOI:https://doi.org/10.1145/3386367.3431311
127. Shah S. A., Issac B. Performance comparison of intrusion detection systems and application of machine learning to Snort system. Future Generation Computer Systems. 2018. Vol. 80. P. 157-170. DOI: https://doi.org/10.1016/j.future.2017.10.016
128. Kirichenko L., Radivilova T., Bulakh V. Machine Learning in Classification Time Series with Fractal Properties. Data. 2019. Vol. 4, iss. 1, 5. P. 1–13. DOI:10.3390/data4010005 8632010.
129. M. Weber, F. Pistorius, E.S ax, J. Maas, B.Zimmer, "A Hybrid Anomaly Detection System for Electronic Control Units Featuring Replicator Neural Networks," In: Arai K., Kapoor S., Bhatia R. (eds), Advances in Information and Communication Networks, FICC 2018, Advances in Intelligent Systems and Computing, Springer, Cham, vol. 887, pp. 43 62, 2019. https://doi.org/10.1007/978-3-030-03405-4_4.
130. Elsayed, M.S., Le-Khac, N., Dev, S., & Jurcut, A.D. (2020). DDoSNet: A Deep-Learning Model for Detecting Network Attacks. 2020 IEEE 21st International Symposi-um on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 391-396.
131. Mulesa, O., Povkhan, I., Radivilova, T., Baranovskyi, O. (2021). Development of the method of construction of the optimal model of time series forecasting on

the basis of the principle of competition. Eastern-European Journal of Enter-prise Technologies, 5 (4 (113)), 6–11. doi: https://doi.org/10.15587/1729-4061.2021.240847

132. Kumar, V., Sinha, D. A robust intelligent zero-day cyber-attack detection technique. Complex Intell. Syst. 7, 2211–2234 (2021). https://doi.org/10.1007/s40747-021-00396-9
133. Kelley T, Amon MJ and Bertenthal BI (2018) Statistical Models for Predicting Threat Detection From Human Behavior. Front. Psychol. 9:466. doi: 10.3389/fpsyg.2018.00466
134. Li Y, Sperrin M, Ashcroft D M, van Staa T P. Consistency of variety of machine learn-ing and statistical models in predicting clinical risks of individual patients: longitudinal cohort study using cardiovascular disease as exemplar BMJ 2020; 371 :m3919 doi:10.1136/bmj.m3919
135. L. Srinivasa Reddy Srikanth Vemuru (2020). A Survey of different machine learning models for static and dynamic malware detection. European Journal of Molecular & Clinical Medicine, 7(3), 4299-4308.
136. Jyothsna V., Prasad K. M. Anomaly-Based Intrusion Detection System. Computer and Network Security. IntechOpen. 2019. DOI: 10.5772/intechopen.82287
137. Lyudmyla Kirichenko, Abed Saif Ahmed Alghawli, Tamara Radivilova. Generalized Approach to Analysis of Multifractal Properties from Short Time Series. International Journal of Advanced Computer Science and Applications(IJACSA), Volume 11 Issue 5, 2020. P.183-198. doi: 10.14569/IJACSA.2020.0110527
138. Radivilova T., Kirichenko L., Alghawli A. S., Ilkov A., Tawalbeh M., Zinchenko P. The Complex Method of Intrusion Detection Based on Anomaly Detection and Misuse Detection. Dependable Systems, Services and Technologies (DESSERT): Proceedings of 2020 IEEE 11th International Conference, 2020, Kyiv, Ukraine. P. 133-137, doi: 10.1109/DESSERT50317.2020.9125051.
139. R.M.A.Ujjan, Z. Pervez,; K. Dahal, W.A. Khan, A.M. Khattak, B. Hayat, “Entropy Based Features Distribution for Anti-DDoS Model in SDN,” Sustainability 2021, 13, 1522. https://doi.org/10.3390/su13031522

140. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(11), 2021, 183-194. https://doi.org/10.28925/2663-4023.2021.11.183194.
141. Common Vulnerability Scoring System v3.1: Specification Document, Forum of Incident Response and Security Teams (2019), available at: https://www.first.org/cvss/specificationdocument
142. Common Vulnerability Scoring System v3.1: Examples, Forum of Incident Response and Security Teams (2019), available at: https://www.first.org/cvss/examples
143. ISO/IEC 17799:2005 (2005), “Information technology, Security techniques, Code of practice for information security management”, available at: https://www.iso.org/standard/39612.html
144. ISO/IEC 15408-1:2009 (2009), “Information technology, Security techniques, Evaluation criteria for IT security, Part 1: Introduction and general model”, available at: https://www.iso.org/standard/50341.html
145. COBIT FRAMEWORK: INTRODUCTION & METHODOLOGY (2019), ISACA, available at: https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-FrameworkIntroduction-and-Methodology_res_eng_1118.pdf
146. COSO (2017), “Enterprise Risk Management Integrating with Strategy and Performance”, available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-andPerformance-Executive-Summary.pdf
147. Rec, I. T. U. T. (1996). M. 3010, Principles for a Telecommunications Management Network (TMN). Study Group IV.

ДОДАТОК А
ПУБЛІКАЦІЇ АВТОРСЬКОГО КОЛЕКТИВУ ЗА РЕЗУЛЬТАТАМИ ВИКОНАННЯ ПРОЄКТУ

А.1 Монографії (розділи монографій) за напрямом проєкту, виданих міжнародними видавництвами офіційними мовами Європейського Союзу та українською мовою

1. Krasnobayev, V., Kuznetsov, A., Yanko, A., Akhmetov, B., Kuznetsova, T., 2021. Processing of the Residuals of Numbers in Real and Complex Numerical Domains, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 529–555. https://doi.org/10.1007/978-3-030-43070-2_24
   Q3 (https://www.scimagojr.com/journalsearch.php?q=17500155101&tip=sid&clean=0)
2. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022s. Stream Ciphers in Modern Real-time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing. https://doi.org/10.1007/978-3-030-79770-6
   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)
3. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022a. Stream Symmetric Cipher “Strumok,” in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 467–516. https://doi.org/10.1007/978-3-030-79770-6_16
   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)
4. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022c. Research of Second-Order Properties of NLFSR. Comparative Analysis of M-NLFSR and M-LFSR, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A.,

Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 419–465. https://doi.org/10.1007/978-3-030-79770-6_15

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

5. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022d. Requirements for Feedback Coefficients, What Should the M-Nlfsr Respond to?, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 319–377. https://doi.org/10.1007/978-3-030-79770-6_13

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

6. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022e. Method of Synthesis M-NLFSR. Hardware and Software Search M-NLFSR Second Order. List M-NLFSR, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 379–418. https://doi.org/10.1007/978-3-030-79770-6_14

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

7. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022f. Introduction, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 1–11. https://doi.org/10.1007/978-3-030-79770-6_1

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

8. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022g. Criteria and Indices Substantiation of the Stream Cryptoconversion

Efficiency, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 13–35. https://doi.org/10.1007/978-3-030-79770-6_2

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

9. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022h. Conclusions, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 517–527. https://doi.org/10.1007/978-3-030-79770-6_17

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

10. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022j. Comparative Research of Fluid Cryptographic Transformation Algorithms, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 265–293. https://doi.org/10.1007/978-3-030-79770-6_11

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

11. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022k. Comparative Analysis of Determined Generators for Random Bits, Defined in the Nist Special Publication 800-90A, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 165–179. https://doi.org/10.1007/978-3-030-79770-6_8

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

12. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022l. Areas of Application for Nonlinear Shift Registers in PRS Generators, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 295–318. https://doi.org/10.1007/978-3-030-79770-6_12

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

13. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022m. Analysis of Synchronous Stream Cryptoconversions, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 47–64. https://doi.org/10.1007/978-3-030-79770-6_4

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

14. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022n. Analysis of Stream Modes for Block Symmetric Ciphers, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 65–98. https://doi.org/10.1007/978-3-030-79770-6_5

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

15. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022o. Analysis of Stream Cryptographic Transfer Algorithms for Light (Less-Resource) Cryptographies Defined in ISO/IEC 29192, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 241–264. https://doi.org/10.1007/978-3-030-79770-6_10

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

16. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022p. Analysis of Stream Cryptoconversion Principles, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 37–45. https://doi.org/10.1007/978-3-030-79770-6_3

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

17. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022q. Analysis of Standardized Algorithms for Streaming Cryptographic Convention, Defined in ISO/IEC 18033-4, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 111–163. https://doi.org/10.1007/978-3-030-79770-6_7

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

18. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022r. Analysis of Bitstreamed Cryptographic Conversion Algorithms from the International Project eSTREAM, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer International Publishing, Cham, pp. 181–240. https://doi.org/10.1007/978-3-030-79770-6_9

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

19. Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N., 2022i. Comparison of Stream Modes in Block Symmetric Ciphers, in: Kuznetsov, A.A., Potii, O.V., Poluyanenko, N.A., Gorbenko, Y.I., Kryvinska, N. (Eds.), Stream Ciphers in Modern Real-Time IT Systems: Analysis, Design and Comparative Studies, Studies in Systems, Decision and Control. Springer

International Publishing, Cham, pp. 99–110. https://doi.org/10.1007/978-3-030-79770-6_6

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100828949&tip=sid&clean=0)

20. Технології інформаційної безпеки в децентралізованих розподілених мережах : монографія. Частина 1 / За загальною редакцією Р. Олійникова, О. Кузнецова та О. Лемешка. – Харків: Видавництво «Форт», 2021. – 300 с.
21. Технології інформаційної безпеки в децентралізованих розподілених мережах : монографія. Частина 2 / За загальною редакцією Р. Олійникова, О. Кузнецова та О. Лемешка. – Харків: Видавництво «Форт», 2021. – 250 с.
22. Kirichenko L., Radivilova T., Ryzhanov V. (2022) Applying Visibility Graphs to Classify Time Series. In: Babichev S., Lytvynenko V. (eds) Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 77. Springer, Cham. https://doi.org/10.1007/978-3-030-82014-5_26
23. Lemeshko O., Yeremenko O., Yevdokymenko M., Radivilova T. (2021) Research of the QoE Fast ReRouting Processes with Differentiated R-Factor Maximization for VoIP-Flows Using the Tensor Model of the Corporate Telecommunication Network. In: Vorobiyenko P., Ilchenko M., Strelkovska I. (eds) Current Trends in Communication and Information Technologies. IPF 2020. Lecture Notes in Networks and Systems, vol 212. pp. 95-110. Springer, Cham. https://doi.org/10.1007/978-3-030-76343-5_6.

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)
24. Kirichenko L., Zinchenko P., Radivilova T. (2021) Classification of Time Realizations Using Machine Learning Recognition of Recurrence Plots. In: Babichev S., Lytvynenko V., Wójcik W., Vyshemyrskaya S. (eds) Lecture Notes in Computational Intelligence and Decision Making. ISDMCI 2020. Advances in Intelligent Systems and Computing, vol 1246. Springer, Cham. https://doi.org/10.1007/978-3-030-54215-3_44

    Q3 (https://www.scimagojr.com/journalsearch.php?q=5100152904&tip=sid&clean=0)

25. Lemeshko O., Hu Z., Shapovalova A., Yeremenko O., Yevdokymenko M. (2021) Research of the Influence of Compromise Probability in Secure Based Traffic Engineering Model in SDN. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 83. pp 47-55. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_5.
26. Kuznetsov, A., Gorbenko, Y., Kolovanova, I., Smirnov, S., Perevozova, I., Kuznetsova, T., 2021a. Output Feedback Encryption Mode: Periodic Features of Output Blocks Sequence, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 621–648. https://doi.org/10.1007/978-3-030-43070-2_27
27. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T., 2021b. Biometric Authentication Using Convolutional Neural Networks, in: Ilchenko, M., Uryvsky, L., Globa, L. (Eds.), Advances in Information and Communication Technology and Systems, Lecture Notes in Networks and Systems. Springer International Publishing, Cham, pp. 85–98. https://doi.org/10.1007/978-3-030-58359-0_6

    Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)
28. Kuznetsov, A., Pushkar'ov, A., Serhiienko, R., Smirnov, O., Babenko, V., Kuznetsova, T., 2021c. Representation of Cascade Codes in the Frequency Domain, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications, Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 557–587. https://doi.org/10.1007/978-3-030-43070-2_25
29. Lutsenko, M., Kuznetsov, A., Kiian, A., Smirnov, O., Kuznetsova, T., 2021. Biometric Cryptosystems: Overview, State-of-the-Art and Perspective Directions, in: Ilchenko, M., Uryvsky, L., Globa, L. (Eds.), Advances in Information and Communication Technology and Systems, Lecture Notes in Networks and

Systems. Springer International Publishing, Cham, pp. 66–84. https://doi.org/10.1007/978-3-030-58359-0_5

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)

30. Lemeshko, O., Kovalenko, T., Nevzorova, O., Ilyashenko, A., 2021a. Diakoptical Method of Inter-area Routing with Load Balancing in a Telecommunication Network, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications: ICT Systems-Theory, Radio-Electronics, Information Technologies and Cybersecurity (Volume 5), Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 747–766. https://doi.org/10.1007/978-3-030-43070-2_32
31. Lemeshko, O., Mersni, A., Nevzorova, O., 2021b. Analysis of Influence of Network Architecture Nonuniformity and Traffic Self-similarity Properties to Load Balancing and Average End-to-End Delay, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications: ICT Systems-Theory, Radio-Electronics, Information Technologies and Cybersecurity (Volume 5), Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 767–787. https://doi.org/10.1007/978-3-030-43070-2_33
32. Lemeshko, O., Yevdokymenko, M., Yeremenko, O., 2021c. Fast ReRoute Tensor Model with Quality of Service Protection Under Multiple Parameters, in: Radivilova, T., Ageyev, D., Kryvinska, N. (Eds.), Data-Centric Business and Applications: ICT Systems-Theory, Radio-Electronics, Information Technologies and Cybersecurity (Volume 5), Lecture Notes on Data Engineering and Communications Technologies. Springer International Publishing, Cham, pp. 489–512. https://doi.org/10.1007/978-3-030-43070-2_22
33. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Sleiman, B., 2021. System of Solutions the Maximum Number of Disjoint Paths Computation Under Quality of Service and Security Parameters, in: Ilchenko, M., Uryvsky, L., Globa, L. (Eds.), Advances in Information and Communication Technology and Systems, Lecture

Notes in Networks and Systems. Springer International Publishing, Cham, pp. 191–205. https://doi.org/10.1007/978-3-030-58359-0_10

Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)

Науковий та авторський вклад основних виконавців проєкту в публікації, виконані в співавторстві із сторонніми особами, був визначальним.

А.2 Статті у журналах, що індексуються в наукометричних базах даних WoS та/або Scopus.

1. Kuznetsov, A., Fedotov, S., Bagmut, M., 2021c. Convolutional Neural Networks to Protect Against Spoofing Attacks on Biometric Face Authentication, in: Wrycza, S., Maślankowski, J. (Eds.), Digital Transformation, Lecture Notes in Business Information Processing. Springer International Publishing, Cham, pp. 123–146. https://doi.org/10.1007/978-3-030-85893-3_9

   Q3 (https://www.scimagojr.com/journalsearch.php?q=17500155101&tip=sid&clean=0)
2. Kuznetsov, A., Kryvinska, N., Kiian, A., Smirnov, O., Kuznetsova, K., 2021e. Full Non-Binary Constant-Weight Codes. SN COMPUT. SCI. 2, 337. https://doi.org/10.1007/s42979-021-00739-w

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)
3. Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., Kolhatin, A., 2021h. Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain. IJCNIS 13, 1–15. https://doi.org/10.5815/ijcnis.2021.02.01
4. Kuznetsov, A., Poluyanenko, N., Kiian, A., 2021i. Fundamentals of Functioning of Global Contact Monitoring Systems in the Context of COVID-19 Spread Prevention, in: Vorobiyenko, P., Ilchenko, M., Strelkovska, I. (Eds.), Current Trends in Communication and Information Technologies, Lecture Notes in Networks and Systems. Springer International Publishing, Cham, pp. 311–328. https://doi.org/10.1007/978-3-030-76343-5_16

   Q4 (https://www.scimagojr.com/journalsearch.php?q=21100901469&tip=sid&clean=0)

5. Poluyanenko, N., Kuznetsov, A., Lisickiy, K., Datsenko, S., Nakisko, O., Rudenko, S., 2021. The Problem of Double Costs in Blockchain Systems, in: Hu, Z., Petoukhov, S., Dychka, I., He, M. (Eds.), Advances in Computer Science for Engineering and Education III, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 640–652. https://doi.org/10.1007/978-3-030-55506-1_57

   Q3 (https://www.scimagojr.com/journalsearch.php?q=5100152904&tip=sid&clean=0)

6. Bespalov, Y., Garoffolo, A., Kovalchuk, L., Nelasa, H., Oliynykov, R. Probability Models of Distributed Proof Generation for zk-SNARK-Based Blockchains. Mathematics 2021, 9(23), 3016. https://www.mdpi.com/2227-7390/9/23/3016

   Q2 (https://www.scimagojr.com/journalsearch.php?q=21100830702&tip=sid&clean=0)

7. Karpinski, M., Kovalchuk, L., Kochan, R., Oliynykov, R., Rodinko, M., Wieclaw, L. Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus. Sensors 2021, 21(19), 6408. https://www.mdpi.com/1424-8220/21/19/6408

   Q2 (https://www.scimagojr.com/journalsearch.php?q=130124&tip=sid&clean=0)

8. Kovalchuk, L., Oliynykov, R., Rodinko M. Security of the Poseidon Hash Function Against Non-Binary Differential and Linear Attacks. Cybernetics and Systems Analysis 2021, 57.2: 268-278. https://link.springer.com/article/10.1007/s10559-021-00352-y

   Q3 (https://www.scimagojr.com/journalsearch.php?q=12933&tip=sid&clean=0)

9. Lyudmila Kovalchuk, Dmytro Kaidalov, Andrii Nastenko, Mariia Rodinko, Oleksiy Shevtsov, and Roman Oliynykov. Decreasing security threshold against double spend attack in networks with slow synchronization. Computer Communications 154 (2020), 75–81. https://www.sciencedirect.com/science/article/abs/pii/S0140366419310758

   Q1 (https://www.scimagojr.com/journalsearch.php?q=13681&tip=sid&clean=0)

10. Lemeshko O., Papan J., Yeremenko O., Yevdokymenko M., Segec P. Research and Development of Delay-Sensitive Routing Tensor Model in IoT Core Networks. Sensors. 2021; 21(11): 3934, P. 1-23. DOI: https://doi.org/10.3390/s21113934.

