НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ШАРОВ ВЛАДИСЛАВ ОЛЕГОВИЧ

УДК 519.72, 004.4:004.7, 004.9

ДИСЕРТАЦІЯ
МОДЕЛІ, МЕТОДИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДВИЩЕННЯ НАДІЙНОСТІ Й ЗАХИЩЕНОСТІ ПЕРЕДАЧІ ДАНИХ У МЕРЕЖАХ

Спеціальність 122 – Комп’ютерні науки

Галузь знань 12 – Інформаційні технології

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.О. Шаров

Науковий керівник:
Нікуліна Олена Миколаївна
доктор технічних наук, професор

Харків – 2026

АНОТАЦІЯ

Шаров В.О. Моделі, методи та інформаційна технологія підвищення надійності й захищеності передачі даних у мережах – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки. – Національний технічний університет «Харківський політехнічний інститут», Харків, 2026.

Дисертаційну роботу присвячено вирішенню актуальної науково-технічної задачі підвищення надійності та захищеності передавання даних у комп'ютерних мережах в умовах дії завад і кіберзагроз шляхом розроблення інтегрованих моделей, методів та інформаційної технології, що поєднують механізми завадостійкого кодування та захищеного тунелювання.

Об'єкт дослідження – процес передавання даних у комп'ютерних мережах за наявності завад і кіберзагроз.

Предмет дослідження – моделі, методи та інформаційна технологія забезпечення надійності й захищеності передавання даних на основі інтеграції завадостійкого кодування та оверлейних технологій.

Метою роботи є підвищення ефективності, надійності та захищеності передавання даних шляхом розроблення та впровадження інтегрованого підходу до забезпечення їх надійності та захищеності.

У *вступі* обґрунтовано актуальність теми, визначено наукову проблему недостатньої ефективності ізольованого застосування засобів захисту та завадостійкості, що не дозволяє забезпечити необхідний рівень стабільності передачі даних у сучасних мережах.

У *першому розділі* проаналізовано сучасний стан методів забезпечення ефективності, надійності та захищеності передавання даних, визначено їх обмеження та сформульовано наукову задачу інтеграції відповідних механізмів.

У *другому розділі* обґрунтовано систему показників оцінювання ефективності, розроблено концептуальну модель гібридного захищеного каналу передавання даних та методи синтезу та формування його параметрів.

У *третьому розділі* розроблено моделі та методи інтеграції завадостійкого кодування та оверлейних технологій, удосконалено метод адаптивного керування параметрами системи та запропоновано інформаційну технологію багаторівневого захисту.

У *четвертому розділі* проведено імітаційне моделювання та експериментальні дослідження ефективності запропонованих рішень із використанням профілів VPN (зокрема IPsec, OpenVPN, WireGuard) та каскадних кодів. Отримані результати підтвердили підвищення стійкості до помилок, зменшення втрат пакетів і покращення стабільності передачі даних порівняно з базовими підходами.

У *висновках* дисертаційної роботи узагальнено результати проведених досліджень та підтверджено досягнення поставленої мети. У роботі розроблено гібридну модель захищеного каналу передавання даних, методи синтезу профілю каналу та адаптивного керування параметрами системи, а також реалізовано інформаційну технологію інтеграції завадостійкого кодування та VPN-протоколів. Доведено ефективність інтегрованого підходу до забезпечення надійності й захищеності передавання даних в умовах завад, втрат пакетів і кіберзагроз. Встановлено, що спільне використання механізмів FEC-кодування та VPN-тунелювання забезпечує підвищення стійкості до помилок, зменшення втрат пакетів і стабілізацію процесу передавання даних у складних умовах функціонування мереж.

За результатами дослідження отримано такі наукові результати:

– удосконалено гібридну модель захищеного каналу передавання даних, побудовану на поєднанні механізмів завадостійкого кодування та VPN-тунелювання з урахуванням впливу завад і кіберзагроз різної природи, яка, на відміну від існуючих підходів до окремого використання зазначених механізмів,

забезпечує їх комплексну взаємодію та дозволяє підвищити стійкість системи до помилок і атак, а також забезпечити стабільність передавання даних у складних умовах функціонування мереж;

– удосконалено метод адаптивного налаштування параметрів завадостійкого кодування та оверлейних протоколів на основі оцінювання стану мережі й показників ефективності передавання даних, який, на відміну від існуючих методів із фіксованими або частково змінними параметрами, забезпечує узгоджене коригування конфігурації системи та дозволяє підвищити ефективність використання мережевих ресурсів і якість обслуговування трафіку;

– отримали подальший розвиток методи формування профілю каналу передавання даних і побудови інформаційної технології багаторівневого захисту на основі комплексного врахування параметрів кодування та характеристик VPN-протоколів, які, на відміну від існуючих рішень, забезпечують інтегроване налаштування параметрів системи та дозволяють реалізувати адаптивне конфігурування захищених каналів зв’язку відповідно до умов функціонування й вимог до надійності та інформаційної безпеки.

Практичне значення отриманих результатів полягає у безпосередньому використанні запропонованих моделей, методів та інформаційної технології при побудові захищених комп’ютерних мереж і каналів передавання даних, завдяки чому досягається підвищення ефективності, надійності та захищеності обміну інформацією в умовах дії завад, втрат пакетів і кіберзагроз різної природи. Запропоновані рішення дозволяють забезпечити адаптивне налаштування параметрів завадостійкого кодування та VPN-протоколів, зменшити рівень помилок передавання даних і підвищити стабільність функціонування мережевих систем.

Практична цінність отриманих результатів дослідження полягає у можливості їх впровадження у таких важливих галузях української економіки:

– безпека та оборона, де інтеграція механізмів завадостійкого кодування та VPN-тунелювання дозволяє забезпечити захищене й стабільне передавання даних

у системах зв’язку, управління, моніторингу та взаємодії безпілотних платформ в умовах активного впливу завад і кіберзагроз;

– інформаційно-телекомунікаційні системи та цифрова інфраструктура, де розроблені моделі й методи можуть бути використані для підвищення надійності функціонування корпоративних мереж, дата-центрів, хмарних сервісів та розподілених інформаційних систем;

– промисловість та автоматизовані системи управління, де застосування адаптивного керування параметрами передавання даних дозволяє забезпечити стабільність обміну інформацією між компонентами автоматизованих і кіберфізичних систем у режимі реального часу;

– транспорт і логістика, де використання запропонованих підходів забезпечує підвищення стійкості телекомунікаційних каналів до помилок і втрат пакетів у системах навігації, диспетчеризації та моніторингу транспортних потоків;

– цифровізація економіки та інформаційна безпека, де запропоновані рішення дозволяють реалізувати гнучке налаштування захищених каналів зв’язку відповідно до вимог користувачів, характеристик мережі та умов функціонування інформаційних систем.За результатами дослідження підтверджено теоретичну обґрунтованість і практичну ефективність запропонованих рішень, що свідчить про завершеність роботи та можливість їх подальшого застосування і розвитку.

Ключові слова: VPN, захищене передавання даних, комп’ютерні мережі, імітаційне моделювання, каскадні коди, адаптивне керування, інформаційна безпека, модель, завадостійкість, безпека даних, кібербезпека, канали передачі даних, цілісність даних, моделювання помилок, якісна пе-редача даних

ABSTRACT

Sharov V.O. Models and methods for ensuring the reliability and security of data transmission in computer networks based on the integration of noise-resistant coding and overlay technologies. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 122 – Computer Science. – National Technical University "Kharkiv Polytechnic Institute", Kharkiv, 2026.

The dissertation is devoted to solving the current scientific and technical problem of increasing the reliability and security of data transmission in computer networks under conditions of interference and cyber threats by developing integrated models, methods and information technology that combine the mechanisms of noise-resistant coding and secure tunneling.

The object of research is the process of data transmission in computer networks in the presence of interference and cyber threats.

The subject of the research is models, methods and information technology for ensuring the reliability and security of data transmission based on the integration of noise-resistant coding and overlay technologies.

The purpose of the research is to increase the efficiency, reliability and security of data transmission by developing and implementing an integrated approach to ensuring their reliability and security.

The introduction substantiates the relevance of the topic, identifies the scientific problem of insufficient effectiveness of the isolated use of protection and noise-resistant means, which does not allow ensuring the required level of data transmission stability in modern networks.

The first section analyzes the current state of methods for ensuring the efficiency, reliability and security of data transmission, identifies their limitations and formulates the scientific task of integrating the relevant mechanisms.

The second section substantiates the system of performance evaluation indicators, develops a conceptual model of a hybrid protected data transmission channel and methods for synthesizing and forming its parameters.

In the third section, models and methods for integrating noise-tolerant coding and overlay technologies are developed, a method for adaptive control of system parameters is improved, and an information technology for multi-level protection is proposed.

In the fourth section, simulation modeling and experimental studies of the effectiveness of the proposed solutions using VPN profiles (in particular, IPsec, OpenVPN, WireGuard) and cascading codes are carried out. The results obtained confirmed the increase in error resistance, reduction of packet loss, and improvement of data transmission stability compared to basic approaches.

The conclusions of the dissertation summarize the results of the research and confirm the achievement of the set goal. The work develops a hybrid model of a secure data transmission channel, methods for channel profile synthesis and adaptive control of system parameters, and also implements information technology for integrating noise-tolerant coding and VPN protocols. The effectiveness of the integrated approach to ensuring the reliability and security of data transmission in conditions of interference, packet loss, and cyber threats is proven. It was established that the joint use of FEC coding and VPN tunneling mechanisms provides increased error resistance, reduced packet loss and stabilization of the data transmission process in difficult network operating conditions.

The research yielded the following scientific results:

– a hybrid model of a secure data transmission channel was enhanced, built on a combination of noise-tolerant coding and VPN tunneling mechanisms, taking into account the impact of interference and cyber threats of various nature, which, unlike existing approaches to the separate use of these mechanisms, ensures their complex interaction and allows to increase the system's resistance to errors and attacks, as well as ensure the stability of data transmission in difficult network operating conditions;

– the method of adaptive adjustment of noise-tolerant coding parameters and overlay protocols based on assessing the network state and data transmission efficiency indicators was improved, which, unlike existing methods with fixed or partially variable parameters, provides coordinated adjustment of the system configuration and allows to increase the efficiency of using network resources and the quality of traffic service;

– the methods for forming a data transmission channel profile and building multi-level protection information technology based on comprehensive consideration of encoding parameters and characteristics of VPN protocols have been further developed, which, unlike existing solutions, provide integrated configuration of system parameters and allow for adaptive configuration of protected communication channels in accordance with operating conditions and requirements for reliability and information security.

The practical significance of the results obtained lies in the direct use of the proposed models, methods and information technology in the construction of secure computer networks and data transmission channels, which results in increased efficiency, reliability and security of information exchange under conditions of interference, packet loss and cyber threats of various nature. The proposed solutions allow for adaptive adjustment of parameters of noise-resistant coding and VPN protocols, reduce the level of data transmission errors and increase the stability of network systems.

The practical value of the obtained research results lies in the possibility of their implementation in the following important sectors of the Ukrainian economy:

– security and defense, where the integration of noise-resistant coding and VPN tunneling mechanisms allows for secure and stable data transmission in communication systems, control, monitoring and interaction of unmanned platforms under conditions of active interference and cyber threats;

– information and telecommunication systems and digital infrastructure, where the developed models and methods can be used to increase the reliability of corporate networks, data centers, cloud services and distributed information systems;

– industry and automated control systems, where the use of adaptive control of data transmission parameters allows to ensure the stability of information exchange between components of automated and cyber-physical systems in real time;

– transport and logistics, where the use of the proposed approaches ensures increased stability of telecommunication channels to errors and packet loss in navigation, dispatching and monitoring systems of transport flows;

– digitalization of the economy and information security, where the proposed solutions allow to implement flexible configuration of protected communication channels in accordance with user requirements, network characteristics and operating conditions of information systems. The results of the study confirmed the theoretical validity and practical effectiveness of the proposed solutions, which indicates the completion of the work and the possibility of their further application and development.

Keywords: VPN, secure data transmission, computer networks, simulation modeling, cascading codes, adaptive control, information security, model, noise immunity, data security, cybersecurity, data transmission channels, data integrity, error modeling, high-quality data transmission

Список публікацій здобувача:

Публікації здобувача за темою дисертації, в яких опубліковані основні наукові результати

1. Шаров В.О., Нікуліна О.М., Северин В.П. Розробка моделі завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами. Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (8), 2022, с. 57–62.

2. Шаров В.О., Нікуліна О.М., Северин В.П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (9)*, 2023, с. 64–69.

3. Шаров В.О., Нікуліна О.М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (11)*, 2024, с. 70–75.

4. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (12)*, 2024, с. 92–97.

5. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (13)*, 2025, с. 112–116.

Опубліковані праці апробаційного характеру:

6. Шаров В.О., Бердніков А.Г. Модель завадостійкого каналу передачі даних. *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2020)*, Харків: ХНУ ім. В.Н. Каразіна, 2020. 4 с.

7. Шаров В.О., Бердніков А.Г. Моделювання коригувального каскадного коду в каналах передачі даних системи управління. *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021)*, Харків: ХНУ ім. В.Н. Каразіна, 2021. 5 с.

8. Шаров В.О., Нікуліна О.М., Лошкарьова С.Є. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: Тези*

доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023, 17-20 травня 2023 р., Харків, НТУ «ХПІ», с. 1048.

9. Шаров В.О., Нікуліна О.М. Модель завадостійкої системи управління з урахуванням штучних перешкод вищого рівня. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: Тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-24 травня* 2024 р., Харків, НТУ «ХПІ», с. 1270.

10. Sharov V.O., Nikulina O.M. The model control system resistant to interference from higher-level artificial sources. *XVIII Міжнар. наук.-практ. конф. магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених», 19–22 листопада* 2024 р., Харків: НТУ «ХПІ», с. 56–57.

ЗМІСТ

Список умовних скорочень

AES-NI – Advanced Encryption Standard New Instructions – Інструкції апаратного прискорення AES

API – Application Programming Interface – Програмний інтерфейс застосунку

ARQ – Automatic Repeat reQuest – Автоматичний запит повторної передачі

ARM CE – ARM Cryptography Extensions – Криптографічні розширення ARM

BCH – Bose–Chaudhuri–Hocquenghem code – Код Боуза–Чоудхурі–Хоквінгема

BER – Bit Error Rate – Ймовірність бітової помилки

CDF – Cumulative Distribution Function – Кумулятивна функція розподілу

CCSDS – Consultative Committee for Space Data Systems – Консультативний комітет з космічних систем передачі даних

CLI – Command Line Interface – Командний інтерфейс

CRC – Cyclic Redundancy Check – Циклічна перевірка надлишковості

CSV – Comma-Separated Values – Формат даних, розділених комами

DPI – Deep Packet Inspection – Глибока інспекція пакетів

DTLS – Datagram Transport Layer Security – Безпека транспортного рівня для дейтаграм

ECDH – Elliptic Curve Diffie–Hellman – Обмін ключами на еліптичних кривих

ECC – Error-Correcting Codes – Коди виправлення помилок

ESP – Encapsulating Security Payload – Навантаження захищеної інкапсуляції (компонент IPsec)

FEC – Forward Error Correction – Пряме виправлення помилок

FER – Frame Error Rate – Ймовірність помилки кадру

HARQ – Hybrid ARQ – Гібридний ARQ

HKDF – HMAC-based Key Derivation Function – Ключова функція витягування на основі HMAC

IETF – Internet Engineering Task Force – Інженерна рада Інтернету

IDS – Intrusion Detection System – Система виявлення вторгнень

IKEv2 – Internet Key Exchange version 2 – Протокол обміну ключами, версія 2

IPS – Intrusion Prevention System – Система запобігання вторгненням

IPI – (у документі – як частина TCP/IP) Internet Protocol Interface – Інтерфейс інтернет-протоколу

iPerf3 – Instrumented Performance Tool 3 – Інструмент вимірювання пропускної здатності мережі

JSON – JavaScript Object Notation – Текстовий формат обміну даними JSON

JNI – Java Native Interface – Інтерфейс Java для виклику нативного коду

KDF – Key Derivation Function – Функція деривації ключа

LDPC – Low-Density Parity-Check – Код з малою щільністю перевіркової матриці

LTE – Long-Term Evolution – Стандарт мобільного зв’язку LTE

L7 – Layer 7 (Application Layer) – 7-й рівень моделі OSI (прикладний)

MSS – Maximum Segment Size – Максимальний розмір сегмента

MTU – Maximum Transmission Unit – Максимальний розмір передавальної одиниці

mKCP – Modified KCP (KCP-протокол зі змінами) – Модифікований транспортний протокол KCP

NAT – Network Address Translation – Трансляція мережевих адрес

PCCC – Parallel Concatenated Convolutional Code (Turbo code) – Паралельно-каскадний згортковий код

pcap4j – Packet Capture for Java – Java-бібліотека для захоплення пакетів

PDU – Protocol Data Unit – Протокольна одиниця даних

PLPMTUD – Packetization Layer Path MTU Discovery – Визначення MTU на рівні пакетизації

PPP – Point-to-Point Protocol – Точковий протокол з’єднання

QC – Quasi-Cyclic (LDPC) – Квазіцилічний (тип LDPC-кодів)

RA – Repeat Accumulate code – Повторно-накопичувальний код

REST – Representational State Transfer – Архітектурний стиль взаємодії в мережі

RS – Reed–Solomon code – Код Ріда–Соломона

RTT – Round-Trip Time – Час проходження пакета туди й назад

RX – Receive – Приймання

SA – Security Association – Параметри безпечного з’єднання (в IPsec)

SC – Successive Cancellation – Послідовне скасування (метод декодування Polar-кодів)

SD-WAN – Software-Defined WAN – Програмно-визначена глобальна мережа

SNR – Signal-to-Noise Ratio – Співвідношення сигнал/шум

TCP – Transmission Control Protocol – Протокол керування передаванням

TCP/IP – Transmission Control Protocol / Internet Protocol – Набір протоколів TCP/IP

TCM – Trellis Coded Modulation – Модульована решіткою модуляція

TLS – Transport Layer Security – Захист транспортного рівня

UDP – User Datagram Protocol – Протокол користувацьких дейтаграм

UDP-scenario – UDP-based scenario – UDP-сценарій

V2Ray – Virtual Router Project (мережева платформа-проксі) – Платформа маршрутизації/проксі V2Ray

VPN – Virtual Private Network – Віртуальна приватна мережа

WireGuard – Назва VPN-протоколу (не абревіатура) – VPN-протокол WireGuard

XRay – Модифікація V2Ray (не абревіатура) – Система XRay

XTLS – Extended TLS – Розширений TLS

YAML – YAML Ain’t Markup Language – Формат структурованих даних YAML

ВСТУП

Актуальність теми дослідження. Стрімкий розвиток цифрових технологій, поширення хмарних сервісів, мобільних мереж нового покоління, систем віддаленого доступу та зростання обсягів мережевого трафіку зумовлюють підвищені вимоги до забезпечення надійності та захищеності передавання даних у комп'ютерних мережах. Сучасні інформаційно-комунікаційні системи функціонують в умовах одночасного впливу випадкових завад каналів зв'язку, перевантажень мережевої інфраструктури та цілеспрямованих кіберзагроз. За таких умов особливого значення набуває забезпечення не лише конфіденційності та цілісності інформації, а й стабільності та безперервності процесів передавання даних.

Теоретичні засади сучасних методів надійного та захищеного передавання даних сформовано у працях К. Шеннона, Р. Хеммінга, Р. Галлагера, Е. Берлекемпа, А. Вітербі, У. Діффі та М. Геллмана. Подальший розвиток методів забезпечення інформаційної безпеки, захищених мережевих технологій і завадостійкого передавання даних здійснено в роботах численних вітчизняних і зарубіжних науковців, присвячених криптографічному захисту інформації, VPN-технологіям, методам контролю цілісності даних, виявлення та виправлення помилок, а також адаптивному керуванню мережевими ресурсами. Водночас більшість існуючих рішень орієнтовані на окремі аспекти забезпечення захищеності або надійності передавання даних та переважно реалізуються на різних рівнях моделі OSI без урахування їх комплексної взаємодії. Це обмежує можливості адаптації таких рішень до умов динамічної зміни характеристик мережі та сучасного ландшафту кіберзагроз.

У зв'язку з цим актуальною є науково-технічна задача розроблення інтегрованих моделей і методів, що поєднують механізми завадостійкого кодування та оверлейних технологій захисту даних, зокрема VPN, у межах єдиного підходу. Така інтеграція дає змогу одночасно підвищити стійкість передавання

даних до випадкових помилок і забезпечити необхідний рівень захищеності інформаційних потоків без суттєвого погіршення продуктивності мережі.

Таким чином, необхідність підвищення ефективності передавання даних у комп'ютерних мережах шляхом комплексного поєднання механізмів забезпечення надійності та захищеності визначає актуальність теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано на кафедрі інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут» відповідно до планів наукових досліджень**.** Результати дисертаційної роботи впроваджені в науково-дослідних роботах: «Розробка математичних моделей та програмних додатків для управління складними системами з використанням штучного інтелекту» (ДР№ 124U001390), «Розробка математичних моделей для оптимізації процесів управління складними динамічними системами з використанням обчислювального інтелекту» (ДР№ 0124U001511), де здобувач був виконавцем.

Мета та задачі дослідження. Метою дисертаційної роботи є підвищення ефективності, надійності та захищеності передавання даних шляхом розроблення та впровадження інтегрованого підходу до забезпечення їх надійності та захищеності.

Для досягнення наміченої мети поставлені такі задачі:

– виконати аналіз сучасного стану методів забезпечення надійності та захищеності передавання даних, визначити їх обмеження та сформулювати наукову задачу інтеграції завадостійкого кодування та оверлейних технологій;

– обґрунтувати систему показників оцінювання ефективності передавання даних та розробити концептуальну модель гібридного захищеного каналу передавання даних;

– розробити методи інтеграції завадостійкого кодування та оверлейних технологій, включаючи метод синтезу профілю каналу та удосконалений метод адаптивного керування параметрами системи;

– реалізувати інформаційну технологію інтеграції завадостійкого кодування та VPN-протоколів, а також провести імітаційне моделювання та експериментальну перевірку ефективності запропонованих рішень.