Q2 (https://www.scimagojr.com/journalsearch.php?q=130124&tip=sid&clean=0)

11. Lemeshko, O., Yevdokymenko, M., Yeremenko, O., Kunicina, N. and Ziravecka, A.. "Investigation of the Flow-Based Fast Reroute Model with Implementation of a Multimedia Quality Protection Scheme" Latvian Journal of Physics and Technical Sciences, vol.58, no.6, 2021, pp.46-60. https://doi.org/10.2478/lpts-2021-0045

    Q3 (https://www.scimagojr.com/journalsearch.php?q=17900156724&tip=sid&clean=0)

У якості співавторів публікацій залучалися студенти-бакалаври, магістранти, аспіранти та докторанти наукового керівника та основних виконавців проєкту. Науковий та авторський вклад основних виконавців проєкту в публікації, виконані в співавторстві із сторонніми особами, був визначальним.

А.3 Статті у наукових фахових журналах України, що відносяться до категорії «Б», статті у закордонних наукових виданнях, що не оцінені за попереднім пунктом, а також англомовні тези доповідей у матеріалах міжнародних конференцій, що індексуються науково-метричними базами даних WoS або Scopus.

1. Krasnobaev, V., Kuznetsov, A., Popenko, V., Kuznetsova, T., 2021. Mathematical Model of the Reliability of a Computer System which is Functioning in the Residual Class System, Taking into Account the Reliability of Switching Devices, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT). Presented at the 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), pp. 225–229. https://doi.org/10.1109/AICT52120.2021.9628929
2. Krasnobaev, V., Popenko, V., Kuznetsov, A., Kuznetsova, T., 2020. Method of Control of Data which is Presented by Residual Classes, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and

Technology (PIC S T). Presented at the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T), pp. 779–784. https://doi.org/10.1109/PICST51311.2020.9468087

3. Krasnobayev, V., Kuznetsov, A., Bagmut, M., Kuznetsova, T., 2021a. Artificial Intelligence and Number System in Residual Classes, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT). Presented at the 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), pp. 171–176. https://doi.org/10.1109/AICT52120.2021.9628970
4. Krasnobayev, V., Kuznetsov, A., Popenko, V., Kuznetsova, T., 2021b. Design of a Residual Adder in Computer Systems (short paper)., in: Paper Proceedings of the Selected Papers on Publishing Papers with CEUR-WS Co-Located with Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021 (Online). pp. 206–212.
5. Krasnobayev, V., Kuznetsov, A., Yanko, A., Kuznetsova, T., 2020a. The Procedure for Implementing the Operation of Multiplying Two Matrices Using the Residual Number System, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T), pp. 353–357. https://doi.org/10.1109/PICST51311.2020.9468076
6. Krasnobayev, V., Kuznetsov, A., Yanko, A., Kuznetsova, T., 2020b. Solving the Shortest Path Problem Using Integer Residual Arithmetic, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T), pp. 563–566. https://doi.org/10.1109/PICST51311.2020.9467947
7. Kuznetsov, A., Datsenko, S., Gorbenko, Y., Chupilko, T., Korneyev, M., Klym, V., 2021a. Experimental Researches of Biometric Authentication Using Convolutional Neural Networks and Histograms of Oriented Graphs, in: 2021

IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT). Presented at the 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), pp. 288–292. https://doi.org/10.1109/AICT52120.2021.9628932

8. Kuznetsov, A., Derevianko, Y., Poluyanenko, N., Bagmut, O., 2021b. Particle Swarm Optimization Based S-boxes Generation, in: Paper Proceedings of the Selected Papers on Publishing Papers with CEUR-WS Co-Located with Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, October 26, 2021 (Online). Presented at the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, October 26, 2021 (online).
9. Kuznetsov, A., Girzheva, O., Kiian, A., Nakisko, O., Smirnov, O., Kuznetsova, T., 2020. Advanced Code-Based Electronic Digital Signature Scheme, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T). Presented at the 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T), pp. 358–362. https://doi.org/10.1109/PICST51311.2020.9467895
10. Kuznetsov, A., Kuznetsova, K.: Comment on “Particle Swarm Optimization Based Highly Nonlinear Substitution-Boxes Generation for Security Applications.” In: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)., Cracow, Poland (September 22-25). https://drive.google.com/drive/folders/1pWMfLjqEPecLchIzOiRBEt7usEm7ONUi?usp=sharing
11. Kuznetsov, A., Kononchenko, A., 2021. Software Implementation of Data Hiding in Vector Images, in: 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON). Presented at the 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 572–577. https://doi.org/10.1109/UKRCON53503.2021.9575240