Об'єкт дослідження – процес передавання даних у комп'ютерних мережах за наявності завад і кіберзагроз.

Предмет дослідження – моделі, методи та інформаційна технологія забезпечення надійності й захищеності передавання даних на основі інтеграції завадостійкого кодування та оверлейних технологій.

Методи дослідження. У роботі використано методи теорії інформації та завадостійкого кодування для аналізу процесів передавання та відновлення даних; методи математичного та імітаційного моделювання для дослідження характеристик гібридного каналу; методи теорії ймовірностей і математичної статистики для оцінювання показників ефективності; методи системного аналізу для побудови інтегрованої інформаційної технології; методи програмної інженерії для реалізації експериментального прототипу системи.

Наукова новизна отриманих результатів полягає у такому:

–удосконалено гібридну модель захищеного каналу передавання даних, побудовану на поєднанні механізмів завадостійкого кодування та VPN-тунелювання з урахуванням впливу завад і кіберзагроз різної природи, яка, на відміну від існуючих підходів до окремого використання зазначених механізмів, забезпечує їх комплексну взаємодію та дозволяє підвищити стійкість системи до помилок і атак, а також забезпечити стабільність передавання даних у складних умовах функціонування мереж;

– удосконалено метод адаптивного налаштування параметрів завадостійкого кодування та оверлейних протоколів на основі оцінювання стану мережі й показників ефективності передавання даних, який, на відміну від існуючих методів із фіксованими або частково змінними параметрами, забезпечує узгоджене коригування конфігурації системи та дозволяє підвищити ефективність використання мережевих ресурсів і якість обслуговування трафіку;

– отримали подальший розвиток методи формування профілю каналу передавання даних і побудови інформаційної технології багаторівневого захисту на основі комплексного врахування параметрів кодування та характеристик VPN-протоколів, які, на відміну від існуючих рішень, забезпечують інтегроване налаштування параметрів системи та дозволяють реалізувати адаптивне конфігурування захищених каналів зв'язку відповідно до умов функціонування й вимог до надійності та інформаційної безпеки.

Практичне значення отриманих результатів полягає у можливості використання розроблених моделей, методів та інформаційної технології для підвищення надійності та захищеності передавання даних у комп'ютерних мережах в умовах дії завад і кіберзагроз, а також для забезпечення стабільності функціонування інформаційно-телекомунікаційних систем.

Розроблені моделі та методи можуть бути використані при проєктуванні захищених каналів зв'язку, оптимізації параметрів завадостійкого кодування та налаштуванні VPN-протоколів у комп'ютерних мережах різного призначення, зокрема в системах управління, розподілених інформаційних системах та мережах із підвищеними вимогами до надійності та інформаційної безпеки.

Запропоновані рішення реалізовано у вигляді експериментального програмного комплексу, що забезпечує моделювання процесів передавання даних, оцінювання ефективності завадостійкого кодування та аналіз впливу параметрів оверлейних технологій на якість обслуговування трафіку.

Матеріали дисертації використані на кафедрі використовуються у навчальному процесі кафедри інформаційних систем та технологій Національного технічного університету «Харківський політехнічний інститут» в спеціальних лекційних курсах «Математичне моделювання та аналіз систем», «Операційні системи мережевих технологій», «Основи комп'ютерних мереж».

Особистий внесок здобувача. Усі основні результати дисертаційної роботи отримані здобувачем самостійно. У наукових роботах, написаних у співавторстві, здобувачеві належить:

А) статті у фахових виданнях України:

[1] – здобувачем розроблено модель завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами, виконано її математичне та імітаційне моделювання й оцінювання ефективності; співавторами Нікуліною О.М. та Севериним В.П. здійснено постановку задачі та узагальнення результатів;

[2] – здобувачем виконано моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем і проведено експериментальні дослідження їх характеристик; співавторами Нікуліною О.М. та Севериним В.П. здійснено методичне забезпечення дослідження та інтерпретацію результатів;

[3] – здобувачем розроблено дворівневу концепцію моделювання єдиної завадостійкої передачі цифрових даних та реалізовано відповідну модель; співавтором Нікуліною О.М. здійснено постановку задачі та узагальнення результатів;

[4] – здобувачем досліджено сумісність методів завадостійкого кодування та протоколів високого рівня, виконано моделювання їх взаємодії та аналіз ефективності; співавтором Нікуліною О.М. проведено узагальнення результатів;

[5] – здобувачем розроблено підхід до багаторівневого захисту в системах передавання даних на основі спільного використання VPN-протоколів і лінійних блокових кодів, виконано експериментальну перевірку ефективності; співавтором Нікуліною О.М. здійснено постановку задачі та інтерпретацію результатів.

Б) матеріали та тези конференцій:

[6] – здобувачем розроблено модель завадостійкого каналу передавання даних та виконано її апробацію; співавтором Бердніковим А.Г. здійснено наукове керівництво та обговорення результатів;

[7] – здобувачем виконано моделювання коригувального каскадного коду в каналах передавання даних систем управління; співавтором Бердніковим А.Г. проведено аналіз і узагальнення результатів;

[8] – здобувачем розроблено гнучку модель завадостійкої передачі даних для управління динамічними системами та проведено її апробацію; співавторами Нікуліною О.М. та Лошкарьовою С.Є. здійснено постановку задачі та узагальнення результатів;

[9] – здобувачем розроблено модель завадостійкої системи управління з урахуванням штучних перешкод вищого рівня та проведено її дослідження; співавтором Нікуліною О.М. здійснено узагальнення результатів;

[10] – здобувачем досліджено модель системи керування, стійкої до завад високого рівня, та виконано аналіз її характеристик; співавтором Нікуліною О.М. здійснено інтерпретацію результатів.

Апробація результатів дисертації. Основні результати дисертаційної роботи, висновки і пропозиції доповідалися і обговорювалися на: Міжнародних науково-технічних конференціях «Комп'ютерне моделювання у наукоємних технологіях» (КМНТ-2020, КМНТ-2021, Харків); XXXI – XXXII Міжнародних науково-практичних конференціях «Інформаційні технології: наука, техніка, технологія, освіта, здоров’я» (MicroCAD-2023, MicroCAD-2024, Харків); XVIII Міжнародній науково-практичній конференції магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених» (2024, Харків).

Публікації. За темою дисертаційної роботи опубліковано 10 наукових праць, у тому числі: 5 статтей – у наукових виданнях, що входять до фахових видань України (категорія Б -5), 5 – у матеріалах апробаційного характеру.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 188 сторінок, у тому числі 61 рисунок, 6 таблиць, список використаних джерел налічує 85 найменувань на 9 сторінок, а також 17 сторінок додатків.

РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ЗАХИЩЕНОСТІ СИСТЕМ ПЕРЕДАЧІ ДАНИХ

1.1 Аналіз сучасних викликів інформаційної безпеки мережевих систем

Стрімкий розвиток цифрових технологій, глобалізація інформаційних процесів і збільшення обсягу переданих даних формують нові умови функціонування мережевих систем. У таких умовах інформаційна безпека стає не лише технічним, а й стратегічним фактором стабільності соціально-економічних систем. Інформаційні ресурси сьогодні є ключовим активом будь-якої організації, а порушення їх конфіденційності, цілісності або доступності здатне призвести до масштабних фінансових збитків, втрати репутації чи навіть загроз національній безпеці.

Зростання кількості підключених пристроїв і розвиток Інтернету речей створюють багаторівневі виклики для безпеки. Кожен вузол мережі потенційно може стати вектором атаки, що суттєво ускладнює задачу комплексного захисту . Проблема ускладнюється тим, що значна частина таких пристроїв має обмежені обчислювальні ресурси, що робить їх неспроможними використовувати класичні криптографічні протоколи.

Актуальною залишається і проблема зростання складності кіберзагроз. Якщо раніше основну небезпеку становили віруси чи примітивні атаки на відмову в обслуговуванні, то сьогодні спостерігається перехід до багатовекторних атак, що поєднують у собі соціальну інженерію, шкідливе програмне забезпечення та мережеві експлойти [1]. Такі атаки здатні обходити традиційні системи захисту і вимагають застосування більш гнучких та інтелектуальних підходів [2].

Зростаюча мобільність користувачів і поширення хмарних сервісів створюють новий тип викликів [3]. Передача даних через публічні канали, а також їх обробка у сторонніх дата–центрах потребують додаткового рівня захисту [4]. Відповідно, у сучасних моделях безпеки важливим є не лише шифрування, а й використання механізмів багаторівневої аутентифікації та контролю доступу.

Одним із ключових викликів інформаційній безпеці залишається зростання кількості кібератак у глобальному масштабі. За статистикою, щороку кількість інцидентів, пов’язаних із несанкціонованим доступом до мережевих систем, зростає на десятки відсотків [5]. Це свідчить про те, що сучасні загрози мають динамічний характер і постійно еволюціонують [6].

Узагальнена класифікація сучасних викликів інформаційній безпеці представлена у таблиці 1.1.

Таблиця 1.1 – Основні виклики інформаційній безпеці мережевих систем

Категорія виклику	Приклад прояву	Потенційні наслідки
Зростання складності атак	Багатовекторні та цільові кібератаки	Компрометація критичних систем, витік даних, загрози для цілісності даних, збільшення доступності даних
Розширення мережевої інфраструктури	Інтернет речей, мобільні пристрої	Збільшення векторів атак, низький рівень захисту
Хмарні технології	Обробка даних у сторонніх середовищах	Ризик порушення конфіденційності та збільшення доступності
Людський фактор	Фішинг, соціальна інженерія	Несанкціонований доступ, втрати фінансових ресурсів
Недосконаліть протоколів	Використання застарілих VPN	Легке блокування, зниження ефективності захисту

Функціонування технології здійснюється з використанням наявної мережевої інфраструктури без порушення сумісності зі стандартним мережевим стеком.

Важливо підкреслити, що загрози інформаційній безпеці мають багаторівневу природу, охоплюючи фізичний, мережевий і прикладний рівні

моделі OSI [7]. Наприклад, на фізичному рівні домінують проблеми перехоплення сигналу та впливу перешкод, тоді як на мережевому рівні поширені атаки на маршрутизацію і протоколи шифрування [8]. На прикладному рівні найчастіше зустрічаються фішинг та експлуатація вразливостей у вебсервісах.

У контексті побудови стійких до збоїв та атак систем особливе значення має інтеграція криптографічних протоколів із механізмами корекції помилок. Це пояснюється тим, що сучасні мережеві системи одночасно піддаються як логічним загрозам (несанкціонований доступ, модифікація даних), так і фізичним (помилки передавання, втрати пакетів). Поєднання цих двох напрямів захисту дозволяє формувати комплексні моделі безпеки, які будуть достатньо стійкими у сучасному середовищі.