12. Kuznetsov, A., Lokotkova, I., Smirnov, O., Kuznetsova, T., Florov, S., Lebid, O., 2021f. Using Orthogonal Signals to Hide Information in Images, in: 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT). Presented at the 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), pp. 255–260. https://doi.org/10.1109/AICT52120.2021.9628959
13. Кузнецов О.О., Кононченко Г.В. Стеганографічні методи в векторній графіці. Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2021. – Вып. 205. – С. 32-41.
14. Кузнецов А.А., Смирнов А.А., Кузнецова Т.Ю. Шумоподобные дискретные сигналы для асинхронных систем кодового разделения радиоканалов. Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2021. – Вып. 205. – С. 175-183.
15. Кузнецов О.О., Полуяненко М.О., Катрич В.О., Кандій С.О., Заиченко Ю.О. Дослідження евристичних функцій пошуку нелінійних підстановок для симетричної криптографії. Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2021. – Вып. 206. – С. 53-63.
16. Кузнецов О.О., Полуяненко М.О., Бердник С.Л., Кандій С.О., Заиченко Ю.О. Оптимізація параметрів алгоритму локального пошуку для генерації нелінійних підстановок. Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2021. – Вып. 206. – С. 64-76.
17. Шеханін К.Ю., Пшенична С.В., Кузнецов О.О. Дослідження обчислювальної складності методів приховування інформації у кластерні стеганосистеми. Радиотехника: всеукр. межвед. науч.-техн. сб. – Харьков: ХТУРЕ. – 2021. – Вып. 206. – С. 77-87.
18. Yuri Bespalov, Alberto Garoffolo, Lyudmila Kovalchuk, Hanna Nelasa, Roman Oliynykov. Game-Theoretic View on Decentralized Proof Generation in zk-SNARK-based Sidechains // Proceedings of Cybersecurity Providing in Information and Telecommunication Systems 2021. Kyiv, Ukraine, January 28, 2021 (online). http://ceur-ws.org/Vol-2923/paper6.pdf

19. Yu. Bespalov, A. Garoffolo, L. Kovalchuk, H. Nelasa, R. Oliynykov. Models of distributed proof generation for ZK-SNARK-based blockchains // Теоретическая и прикладная криптография : материалы междунар. науч. конф., Минск, 20-21 окт. 2020 г. / Белорус. гос. ун-т ; редкол.: Ю. С. Харин (гл. ред.) [и др.]. – Минск : БГУ, 2020. – С. 114-120. https://elib.bsu.by/handle/123456789/269354
20. Yuri Bespalov, Lyudmila Kovalchuk, Hanna Nelasa and Roman Oliynykov. On Generation of Cycles, Chains and Graphs of Pairing-Friendly Elliptic Curves // Proceedings of Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2020. Kharkiv, Ukraine, 6 9 October, 2020. P. 137-141. https://ieeexplore.ieee.org/abstract/document/9468050
21. Lyudmila Kovalchuk, Mariia Rodinko, Roman Oliynykov. Security of Poseidon Hash Function Against Linear and Differential Attacks with respect to field operations // 20th Central European Conference on Cryptology : Book of Abstracts, 2020. Zagreb, Croatia, 24-26 June, 2020. P. 35-36. https://web.math.pmf.unizg.hr/cecc2020/files/cecc-bookofabstracts-str.pdf
22. Lyudmila Kovalchuk, Mariia Rodinko, and Roman Oliynykov. 2020. Upper Bound Probability of Double Spend Attack on SPECTRE // CryBlock ’20:3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, September 25th, 2020, Virtual (online) Conference. ACM, New York, NY, USA. P. 18-20. https://dl.acm.org/doi/abs/10.1145/3410699.3413792
23. Lemeshko O., Yeremenko O., Shapovalova A., Yevdokymenko M., Lemeshko V., Persikov M. Analysis of Secure Routing Processes Using Traffic Engineering Model. The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 22-25 September, 2021, Cracow, Poland, P. 1-5.
24. Radivilova T., Kirichenko L., Lemeshko O., Ageyev D., Mulesa O., Ilkov A. Analysis of Anomaly Detection and Identification Methods in 5G Traffic. The 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 22-25 September, 2021, Cracow, Poland, P. 1-5.

25. Lemeshko O., Yeremenko O., Shapovalova A., Yevdokymenko M., Omowumi S.O., Hailan A.M. Secure Routing with Power Link Blocking Model and Load Balancing. 4th IEEE International Conference on Advanced Information and Communication Technologies (AICT), 21-25 September, 2021, Lviv, Ukraine, pp. 216-219, doi: 10.1109/AICT52120.2021.9628938.
26. Lemeshko O., Kruhlova A., Zhuravlova A., Yeremenko O. Research and Development of Improved Routing Mechanism with Load Balancing in Communication Network. ACM womENcourage 2021. P. 1-2.
27. Lemeshko O., Yeremenko O., Yevdokymenko M., Zhuravlova A., Kruhlova A., Lemeshko V. "Research of Improved Traffic Engineering Fault-Tolerant Routing Mechanism in SD-WAN," 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2021, pp. 187-190, doi: 10.1109/UKRCON53503.2021.9575272.
28. Lemeshko O., Yeremenko O., Mersni A. Investigation of Enhanced Mathematical Model for Fault-tolerant Routing. Seventh International Conference on Engineering and Emerging Technologies (ICEET 2021), 27-28 October 2021, Istanbul, Turkey. IEEE, 2021. P. 1-6.
29. Lemeshko O., Yeremenko O., Yevdokymenko M., Kuzminykh I., Mersni A. Development of Virtual Laboratories and Innovative Cybersecurity Courses for Distance Learning. Workshop on Cybersecurity Providing in Information and Telecommunication Systems - CPITS II 2021. Kyiv, Ukraine. P. 1-10.
30. Лемешко А. В. Сетевая безопасность средствами маршрутизации: проблемы и решения / А. В. Лемешко, М. А. Евдокименко, А. С. Еременко // Международная конференция «Информационная безопасность: проблемы и перспективы», 29 октября 2021 г., Баку, Азербайджан. - С. 6-8.
31. Lemeshko O., Mersni A., Yeremenko O., Omowumi S.O., Volotka V., Al-Dulaimi A.M. K. Application Prospects of First Hop Redundancy Protocols for Fault-Tolerant SDN Controllers: A Survey. 2021 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2021, pp. 1-5.