1.2 Кібератаки як джерело загроз безпеці комп’ютерних систем

Кібератаки сьогодні є одним із ключових джерел загроз для безпеки комп’ютерних систем, оскільки вони безпосередньо спрямовані на порушення конфіденційності, цілісності та доступності інформаційних ресурсів . Характерною особливістю сучасних атак є їхня динамічність: щодня фіксується поява нових методів і інструментів, які з високою швидкістю поширюються завдяки глобальній мережевій інфраструктурі. Це призводить до того, що традиційні засоби захисту часто не встигають адаптуватися до нових векторів загроз.

За даними Check Point Research, середня кількість кібератак на одну організацію у світі демонструє стійку тенденцію до зростання, що свідчить про постійне ускладнення сучасного ландшафту кіберзагроз. Візуальне представлення кількості кібератак на одну організацію у світі наведене на рисунку 1.1

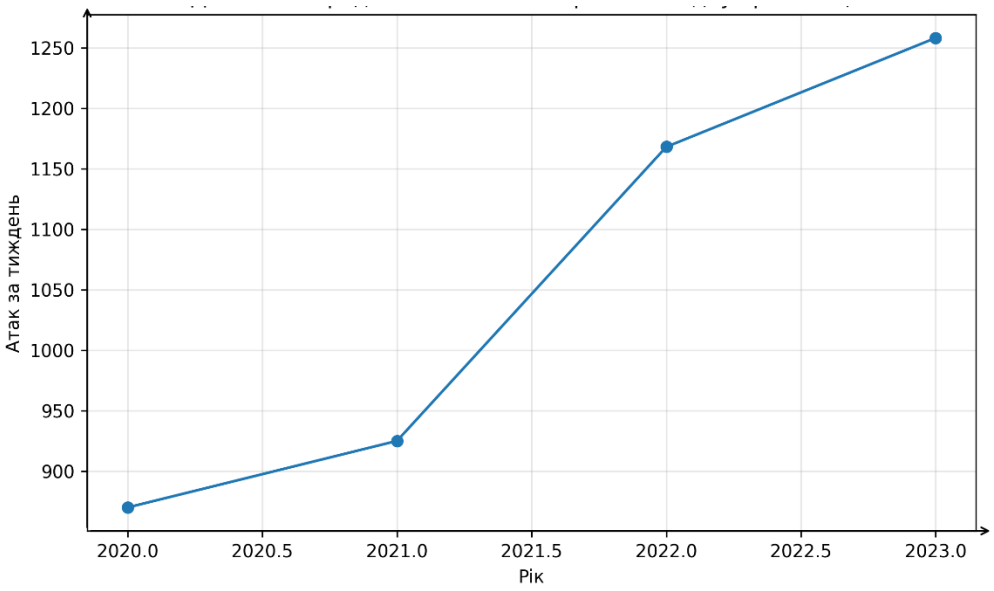


Рисунок 1.1 – Динаміка середньої кількості кібератак на одну організацію у світі (2020–2023 рр.)

Одним із найважливіших аспектів аналізу кібератак є їх класифікація за основними критеріями. До найпоширеніших належать атаки на відмову в обслуговуванні (DoS/DDoS), спрямовані на перевантаження ресурсів системи; атаки, що використовують уразливості протоколів (наприклад, IP spoofing, TCP hijacking); атаки на рівні прикладного програмного забезпечення, зокрема SQL–ін’єкції чи міжсайтове виконання скриптів (XSS). Водночас зростає роль атак соціальної інженерії, які експлуатують психологічні слабкості користувачів для отримання несанкціонованого доступу.

Крім того, сучасні кібератаки дедалі частіше відзначаються комплексним характером. Це означає, що зловмисники комбінують кілька методів – від фішингу до використання шкідливого програмного забезпечення і вразливостей нульового дня – для досягнення поставленої мети. Такий підхід значно підвищує ефективність атак та ускладнює їх виявлення і локалізацію.

Особливу небезпеку становлять атаки на критичну інфраструктуру, зокрема енергетичні системи, транспорт, охорону здоров’я та банківський сектор. Порушення їхньої роботи може призвести не лише до економічних збитків, але й до соціальних чи навіть гуманітарних катастроф. Зважаючи на це, міжнародні

організації, такі як ENISA чи NIST, наголошують на необхідності багаторівневого підходу до захисту та впровадження стійких моделей виявлення й реагування на атаки.

За результатами досліджень, у 2024 році середній розмір збитків від одного витоку даних у світі перевищив 4,5 мільйона доларів США. При цьому основними причинами інцидентів залишаються фішингові кампанії, компрометація облікових даних і атаки на вразливості ПЗ. Така статистика свідчить про те, що кібератаки є не поодинокими подіями, а системним фактором ризику для будь–якої організації.

Узагальнені основні типи кібератак та їхні наслідки наведено у таблиці 1.2.

Таблиця 1.2 – Класифікація основних типів кібератак і їх вплив на комп'ютерні системи

Тип атаки	Характеристика	Можливі наслідки
DoS/DDoS	Перевантаження мережевих ресурсів	Відмова у доступі до сервісів
Атаки на протоколи	Використання уразливостей TCP/IP	Перехоплення сесій, модифікація трафіку
Шкідливе ПЗ	Віруси, трояни, програми-вимагачі	Пошкодження або шифрування даних, фінансові втрати
Соціальна інженерія	Фішинг, маніпуляції користувачами	Викрадення облікових даних, несанкціонований доступ
Експлойти нульового дня [9]	Використання невідомих уразливостей	Компрометація критичних систем

З огляду на масштаби загроз, у багатьох наукових працях пропонується аналізувати кібератаки через призму так званих "поверхонь атаки", що включають фізичний, мережевий та прикладний рівні. Це дозволяє систематизувати потенційні вектори атак і побудувати комплексну систему захисту [10].

На рисунку 1.2 представлено узагальнену схему розподілу кібератак за типами, що дозволяє наочно показати різноманіття загроз і специфіку їх впливу на мережеві системи.

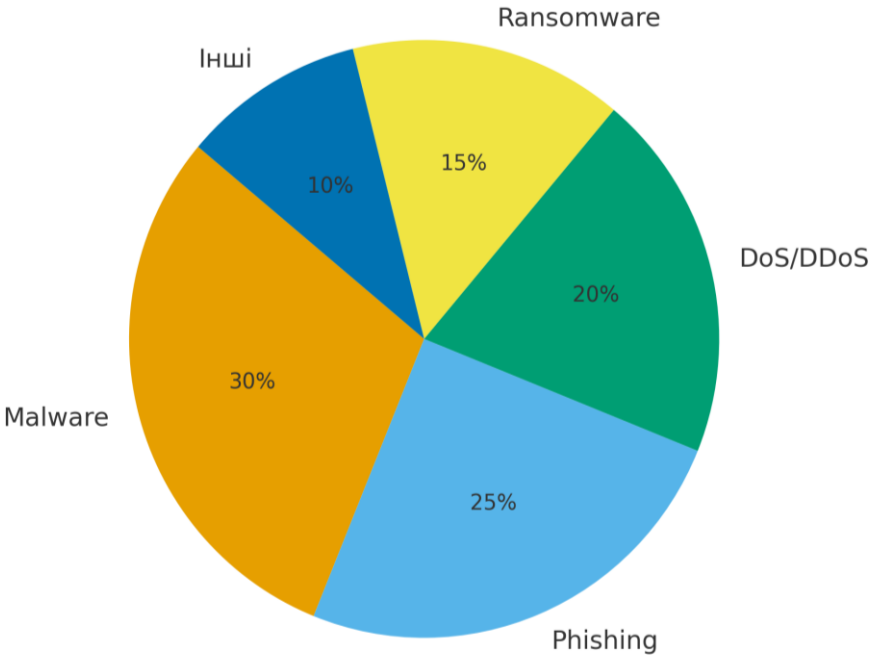


Рисунок 1.2 – Типи кібератак

Таким чином, кібератаки виступають не лише як окремий інцидент, а як постійний фактор, що супроводжує розвиток цифрових технологій [11]. Їхнє зростання у кількісному та якісному вимірах вимагає від дослідників і практиків розробки нових підходів, здатних враховувати не лише відомі методи атак, але й потенційні загрози, що можуть виникнути в майбутньому.

1.3 Концептуальні засади гібридних моделей інформаційної безпеки

Сучасні інформаційно-комунікаційні системи характеризуються високим ступенем складності та динамічності, що обумовлює необхідність формування принципово нових підходів до забезпечення їхнього захисту. У цьому контексті дедалі більшої актуальності набувають гібридні моделі інформаційної безпеки, які поєднують у собі різнорідні методи та механізми протидії загрозам. Основна ідея

гібридності полягає у створенні системи, де окремі елементи взаємодоповнюють один одного, формуючи багаторівневу й стійку архітектуру безпеки.

Зокрема застосовуються методи формування структури даних, методи завадостійкого кодування, методи криптографічного захисту та методи адаптації параметрів передавання.

Одним із ключових принципів побудови гібридних моделей є багаторівневість. Вона передбачає застосування кількох незалежних рівнів захисту, що дозволяє мінімізувати наслідки успішної атаки на один із компонентів системи. Наприклад, навіть якщо зловмиснику вдалося обійти мережевий екран, дані можуть залишатися захищеними завдяки криптографічному шифруванню або механізмам контролю доступу. Такий підхід відомий у світовій практиці як *defense in depth* і вважається одним із базових у сучасних системах кіберзахисту.

Другим важливим принципом є синергетичність. Використання різних методів у межах єдиної архітектури забезпечує не лише додаткові бар'єри для зловмисників, а й створює якісно новий рівень захисту. Наприклад, поєднання VPN-тунелювання з методами завадостійкого кодування дозволяє одночасно гарантувати як конфіденційність, так і цілісність даних . У результаті створюється ефект взаємного підсилення, коли надійність системи перевищує просту суму надійності окремих складових.

Ще одним фундаментальним принципом виступає адаптивність, тобто здатність системи змінювати власні налаштування залежно від актуальних умов та нових загроз. Гібридні моделі мають бути здатними автоматично підвищувати рівень безпеки в умовах виявлення аномалій або підозрілої активності. Для цього активно застосовуються методи машинного навчання, що дозволяють у реальному часі аналізувати трафік і коригувати параметри роботи системи.

Не менш значущим принципом є масштабованість. Сучасні інформаційні системи постійно зростають і змінюються, тому модель захисту повинна легко розширюватися без необхідності повного перероблення архітектури. Це

досягається шляхом модульного підходу, коли кожен компонент гібридної моделі може бути інтегрований або замінений незалежно від інших [12].

Також слід відзначити принцип гнучкої інтеграції. Він передбачає, що різні технології, які входять до складу гібридної моделі, повинні бути сумісними між собою та функціонувати в єдиному інформаційному просторі. У практиці це означає необхідність використання відкритих стандартів і протоколів взаємодії між різними системами безпеки. В іншому випадку існує ризик створення фрагментованої інфраструктури, де окремі елементи захисту не взаємодіють належним чином [13].