32. Lemeshko O., Yevdokymenko M., Shapoval M. Routing Model with Load Balancing on the Traffic Engineering Principles based on Information Security Risks. 2021 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, 2021, pp. 1-5.
33. Radivilova T., Kirichenko L., Lemeshko O. ”Provide information security for the web application in Amazon Web Services” 2021 IEEE 8th International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2021, pp. 1-6.
34. Kuzminykh, I., Yevdokymenko, M., Yeremenko, O., Lemeshko, O. Increasing Teacher Competence in Cybersecurity using the EU Security Frameworks. I.J. Modern Education and Computer Science, 2021, 6, p. 60-68. DOI: 10.5815/ijmecs.2021.06.06
35. Lemeshko O., Yeremenko O., Mersni A., Yevdokymenko M. Resilience Aware Traffic Engineering FHRP Solution (Invited Paper). 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, November 29 – December 3, 2021. P. 88-92.
36. Лемешко О.В., Грачов Ю.В., Слейман Б. Дослідження методу безпечної маршрутизації конфіденційних повідомлень за шляхами, які не перетинаються // Проблеми телекомунікацій. 2020. 2(27). С. 43-55. URL: https://doi.org/10.30837/pt.2020.2.04
37. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Baranovskyi O. (2022) Complex Investigation of the Compromise Probability Behavior in Traffic Engineering Oriented Secure Routing Model in Software-Defined Networks. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol 831. Springer, Cham. pp. 145-160. DOI: https://doi.org/10.1007/978-3-030-92435-5_8
38. Radivilova T., Kirichenko L., Lemeshko O., Ageyev D., Tawalbeh M., Ilkov A. "Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks," 2020 IEEE International Conference on Problems of

Infocommunications. Science and Technology (PIC S&T), 2020, pp. 819-822, DOI: https://doi.org/10.1109/PICST51311.2020.9467973

39. Garoffolo A., Kaidalov D., Oliynykov R. Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. The Second IEEE International Workshop on Blockchain and Mobile Applications (BlockApp 2020), 40th IEEE International Conference on Distributed Computing Systems (ICDCS).
40. Lemeshko O., Yeremenko O., Shapovalova A., Hailan A.M., Yevdokymenko M., Persikov M. Design and Research of the Model for Secure Traffic Engineering Fast ReRoute under Traffic Policing Approach. 2021 16th International Conference on the Experience of Designing and Application of CAD System in Microelectronic (CADSM), 22-26 February 2021. Lviv, Ukraine. pp. 23-26, doi: 10.1109/CADSM52681.2021.9385253.
41. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Lemeshko V. Network Security Approach Based on Traffic Engineering Fast ReRoute with support of Traffic Policing. Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021). Kyiv, Ukraine, 2021. P. 1-10.
42. Krasnobayev, V., Kuznetsov, A., Kononchenko, A., Kuznetsova, T.: Method of Diagnostic of Non-Positional Code Structures in the System of Residue Classes Basing on the Usage of an Alternative Number Set Informativeness. In: Paper Proceedings of the Selected Papers on Publishing Papers with CEUR-WS co-located with Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021 (online). pp. 97–106 (2021).
43. Lemeshko O., Yeremenko O., Yevdokymenko M., Sleiman B. QoS Routing Model over Disjoint Paths with Guaranteed Bandwidth in Software-Defined Networks // Computer and information systems and technologies, Kharkiv, April 2021. P. 93. DOI: https://doi.org/10.30837/csitic52021232902

44. Lemeshko O., Yeremenko O., Shapovalova A., Yevdokymenko M., Akulynichev A., Porokhniak V. Research of Secure Routing with Load Balancing and Compromise Probability Behavior Account. 2021 IEEE 19th International Conference on Smart Technologies (EUROCON), Lviv, Ukraine, 6-8 July, 2021. IEEE, 2021. pp. 296-299, doi: 10.1109/EUROCON52738.2021.9535642.
45. Kuznetsov, A., Horkovenko, I., Maliy, O., Goncharov, N., Kuznetsova, T., Kovalenko, N.: Non-Binary Cryptographic Functions for Symmetric Ciphers. In: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S T). pp. 567–572 (2020). https://doi.org/10.1109/PICST51311.2020.9467982.
46. Kuznetsov, A., Kononchenko, A.: Message Concealing in Vector Images. In: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)., Cracow, Poland (September 22-25). https://drive.google.com/drive/folders/1pWMfLjqEPecLchIzOiRBEt7usEm7ONUi?usp=sharing
47. Kuznetsov, A., Lutsenko, M., Bagmut, M., Zhora, V.: Performance Evaluation of the Classic McEliece Key Encapsulation Algorithm. In: 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)., Cracow, Poland (September 22-25). https://drive.google.com/drive/folders/1pWMfLjqEPecLchIzOiRBEt7usEm7ONUi?usp=sharing
48. Kirill Shekhanin, Lyudmila Gorbachova, Alexander Kuznetsov. “Comparative Analysis and Study of Storage Devices Properties for Steganographic Data Hiding in Cluster File Systems,” Proceedings of 2nd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, Kyiv, 30 Nov.2020.
49. Alexandr Kuznetsov, Anastasiia Kiian, Kateryna Kuznetsova and Alexey Smirnov. “Data Hiding Scheme Based on Spread Sequence Addressing,” Proceedings of 1st

International Workshop on Computational & Information Technologies for Risk-Informed Systems CITRisk-2020, Kherson, Ukraine, October, 2020.

50. Victor Krasnobayev, Alexandr Kuznetsov, Anna Kononchenko and Tetiana Kuznetsova. “Algorithms for Determining Residues Modulo in a Complex Numerical Domain,” Proceedings of 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems CITRisk-2020, Kherson, Ukraine, October, 2020.
51. Radivilova T. , Kirichenko L, Lemeshko O., Ageyev D., Tawalbeh M., Ilkov A. "Analysis of Approaches of Monitoring, Intrusion Detection and Identification of Network Attacks," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 819-822, doi: 10.1109/PICST51311.2020.9467973.
52. D. Ageyev, T. Radivilova, O. Bondarenko and O. Mohammed, "Traffic Monitoring and Abnormality Detection Methods for IoT," 2021 IEEE 4th International Conference on Advanced Information and Communication Technologies (AICT), 2021, pp. 250-254, doi: 10.1109/AICT52120.2021.9628954.
53. Tamara Radivilova, Lyudmyla Kirichenko, Oleksandr Lemeshko, Dmytro Ageyev and Maksym Tawalbeh. “Formation of network and user behavior features set for their use in the process of early intrusion detection and identification of network attacks,” Proceedings of the Selected Papers on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021). Kyiv, Ukraine, January 27, 2021 (online).
54. Papan J., Segeč P., Dobrota J., Koncz L., Yeremenko O., Lemeshko O., Yevdokymenko M. Review of Fast ReRoute solutions. 2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA), Košice, Slovakia, 2020, pp. 498-504, doi: 10.1109/ICETA51985.2020.9379175.
55. Lemeshko O., Yeremenko O., Yevdokymenko M., Shapovalova A., Radivilova T., Ageyev D. Secure Based Traffic Engineering Model in Softwarized Networks. 2020 IEEE International Conference on Advanced Trends in Information Theory ATIT, Kyiv. 2020, pp. 143-147, doi: 10.1109/ATIT50783.2020.9349301.