З огляду на наведене, можна зробити висновок, що загальні принципи побудови гібридних моделей забезпечення інформаційної безпеки ґрунтуються на поєднанні багаторівневості, синергетичності, адаптивності, масштабованості та гнучкої інтеграції. Саме дотримання цих принципів дозволяє створити інформаційну технологію, здатну ефективно протидіяти сучасним і майбутнім викликам у сфері кібербезпеки.

Сучасні інформаційні системи функціонують у середовищі, де інтенсивність та складність кібератак постійно зростають, що вимагає поєднання різних методів забезпечення безпеки у межах єдиного підходу. Інтеграція різних технологій у єдину інформаційну технологію є необхідним кроком для створення більш гнучкої, масштабованої та ефективної системи захисту. У цьому контексті ключовими є методи тунелювання (зокрема VPN), завадостійке кодування, криптографічні алгоритми та інтелектуальні системи виявлення загроз [14].

Одним із найбільш поширених підходів є використання VPN (Virtual Private Network) для побудови захищених каналів передавання даних. VPN забезпечує конфіденційність інформації шляхом створення зашифрованого тунелю між вузлами мережі, що дозволяє захистити дані від перехоплення навіть у відкритих мережах [15]. Проте VPN не надає абсолютної безпеки: можливі атаки на протоколи шифрування, витоки через вразливості у програмному забезпеченні або

навіть компрометація ключів. Саме тому VPN доцільно розглядати лише як одну з ланок у комплексній гібридній моделі.

Окрім прикладних даних, у процес передавання залучаються службові дані сесії передавання, які містять керувальну інформацію щодо параметрів тунелювання, службових заголовків, ідентифікації пакетів та іншої метаінформації, необхідної для коректної роботи механізмів захисту й відновлення даних.

До вхідних параметрів також належать початкові параметри сеансу зв'язку, які визначають конфігурацію процесу передавання даних, зокрема параметри пакетизації, кодування та тунелювання.

Не менш важливою складовою інтеграції є завадостійке кодування. У системах передавання даних воно відіграє роль додаткового захисного шару, що гарантує збереження цілісності інформації навіть у випадку часткових втрат або спотворень пакетів. Прикладом є використання кодів Хеммінга чи турбокодів, які забезпечують відновлення даних після впливу шумів чи цілеспрямованих атак на канали зв'язку. В умовах інтеграції з VPN технологіями завадостійке кодування дозволяє сформувати багаторівневий захист, де кожен рівень відповідає за окремий аспект – анонімність, конфіденційність, автентичність і цілісність.

Інтеграція також передбачає синхронізацію роботи криптографічних алгоритмів із методами корекції помилок. На практиці це означає, що зашифровані дані додатково захищаються механізмами кодування, здатними відновлювати інформацію навіть після спроб активного впливу на канали передачі. Таким чином досягається подвійний рівень захисту: зловмисник, навіть перехопивши пакети, стикається не лише з криптографічною стійкістю, а й з надлишковістю, закладеною у кодах виправлення помилок.

Особливої уваги заслуговує питання інтеграції інтелектуальних систем аналізу трафіку. Якщо VPN та коди корекції помилок забезпечують захист даних у процесі передавання, то системи на основі машинного навчання дозволяють у режимі реального часу виявляти аномалії, які можуть свідчити про кібератаку. Їхнє поєднання у межах єдиної інформаційної технології дає змогу створити гнучку та

адаптивну архітектуру, здатну одночасно запобігати атакам та відновлювати дані після їхнього впливу.

Прикладом успішної інтеграції є створення прототипів гібридних інформаційних технологій, де VPN використовується як базовий рівень безпеки, поверх якого реалізуються алгоритми корекції помилок і системи автоматичного моніторингу. Такі підходи вже частково впроваджуються у телекомунікаційних мережах нового покоління, зокрема у сегменті 5G та IoT, де важливим є не лише захист від атак, а й стабільність роботи у складних умовах.

Важливо відзначити, що інтеграція технологій вимагає стандартизації та уніфікації протоколів взаємодії. У протилежному випадку виникає проблема сумісності, коли окремі компоненти системи не можуть ефективно обмінюватися інформацією. Тому міжнародні організації, зокрема ISO та ITU-T, активно працюють над розробленням стандартів, які регламентують використання криптографії, VPN та кодів корекції помилок у комплексних системах безпеки [16].

Таким чином, інтеграція різних технологій у межах єдиної інформаційної технології дозволяє створити комплексний захист, що поєднує кілька взаємодоповнюючих рівнів. Поєднання VPN-тунелювання, криптографії, завадостійкого кодування та інтелектуальних систем моніторингу створює основу для нової парадигми гібридних моделей, які здатні протистояти навіть складним багатовекторним кібератакам [17].

З розвитком інформаційних технологій та ускладненням архітектури мережевих систем зростає потреба у системах, здатних не лише захищати дані від перехоплення чи спотворення, але й виявляти та оперативно реагувати на спроби кібератак [18]. Традиційні інструменти, орієнтовані на сигнатурний аналіз або статичне виявлення загроз, поступово втрачають свою ефективність, оскільки сучасні атаки набувають динамічного характеру, часто змінюють свої параметри та використовують складні методи обходу захисту [19,20]. Це створює передумови для переходу до нових моделей виявлення загроз, інтегрованих у комплексні інформаційні технології. Питання оптимізації передавання та завантаження даних

у клієнтських застосунках також розглядаються у роботах Кучука Г.А., де запропоновано математичну модель завантаження 3D-моделей з урахуванням пропускної здатності мережі та затримок обробки [21]. Окремі дослідження також присвячені спеціалізованим методам прихованого передавання службової інформації, зокрема із використанням стеганографічних підходів у каналах зв’язку безпілотних систем [22].

Одним з головних викликів сучасних систем є надлишковість даних, які генеруються мережевими пристроями та сервісами. Традиційні системи IDS/IPS не завжди здатні ефективно обробляти великий обсяг трафіку, що призводить до високого рівня помилкових спрацювань і пропуску реальних атак. У цьому контексті актуальним стає застосування методів машинного навчання та штучного інтелекту, здатних адаптивно аналізувати поведінку мережі, формувати профілі нормального функціонування та виявляти відхилення у режимі реального часу.

Важливою складовою інтеграції є поєднання систем виявлення з іншими шарами захисту, зокрема з VPN та завадостійким кодуванням. У випадку з VPN системи виявлення отримують змогу аналізувати не лише метадані трафіку, а й структуру тунелів, визначаючи потенційні спроби обходу або маніпуляції шифрованими каналами. Додавання ж кодів виправлення помилок ускладнює задачу зловмисників: навіть якщо атака спрямована на порушення цілісності передавання, вбудовані механізми корекції забезпечують відновлення інформації, а системи виявлення фіксують сам факт аномальної активності. Таким чином формується подвійний механізм протидії – превентивний і реактивний.

Питання потокового шифрування та архітектур криптографічного захисту в системах з обмеженими ресурсами детально розглянуті у сучасних дослідженнях CET-операцій [23].

Серед перспективних напрямів розвитку виділяється інтеграція методів поведінкового аналізу та когнітивних обчислень. Такі системи здатні імітувати процеси людського мислення, встановлювати причинно-наслідкові зв’язки між подіями та робити висновки про потенційні атаки на основі неповних даних. Це

дозволяє знизити залежність від наперед визначених сигнатур і робить систему більш стійкою до нових, ще невідомих типів атак.

Додатковим викликом є забезпечення масштабованості. У великих корпоративних мережах та розподілених інфраструктурах (наприклад, у хмарних обчисленнях чи IoT) необхідно інтегрувати системи виявлення у сотні вузлів одночасно. Це вимагає використання розподілених архітектур, де аналіз даних здійснюється як на локальному рівні (edge-computing), так і централізовано у хмарних серверах. Такий підхід дозволяє зменшити затримки у реагуванні та забезпечує більш гнучку адаптацію до специфіки окремих сегментів мережі.

Не менш важливим викликом залишається захист від внутрішніх загроз. У багатьох випадках саме легітимні користувачі або адміністратори, які мають доступ до критичних ресурсів, можуть становити небезпеку для системи. Традиційні IDS/IPS часто орієнтовані на зовнішній трафік, тоді як інтегровані системи повинні також відстежувати внутрішні аномалії, включаючи підозрілу поведінку користувачів або спроби несанкціонованого доступу до службових ресурсів.

Перспективним напрямом є також розвиток гібридних систем виявлення, які поєднують сигнатурні, аномалійні та евристичні методи аналізу. Такі рішення здатні забезпечити баланс між точністю та швидкістю, одночасно зменшуючи кількість хибнопозитивних результатів. При цьому інтеграція з криптографічними технологіями, VPN та завадостійким кодуванням створює багаторівневу модель, що відповідає вимогам сучасних кіберзагроз.

У довгостроковій перспективі очікується, що системи виявлення кібератак трансформуються у комплексні платформи кіберзахисту, де виявлення стане лише одним із модулів. Такі платформи включатимуть автоматичне усунення наслідків атак, динамічне відновлення працездатності системи та навіть прогнозування потенційних загроз на основі аналізу великих даних.

Результатом роботи інформаційної технології є передані та відновлені прикладні дані на стороні приймача.

Таким чином, виклики, що постають перед системами виявлення кібератак, зумовлені необхідністю роботи у складних і динамічних умовах. Їхнє подальше вдосконалення потребує інтеграції з VPN-протоколами, кодами корекції помилок, а також застосування штучного інтелекту та когнітивних обчислень. Це формує основу для створення комплексних інформаційних технологій, здатних протистояти багатовекторним загрозам та забезпечувати надійну безпеку навіть у високонавантажених мережевих середовищах .

Інтеграція VPN-технологій, механізмів виправлення помилок та систем виявлення вторгнень утворює багаторівневу архітектуру інформаційної технології, яка забезпечує комплексний захист даних у розподілених мережах .

Дослідження оцінювання ймовірності помилок під час обробки персональних даних у BPMN-моделях також підтверджують актуальність формалізації процесів забезпечення безпеки [24]. При цьому обов’язково треба враховувати актуальні потреби по софту для різних бізнес-процесів [25].

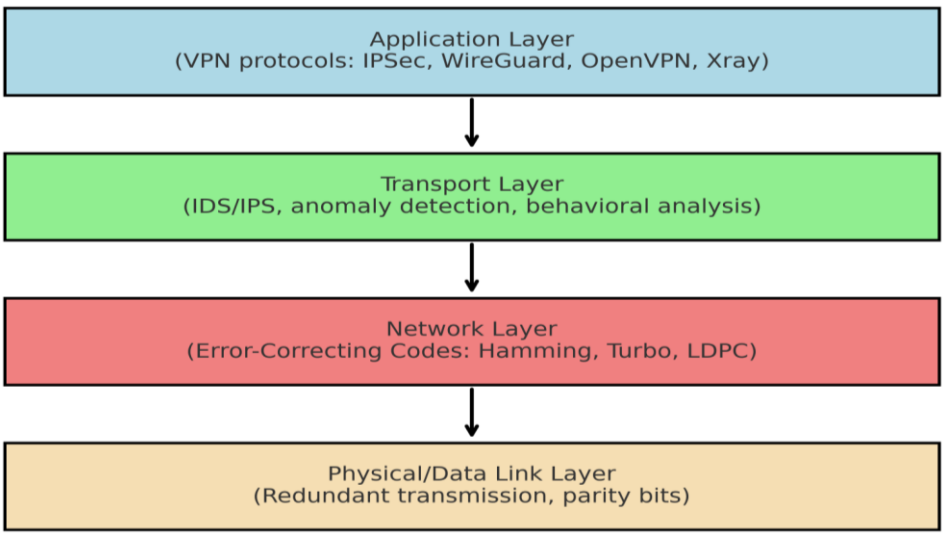


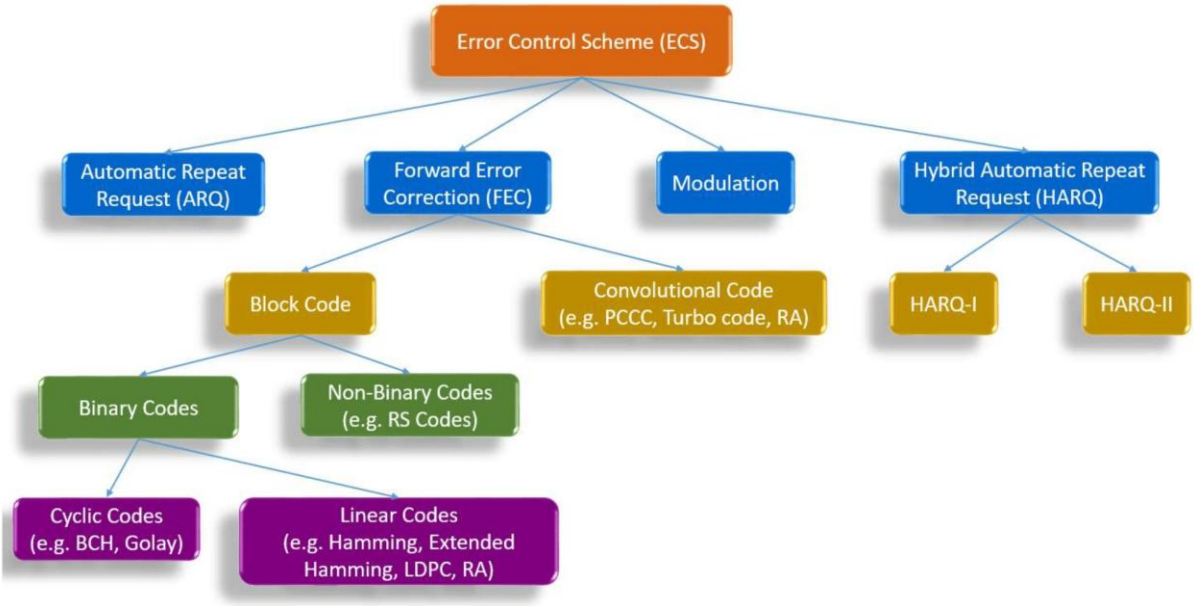
Рисунок 1.3 – Узагальнена схема інтеграції VPN, ECC та IDS/IPS у єдину модель захисту

1.4 Завадостійке кодування для підсилення надійності фізичного рівня

Завадостійке кодування є надзвичайно різноманітною та багаторівневою галуззю, яка розвивається вже кілька десятиліть. Існують різні підходи до класифікації кодів, що застосовуються для контролю та виправлення помилок у цифрових системах передавання даних. Найбільш загальною можна вважати схему Error Control Scheme (ECS), де всі методи контролю помилок поділяються на кілька основних груп:

- Automatic Repeat reQuest (ARQ) – методи повторної передачі, коли виявлена помилка призводить до запиту повтору пакета.
- Forward Error Correction (FEC) – виправлення помилок на основі надлишкових кодів, що дозволяють відновити початкову інформацію без повтору передачі.
- Hybrid ARQ (HARQ) – комбінація ARQ та FEC, яка поєднує переваги обох підходів.
- Modulation schemes – методи, що інтегрують корекцію помилок із модуляцією, утворюючи комплексні системи на фізичному рівні.

У межах ECS особливе місце займають блокові та згорткові коди. На рисунку 1.4 наведено загальну схему ECS, яка демонструє різні рівні класифікації, включаючи блокові коди (бінарні, небінарні, циклічні, лінійні) та згорткові коди (Turbo, RA, PCCC). У результаті формуються кількісні показники надійності передавання, що характеризують рівень втрат та імовірність успішного відновлення.



Рисунку 1.4 – Загальна класифікація схем контролю помилок

Ще одним поширеним способом класифікації є розподіл за типами FEC-кодів. У даному підході виділяють три головні категорії: блокові коди (linear, non-linear, cyclic, LDPC, BCH, Reed-Solomon, Hamming, Golay); згорткові коди (включно з Trellis Coded Modulation та Turbo-кодами); техніки модульованого кодування (Coded Modulation techniques).

Ця класифікація дозволяє побачити як еволюцію від простих кодів Хеммінга до сучасних LDPC та Turbo-кодів, так і зв’язок між різними напрямами розвитку кодування. Вона наведена на рисунку 1.5.

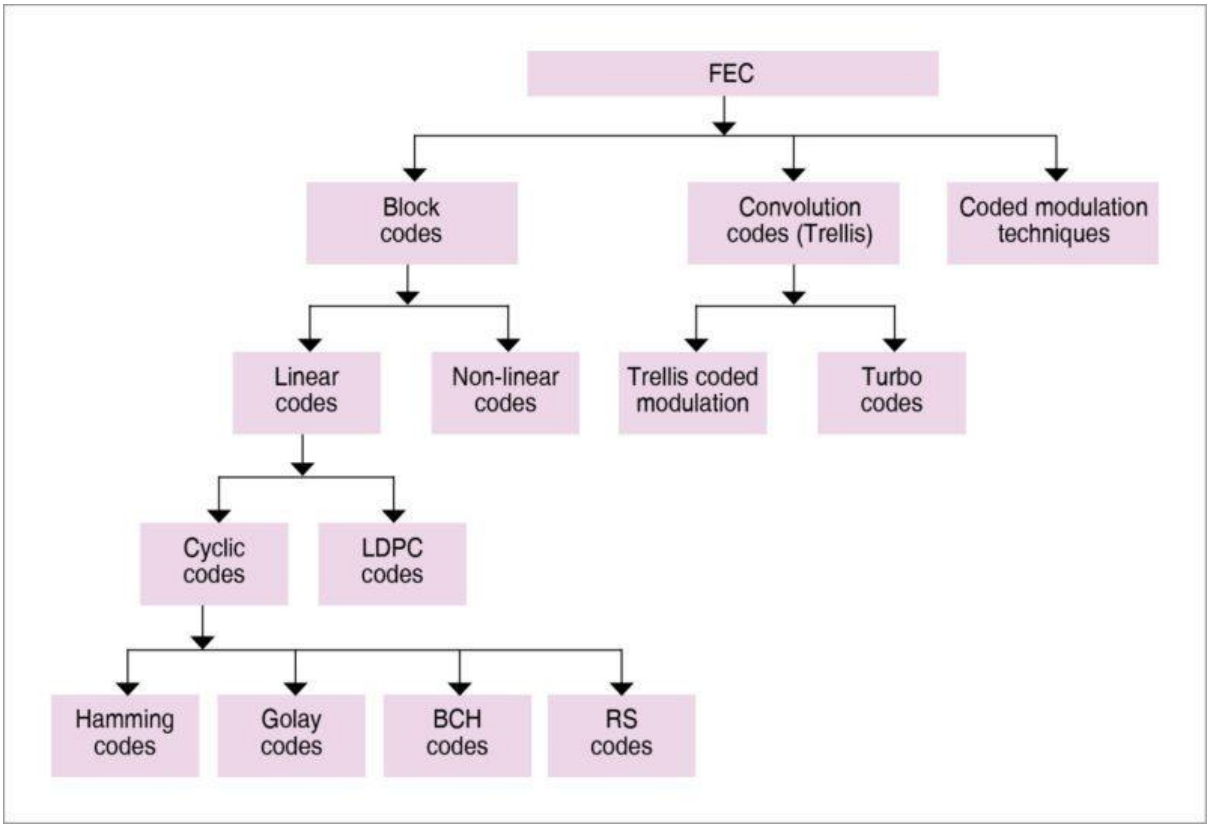


Рисунок 1.5 – Класифікація кодів у межах FEC

Таким чином, представлені схеми демонструють різні підходи до систематизації кодів: ECS – як універсальна модель контролю помилок, а FEC-орієнтована схема – як детальна ієрархія завадостійких кодів. Разом вони дають повне уявлення про сучасний стан методів забезпечення надійності передавання даних.

Забезпечення надійності передавання даних у мережах будь-якого рівня базується на фундаментальному положенні теорії інформації, сформульованому Клодом Шенноном у 1948 році, відповідно до якого в каналі із завадами можливо забезпечити безпомилкову передачу інформації, якщо швидкість передавання даних не перевищує так звану пропускну здатність каналу. Саме цим твердженням було закладено підґрунтя розвитку методів завадостійкого кодування, які й сьогодні є невід'ємною складовою фізичного рівня сучасних систем зв'язку.

Завадостійке кодування (ЗСК) базується на ідеї введення надмірності у вихідний потік даних. Надмірність означає, що до корисної інформації додаються

додаткові біти, завдяки яким приймач може виявляти та, в багатьох випадках, виправляти помилки, спричинені завадами, флуктуаціями сигналу або зловмисними діями. Важливим теоретичним показником у цьому контексті є кодова відстань (мінімальна відстань Хеммінга між будь-якими двома допустимими кодовими словами). Відстань Хеммінга визначає здатність коду до виявлення та виправлення помилок: код із відстанню d може гарантовано виявляти $d-1$ помилку та виправляти $\left[\frac{d-1}{2}\right]$ помилок .

Загальна ідея роботи ПСК полягає в тому, що на передавальному боці виконується кодування повідомлення з використанням визначеного коду, після чого передані дані проходять канал, у якому вони піддаються впливу шумів, завад чи атак. На приймальному боці реалізується процедура декодування, яка дозволяє відновити початкове повідомлення з певною ймовірністю успіху. У класичному випадку декодування може бути жорстким (hard decision) – коли кожен прийнятий біт трактують як 0 або 1, або м’яким (soft decision) – коли декодер працює з імовірностями приналежності біта до певного значення.

Важливим аспектом теорії ПСК є компроміс між рівнем надійності та швидкістю передавання. Введення надмірних бітів знижує ефективну пропускну здатність каналу, проте підвищує стійкість системи до помилок. У практичних системах проектувальники завжди мають знайти баланс між цими параметрами: надмірність має бути мінімальною, але достатньою для досягнення заданого рівня надійності.

Ключовим критерієм ефективності завадостійких кодів є показник ймовірності бітової помилки (BER – Bit Error Rate), що визначає частку неправильно переданих бітів від загальної кількості. Інший важливий показник – ймовірність помилки кадру (FER – Frame Error Rate), яка відображає ймовірність того, що весь блок даних буде пошкоджений настільки, що декодування стане неможливим. Для оцінки ефективності коду зазвичай будують залежності BER від співвідношення сигнал/шум (SNR) при застосуванні різних методів кодування.