56. Lemeshko O., Yeremenko O., Yevdokymenko M., Ageyev D. "Redundancy Cyber Resiliency Technique Based on Fast ReRouting under Security Metric" 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2020, pp. 815-818, doi: 10.1109/PICST51311.2020.9468072.
57. Ageyev D., Radivilova T., Mohammed O., "Traffic Monitoring and Abnormality Detection Methods Analysis," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020, pp. 823-826, doi: 10.1109/PICST51311.2020.9468103.
58. Radivilova, T., Kirichenko, L., Tawalbeh, M., & Ilkov, A. (2021). Виявлення аномалій в телекомунікаційному трафіку статистичними методами. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(11), 183-194. https://doi.org/10.28925/2663-4023.2021.11.183194
59. Лемешко О., Єременко О., Євдокименко М., Кузьміних Є. Особливості створення віртуальної лабораторії кібербезпеки для дистанційного навчання // Новий колегіум. 2020. №3. С. 41-45.
60. Lemeshko O., Shapovalova A., Al- Dulaimi A.M.K., Yeremenko O., Yevdokymenko M. Flow-Based Routing Model With Load Balancing Under Network Security Parameters // Information and Telecommunication Sciences. No 2 (2020). P. 44-50.

У якості співавторів публікацій залучалися студенти-бакалаври, магістранти, аспіранти та докторанти наукового керівника та основних виконавців проєкту. Науковий та авторський вклад основних виконавців проєкту в публікації, виконані в співавторстві із сторонніми особами, був визначальним.

А.4 Патенти України або інших країн на винахід чи охоронних документів на промисловий зразок/корисну модель чи інші отримані охоронні документи на об’єкти права інтелектуальної власності

1. Пат. UA 149074, МПК G06F 7/00, G06F 7/72 (2006.01). Операційний пристрій у системі залишкових класів. Краснобаєв В. А.; Кошман С. О.; Кузнецов О. О.; Мавріна М. О.; Ковальчук Д. М. Пат. UA 149074, МПК G06F 7/00, G06F 7/72 (2006.01). № u202102897; Заявл. 31.05.2021; Опубл. 13.10.2021, бюл. № 41. – 4с. https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=278540
2. Пат. UA 149421, МПК G06F 5/00 (2006.01). Пристрій для визначення лишків числа за довільним модулем системи залишкових класів. Краснобаєв В. А.; Кошман С. О.; Кузнецов О. О.; Мавріна М. О.; Ковальчук Д. М. Пат. UA 149421, МПК G06F 5/00 (2006.01). № u202102898; Заявл. 31.05.2021; Опубл. 17.11.2021, бюл. № 46. – 4с. https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=279077
3. Пат. UA 148170, МПК G06F 7/50 (2006.01). Суматор за довільним модулем m системи залишкових класів. Краснобаєв В. А.; Кошман С. О.; Кузнецов О. О.; Мавріна М. О.; Ковальчук Д. М. Пат. UA 148170, МПК G06F 7/50 (2006.01). № u202100701; Заявл. 17.02.2021; Опубл. 14.07.2021, бюл. № 28. – 4с. https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=277110
4. Пат. UA 149060, МПК G06F 7/50 (2006.01). Пристрій для контролю та виправлення однократних помилок у даних, які представлені системою залишкових класів. Краснобаєв В. А.; Кошман С. О.; Кузнецов О. О.; Ковальчук Д. М. Пат. UA 149060, МПК G06F 7/50 (2006.01). № u202102707; Заявл. 24.05.2021; Опубл. 13.10.2021, бюл. № 41. – 4с. https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=278526

А.5 Підручники, навчальні посібники України.

1. Програмне середовище для роботи з довгою арифметикою : методичні рекомендації до лабораторної роботи з дисципліни “Теорія чисел, груп, полів, кілець” для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко, Ю. М. Рябуха. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 31 с.
2. Алгоритм Ель-Гамаля : методичні рекомендації до лабораторної роботи з дисципліни “Теорія чисел, груп, полів, кілець” для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко, Ю. М. Рябуха. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 102 с.
3. Огляд технології блокчейн : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 84 с.
4. Протоколи консенсусу децентралізованих систем : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 60 с.
5. Питання безпеки децентралізованих систем : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 36 с.
6. Подвійні витрати : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 76 с.

7. Огляд сучасних алгоритмів гешування у блокчейн-системах : конспект лекцій з дисципліни «Технології блокчейн» для студентів спеціальності 125 «Кібербезпека» / О. О. Кузнецов, М. О. Полуяненко, О. О. Полуяненко. – Харків : ХНУ імені В. Н. Каразіна, 2021. – 140 с.
8. О. О. Кузнецов, М. О. Полуяненко, В. А. Краснобаєв, С. О. Кошман. Довідник термінів і визначень технології блокчейн / уклад. О. О. Кузнецов, М. О. Полуяненко, В. А. Краснобаєв, С. О. Кошман. Харків: ХНУ імені В. Н. Каразіна, 2020. 48 с.
9. В. А. Краснобаєв, С. О. Кошман, О. О. Кузнецов, М. О. Полуяненко. Непозиційна система числення в залишкових класах: довідник термінів і визначень / уклад. В. А. Краснобаєв, С. О. Кошман, О. О. Кузнецов, М. О. Полуяненко. – Харків : ХНУ ім. В. Н. Каразіна, 2020. – 36 с.