З точки зору архітектури мережевих систем, методи ПСК найчастіше застосовуються на фізичному рівні моделі OSI або на першому рівні TCP/IP, де забезпечують цілісність бітового потоку в умовах завад. Проте у випадках багаторівневого підходу частина функцій ПСК може бути інтегрована і на канальному рівні (наприклад, у технологіях Wi-Fi, LTE), що дозволяє підвищувати надійність уже на етапі формування кадрів.

Таким чином, основи ПСК формують фундаментальні механізми для забезпечення стійкості інформаційних систем до випадкових та цілеспрямованих помилок. Надмірність, кодова відстань, алгоритми кодування та декодування, а також компроміси між швидкістю й надійністю становлять теоретичний базис, на якому ґрунтується подальший розвиток сучасних методів і практичних рішень у сфері інформаційної безпеки.

Сучасні мережеві системи функціонують у середовищі, де якість каналів передачі даних може значно відрізнятися залежно від фізичних характеристик середовища, використовуваних технологій доступу та рівня завад. У цьому контексті саме методи завадостійкого кодування стають базовим інструментом забезпечення надійності передачі інформації. Від простих бітових кодів, таких як коди з парністю чи класичні коди Хеммінга, дослідження поступово перейшло до більш потужних підходів, включаючи циклічні коди (CRC), коди Боуза-Чоудхурі-Хоквінгема (BCH), Ріда-Соломона, турбокоди та LDPC-коди.

CRC-коди використовуються у більшості протоколів передачі даних на канальному рівні (Ethernet, Wi-Fi, USB тощо), забезпечуючи швидке виявлення помилок без значного збільшення надмірності. Однак їхня головна функція полягає у детекції помилок, а не у їх виправленні, що обмежує їх застосування у випадках з високим рівнем завад. Натомість BCH- і коди Ріда-Соломона дозволяють виправляти цілі групи бітових чи символних помилок, що робить їх незамінними в телекомунікаційних стандартах, зокрема в супутниковому зв’язку, DVD-носіях та мобільних мережах .

Одним із фундаментальних понять у теорії інформації є межа Шеннона, яка визначає максимально можливу пропускну здатність каналу зв’язку за наявності шуму. Ця межа формулюється через теорему Шеннона про каналову ємність: для будь-якого каналу з пропускною здатністю C (у біт/с) передача даних з імовірністю помилки, що прямує до нуля, можлива лише за умови, що швидкість передавання R не перевищує C. Іншими словами, якщо швидкість перевищує межу Шеннона, то жодні методи кодування не забезпечать гарантовано достовірну доставку повідомлень.

Завадостійке кодування відіграє ключову роль у наближенні до цієї межі. Наприклад, блокові коди, такі як коди Хеммінга, демонструють достатню ефективність лише при роботі на відстані від межі Шеннона, забезпечуючи захист від одиничних чи подвійних помилок, але не здатні ефективно працювати у каналах із високим рівнем шуму. Конволюційні коди дозволяють досягати кращих результатів завдяки послідовному використанню пам’яті та ітераційного декодування, однак їхня продуктивність усе ж таки залишається помітно нижчою від теоретичної межі.

Найбільш значний прорив відбувся з появою турбокодів та LDPC-кодів, які забезпечують роботу на відстані кількох десятих децибела від межі Шеннона. Це стало можливим завдяки використанню ітераційних алгоритмів декодування, що ґрунтуються на обміні ймовірностями між частинами кодувальної схеми. Внаслідок цього такі коди вважаються сучасним стандартом для застосування у високошвидкісних мережах зв’язку, супутникових та мобільних системах.

Таким чином, дослідження межі Шеннона має не лише теоретичне, а й прикладне значення. Воно дозволяє визначати, наскільки близькими до оптимальних є ті чи інші методи кодування, а також орієнтуватися у виборі алгоритмів для практичних систем.

Особливе місце у сучасних дослідженнях займають турбокоди та LDPC-коди, які забезпечують близьку до межі Шеннона ефективність передачі інформації. Турбокоди активно використовуються в стандартах 3G/4G, тоді як

LDPC-коди стали основою технологій 5G та Wi-Fi 6, завдяки своїй здатності обробляти великі обсяги даних із мінімальними втратами. Порівняльний аналіз показує, що LDPC-коди забезпечують кращу масштабованість і продуктивність у високошвидкісних системах, тоді як турбокоди мають переваги у сценаріях із низьким співвідношенням сигнал/шум.

У науковій літературі відзначається, що застосування комбінаційних підходів, коли корекційні коди поєднуються з криптографічними протоколами верхніх рівнів, дозволяє значно підвищити загальну стійкість до як фізичних, так і логічних загроз. Наприклад, впровадження завадостійкого кодування після криптографічного шифрування в рамках VPN дозволяє зберегти цілісність зашифрованих пакетів навіть у разі наявності шуму на фізичному рівні, тоді як традиційні VPN-пакети при пошкодженні окремих бітів стають непридатними для дешифрування.

Варто підкреслити, що оцінка ефективності методів корекції помилок у мережевих системах повинна здійснюватися не лише за кількістю виявлених і виправлених бітів, але й за такими критеріями, як латентність обробки, обчислювальні витрати та сумісність із існуючими протоколами. Так, LDPC-коди демонструють відмінні показники стійкості, проте вимагають складної реалізації та значних ресурсів, тоді як коди Ріда-Соломона лишаються компромісним рішенням для систем, де потрібна збалансованість між швидкістю та надійністю.

Таким чином, сучасна парадигма розвитку систем передачі даних передбачає багаторівневий підхід, у якому різні типи завадостійких кодів застосовуються залежно від специфіки середовища та вимог до швидкості чи надійності. З огляду на перспективи впровадження нових поколінь мобільного зв’язку та інтернету речей, можна очікувати подальшого поширення LDPC- та гібридних кодів у комбінації з криптографічними технологіями для побудови комплексних захищених каналів.

Порівняльну характеристику сучасних методів завадостійкого кодування сформовано на основі аналізу фундаментальних праць Р. Хеммінга, Р. Галлагера,

А. Хоквенгема, Р. Боуза, І. Ріда, Г. Соломона та досліджень К. Берру з турбокодування. Узагальнені результати щодо надмірності, коригувальної здатності, обчислювальної складності та сфер практичного застосування кодів наведено в табл. 1.3.

Таблиця 1.3 – Порівняльна характеристика сучасних методів завадостійкого кодування

Код	Надмірність	Виправлення помилок	Швидкодія обробки	Типові застосування
Хеммінга	Низька	Поодинокі біти	Дуже висока	Комп’ютерна пам’ять, прості канали
CRC	Низька	Лише виявлення	Дуже висока	Ethernet, Wi-Fi, USB, мережеві протоколи
BCH	Середня	Кілька бітових помилок	Висока	Супутниковий зв’язок, флеш-пам’ять
Ріда-Соломона	Середня-висока	Символьні та групові помилки	Середня	DVD, мобільний зв’язок, цифрове ТБ
Турбокоди	Висока	Дуже ефективне при низькому SNR	Середня-низька	3G/4G, супутникові канали
LDPC	Висока	Дуже ефективне, близьке до межі Шеннона	Середня (вимагає значних ресурсів)	5G, Wi-Fi 6, високошвидкісні системи

Завадостійкі коди мають різну ефективність залежно від умов застосування та відстані до теоретичної межі Шеннона. Для наочності на рисунку наведено

порівняння ефективності класичних та сучасних методів кодування в координатах "енергетична ефективність – відносна швидкість коду".

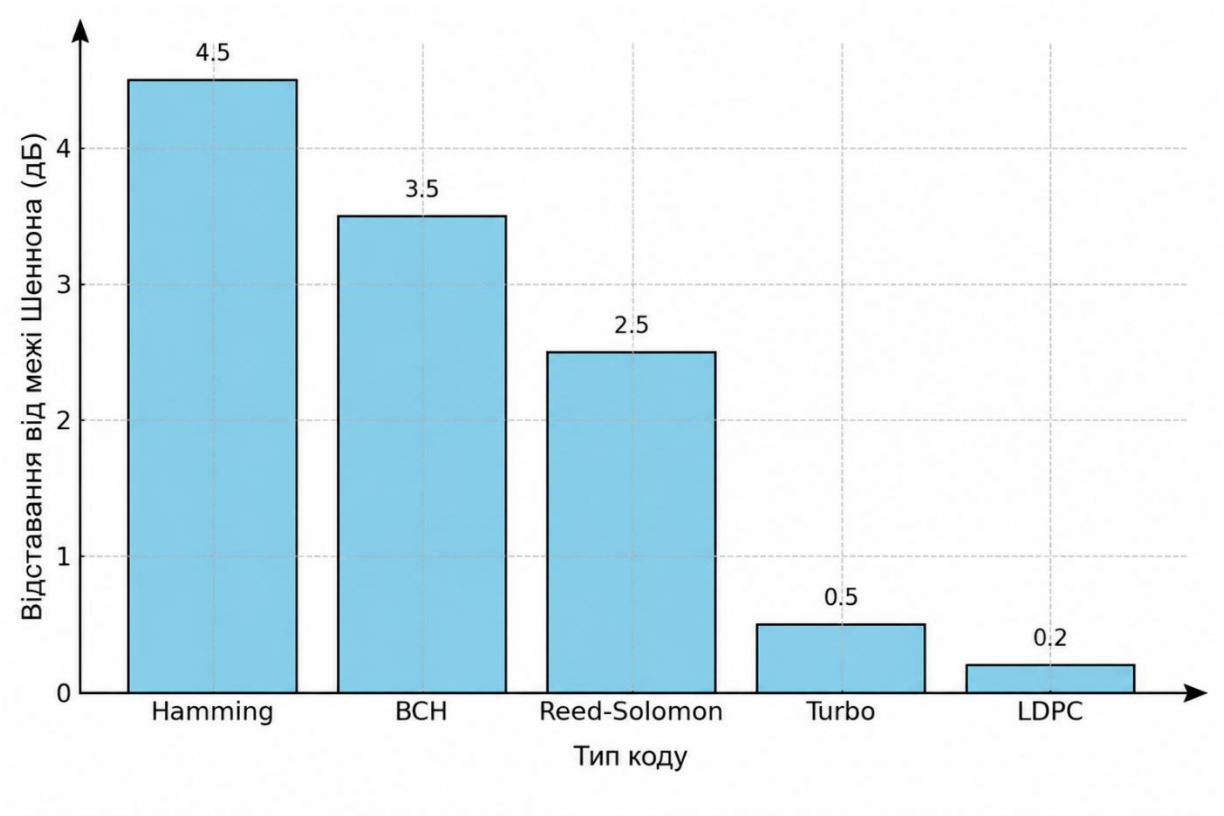


Рисунок 1.6 – Порівняння ефективності різних завадостійких кодів відносно межі Шеннона

Як видно з рисунка 1.6, коди Хеммінга, хоча й мають низьку складність реалізації, забезпечують відносно невисоку енергетичну ефективність. Конволюційні коди дещо покращують результат, однак для досягнення високих показників потрібні турбокоди та LDPC-коди, які наближаються до межі Шеннона. Це підтверджує тенденцію до переходу від простих блокових кодів до гнучкіших і складніших рішень, що дозволяють досягти вищого рівня надійності без суттєвої втрати швидкодії.