А.6 Перелік поданих до публікації матеріалів

1. Dmytro Ageyev, Tamara Radivilova, Oksana Mulesa, Oleg Bondarenko, Othman Mohammed. Traffic Monitoring and Abnormality Detection Methods for Decentralized Distributed Networks. Springer
2. Tamara Radivilova, Lyudmyla Kirichenko, Abed Saif Alghawli, Dmytro Ageyev, Oksana Mulesa, Oleksii Baranovskyi, Andrii Ilkov, Vladyslav Kulbachnyi, Oleg Bondarenko. Statistical and signature analysis methods of intrusion detection. Springer
3. Oksana Mulesa, Oleksandr Mitsa, Tamara Radivilova, Igor Povkhan and Olena Melnyk. Development of a Method to Find the Location of a Logistics Hub. Conference of Information technology and implementation. CEUR.

4. Dmytro Ageyev, Tamara Radivilova, Oleg Bondarenko and Othman Mohammed. Traffic Abnormality Detection ML-based Method for IoT. Conference IEEE UkrMiCo’2021.
5. Tamara Radivilova, Lyudmyla Kirichenko, Oleksandr Lemeshko, Andrii Ilkov, Maksym Tawalbeh, Volodymyr Sokolov. Ensuring network security based on traffic engineering approach. Springer.
6. Oleksandr Lemeshko, Oleksandra Yeremenko, Maryna Yevdokymenko and Batoul Sleiman. Research and Development Bilinear QoS Routing Model over Disjoint Paths with Bandwidth Guarantees in SDN. CEUR, 2021. P. 1-10.
7. Zhengbing Hu, Oleksandr Lemeshko, Oleksandra Yeremenko, Batoul Sleiman, Amal Mersni and Artem Akulynichev. Investigation of the Multicast Routing Model with Support of Traffic Engineering and Its Application in Software-Defined Networking. Springer, 2021, P. 1-16.
8. Oksana Mulesa, Anatoliy Batyuk, Fedir Geche, Olena Melnyk, Mykola Palinchak and Tamara Radivilova. Information technology for time series forecasting based on the evolutionary method of the forecasting scheme synthesis. CSIT 2021.
9. Radivilova T., Kirichenko L., Lemeshko O., Ageyev D., Tawalbeh M. Analysis of models and methods of traffic engineering in intrusion detection system (подано до редакції Springer International Publishing, Cham).
10. Lemeshko O., Papan J., Yevdokymenko M., Yeremenko O.. Advanced Tensor Solution to the Problem of Inter-Domain Routing with Normalized Quality of Service // Applied Sciences (MDPI). Received: 10 December 2021

А.7 Захищені дисертації доктора філософії (кандидата наук) авторами проєкту або під керівництвом авторів проєкту

1. Ігнатенко С.М. Методи розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. – Харківський національний

університет імені В. Н. Каразіна, Міністерства освіти і науки України. – Харків, 2021. (захищена 22.04.2021). Науковий керівник: виконавець проєкту, д.т.н., проф. Кузнецов О.О. http://ekhnuir.univer.kharkov.ua/handle/123456789/16047

2. Родінко М. Ю. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів. Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки (Галузь знань 12 – Інформаційні технології). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2020. (захищена 14.09.2021). Науковий керівник: науковий керивник проєкту, д.т.н., доц. Олійников Р.В. http://ekhnuir.univer.kharkov.ua/handle/123456789/16541
3. Шеханін К.Ю. Розробка та аналіз стеганографічних методів приховування даних в структуру файлових систем. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (Галузь знань 12 – «Інформаційні технології»). – Харківський національний університет імені В. Н. Каразіна Міністерство освіти і науки України, Харків, 2021. (захист запланований у грудні 2021 року). Науковий керівник: виконавець проєкту, д.т.н., проф. Кузнецов О.О. http://rada.karazin.ua/public/uploads/2021/12/33-%D0%A8%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%BD.pdf

А.8 Захищені дисертації доктора наук авторами проєкту або під консультуванням авторів проєкту

1. Дисертація Радівілової Тамари Анатоліївни (виконавець проєкту) «Моделі та методи забезпечення безпеки та якості обслуговування в комп'ютерних системах із самоподібними інформаційними потоками» на здобуття наукового ступеня доктора технічних наук зі спеціальності 05.13.21 – системи захисту інформації. Місце захисту: Державний університет телекомунікацій (дата захисту 28 січня 2021 року) http://www.dut.edu.ua/uploads/p_1539_98959884.pdf

2. Дисертація Євдокименко Марини Олександрівни «Теоретичні основи відмовостійкої маршрутизації чутливого до затримок та втрат трафіка в телекомунікаційних мережах з використанням тензорних моделей і методів» на здобуття наукового ступеня доктора технічних наук зі спеціальності 05.12.02 – телекомунікаційні системи та мережі. Місце захисту: Харківський національний університет радіоелектроніки. Науковий консультант: виконавець проєкту, проф. Лемешко О.В. (дата захисту 28 грудня 2020 року)
https://nure.ua/wp-content/uploads/2020/Disertation/avtoreferat-ievdokimenko.pdf

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
"ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ" (АТ "ІІТ")
Україна, 61166, м. Харків, вул. Косомисська, 15
Адреса для листування: Україна, 61166, м. Харків, вул. Бакулина, 12
Тел./факс (057) 714-22-05, тел. (057) 702-16-25
e-mail: itz@iit.kharkov.ua, web-сайт: www.iit.com.ua

АКТ
впровадження результатів проєкту 2020.01/0351

Даним актом підтверджується, що результати проєкту

Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій, номер державної реєстрації 0121U112489, грантова підтримка Національного фонду досліджень України

яка виконується Харківським національним університетом імені В.Н. Каразіна,

науковим керівником якої є Олійников Роман Васильович

впроваджено: в Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків.

Термін впровадження: 2021, грудень

Форма впроваджених результатів: результати впроваджено при розробки спеціального математичного та програмного забезпечення щодо оцінки криптографічної стійкості існуючих методів та механізмів криптографічного захисту інформації у пост-квантовий період.

Характеристика масштабу впровадження: унікальне та одиночне

Новизна впроваджених результатів: нове

Ефективність впровадження: з соціальним, економічним і науково-технічним ефектом

Виконавчий директор АТ "ІІТ" В.Д. Кравченко

М.П.