Застосування завадостійких кодів у сучасних телекомунікаційних системах вийшло за межі класичного «виправлення помилок». Сьогодні вони є невід’ємним

елементом архітектури безпеки, оскільки впливають на цілісність, доступність та навіть конфіденційність інформації.

Роль у багаторівневій моделі OSI:

- Фізичний рівень. Тут завадостійкі коди працюють як бар'єр проти шуму, знижуючи ймовірність спотворення даних під час передавання по дротових і бездротових каналах. Наприклад, LDPC-коди у Wi-Fi 6 дозволяють підтримувати стабільний зв'язок навіть у перевантажених середовищах.
- Канальний рівень. Використання CRC у поєднанні із завадостійкими кодами забезпечує механізм раннього виявлення маніпуляцій із пакетами. Це підсилює протидію атакам типу *frame injection* чи *bit-flipping*.
- Мережевий та транспортний рівні. Хоча ECC безпосередньо не реалізуються тут, надійність нижчих рівнів зменшує потребу в повторних передачах, що знижує ризик *DoS-атак через перевантаження каналів*.
- Рівень сеансів і вище. На прикладі VPN-контейнерів можна побачити, як коди забезпечують цілісність даних до моменту шифрування. Це унеможливлює використання «битових помилок» для розкриття криптографічних ключів.

Взаємозв'язок із криптографією та безпекою. Завадостійкі коди не є засобом шифрування, але вони доповнюють його. У поєднанні з криптографічними протоколами (TLS, IPsec, WireGuard) вони виконують роль захисної підстилки, яка: забезпечує доставку коректних даних до шифрувальних блоків (виключає помилки, які можуть бути використані як вектор атаки); створює додатковий рівень захисту від атаки на основі диференційного аналізу трафіку, ускладнюючи виділення закономірностей; дозволяє реалізувати стійкість до помилок у критично важливих мережах (банківські транзакції, системи управління енергетикою, оборонні комплекси).

Ключові практичні напрями застосування: Мобільний зв'язок (4G/5G/6G). У 5G NR використання LDPC (для даних) та полярних кодів (для керування) забезпечує синергію високої пропускної здатності та низьких затримок. Це

критично для автономного транспорту та телемедицини. Космічні системи. Коди Ріда-Соломона у поєднанні з турбокодами стали стандартом для NASA та ESA, дозволяючи уникати втрат інформації у далеких космічних місіях, де повторна передача даних неможлива. VPN та корпоративні мережі. Приклад: у фінансових компаніях коди інтегруються в апаратні VPN-шлюзи для захисту від *data corruption attacks*. Вони стають невидимим, але критичним шаром безпеки. IoT-системи. У сенсорних мережах (розумні міста, медицина) енергоспоживання обмежене. Використання завадостійких кодів дозволяє зменшити повторні передачі, тим самим подовжуючи час роботи сенсорів. Хмарні та CDN-сервіси. При передаванні великих обсягів мультимедіа (відео 4K/8K) застосування кодування на рівні сегментації пакетів забезпечує стабільність потоків навіть у випадку втрат частини пакетів.

До механізмів реалізації також належать обчислювальні ресурси вузлів, зокрема процесорні потужності та обсяги оперативної пам’яті.

Аспекти протидії атакам. Bit-flipping attacks. Завадостійкі коди знижують ефективність атак, де зловмисник змінює окремі біти у потоці. Replay-атаки. Завдяки кодам можна швидше виявити дублікати, адже вони не збігаються з контрольними сумами. Side-channel атаки. Завадостійке кодування у поєднанні з криптографією ускладнює отримання побічних сигналів через стабільність структури даних. Для підвищення семантичної якості моделей можуть використовуватись спеціалізовані програмні засоби автоматизованого аналізу [26]. Архітектурні підходи до побудови безпечних систем зберігання та передавання конфіденційної інформації також активно досліджуються у сучасних роботах українських науковців [27].

1.5 Аналіз сучасних VPN-протоколів

Розвиток VPN-технологій тісно пов’язаний з еволюцією мережевих протоколів та потребами у забезпеченні безпеки корпоративних і глобальних комунікацій. Початково віртуальні приватні мережі створювалися як інструмент

для безпечного доступу до корпоративних ресурсів через публічний Інтернет, однак з часом перетворилися на універсальний механізм захисту конфіденційності, цілісності та автентичності даних.

Виникнення перших протоколів: PPTP, L2TP та IPSec. PPTP (Point-to-Point Tunneling Protocol) був розроблений компанією Microsoft у середині 1990-х як розширення PPP-протоколу. Він забезпечував просте тунелювання трафіку через Інтернет, проте мав серйозні вразливості: слабку криптографію (MPPE, RC4), відсутність належної перевірки цілісності й стійкого механізму автентифікації. Це робило PPTP швидким, але небезпечним для використання у середовищах з високими вимогами до захисту.

L2TP (Layer 2 Tunneling Protocol) став наступним етапом розвитку. Він об’єднав можливості L2F (Cisco) та PPTP (Microsoft), дозволяючи інкапсулювати пакети PPP у UDP. L2TP не мав власних засобів шифрування, тому на практиці часто застосовувався разом з IPSec («L2TP/IPSec»). Це рішення суттєво підвищувало безпеку, але ускладнювало архітектуру.

IPSec (Internet Protocol Security) з’явився наприкінці 1990-х як універсальний набір протоколів безпеки на мережевому рівні (OSI Layer 3). Його особливістю є можливість прозорого захисту IP-трафіку, незалежно від прикладних протоколів. IPSec використовує такі механізми: AH (Authentication Header) – автентифікація та контроль цілісності пакетів; ESP (Encapsulation Security Payload) – шифрування та цілісність; IKE (Internet Key Exchange) – протокол узгодження ключів. IPSec отримав широке поширення у корпоративних мережах завдяки високому рівню захисту, але відзначався складністю конфігурації та значними накладними витратами на обчислення.

Щодо існуючих архітектурні підходів інформація береться з RFC 2637 (PPTP), RFC 2661 (L2TP), RFC 4301 та RFC 4303 (IPSec). VPN складається з: тунелювання, інкапсуляції, автентифікації:

- тунелювання: полягає у створенні «віртуального каналу» поверх існуючої мережі. У цьому каналі дані передаються у зашифрованому вигляді,

приховуючи їх від зовнішніх спостерігачів. PPTP і L2TP реалізовували тунелювання на канальному рівні (L2), тоді як IPSec – на мережевому рівні (L3);

- інкапсуляція: пакети оригінального протоколу «загортаються» у новий протокол із власними заголовками. Це дозволяє приховати структуру трафіку й забезпечити його доставку навіть через несумісні середовища. Приклад: інкапсуляція PPP у GRE для PPTP або використання ESP в IPSec;
- автентифікація: підтвердження автентичності користувачів та пристроїв. У PPTP застосовувалася слабка схема MS-CHAPv2, тоді як IPSec використовував більш надійні методи – сертифікати X.509, Kerberos, або попередньо розподілені ключі.

Ключові особливості старих протоколів: швидкість проти безпеки:

- PPTP: забезпечував високу швидкість через мінімальні накладні витрати на шифрування, проте вже на початку 2000-х був визнаний небезпечним через можливість розкриття ключів RC4 і вразливість MS-CHAPv2.
- L2TP/IPSec: суттєво підвищував захист, але через подвійний рівень інкапсуляції та криптографічну складність мав помітні втрати продуктивності, особливо на повільних з’єднаннях.
- IPSec: став стандартом де-факто для організаційних VPN, але його складність конфігурації і значні обчислювальні навантаження стимулювали пошук нових, більш легких рішень (наприклад, OpenVPN і пізніше WireGuard).

Таким чином, перші VPN-протоколи сформували основу для сучасних підходів до захищеної комунікації: вони заклали баланс між швидкістю, простотою використання і рівнем безпеки, який у подальшому став одним із головних критеріїв вибору VPN-технологій.

Надалі порівняємо сучасні інструменти побудови захищених тунелів – IPSec, OpenVPN, WireGuard та екосистемних рішень на зразок V2Ray/XRay. Аналіз охоплює технічні відмінності, метрики безпеки та продуктивності, а також показує практичні компроміси при виборі протоколу.

Розглянемо технічні відмінності і архітектурні особливості кожного з протоколів.

IPSec працює на мережевому рівні OSI (L3) та зазвичай реалізується безпосередньо в ядрі операційної системи або в мережевому стеку. Такий підхід дозволяє захищати весь IP-трафік незалежно від прикладних протоколів і сервісів. Основними компонентами IPSec є AH (Authentication Header), ESP (Encapsulation Security Payload), а також протоколи обміну ключами IKEv1 та IKEv2. Особливо поширеним є IKEv2 (RFC 7296), який забезпечує узгодження параметрів безпеки, підтримку MOBIKE, автоматичне оновлення ключів і повторну автентифікацію. У сучасних реалізаціях використовуються AES-GCM, AES-CBC у поєднанні з HMAC, а також режими AEAD і апаратне прискорення AES-NI. До переваг IPSec належать високий рівень стандартизації, сумісність із великою кількістю мережевого обладнання та підтримка різних механізмів автентифікації, зокрема сертифікатів X.509, PSK і EAP. Недоліками є складність налаштування, додаткове навантаження на систему при відсутності апаратного прискорення та необхідність використання NAT-T у мережах із NAT

OpenVPN працює поверх UDP або TCP у просторі користувача та використовує інтерфейси tap/tun для організації тунелювання на рівні L2 або L3. Архітектура рішення базується на використанні TLS через OpenSSL або LibreSSL для автентифікації сторін і встановлення захищеного каналу. Після завершення TLS-узгодження передавання IP-пакетів здійснюється через сформований тунель. Найчастіше застосовуються AES-256-GCM, TLS 1.2 або TLS 1.3 та HMAC. Основними перевагами OpenVPN є широка підтримка різних платформ, гнучкі можливості конфігурації та здатність працювати через TCP, що є корисним в умовах мережевих обмежень або цензури. Крім того, протокол давно використовується на практиці та вважається стабільним і добре перевіреним рішенням. До недоліків належать підвищені затримки через роботу в просторі користувача, значні накладні витрати TLS-узгодження та залежність від криптографічних бібліотек, у яких можуть виявлятися вразливості.

WireGuard є мінімалістичним VPN-протоколом, який фактично працює як L3-тунель і в Linux реалізується безпосередньо в ядрі. В інших операційних системах застосовуються окремі модулі або бібліотеки. Криптографічна модель побудована на сучасному стеку Noise Protocol Framework і використовує Curve25519 для ECDH, ChaCha20-Poly1305 для AEAD-шифрування, BLAKE2s для хешування та HKDF для генерації ключів. На відміну від IPSec, WireGuard не використовує складні механізми узгодження політик, а конфігурація базується на простій моделі обміну ключами. Перевагами WireGuard є невелика кодова база, висока продуктивність, низькі затримки та відносна простота налаштування. Протокол також демонструє хорошу роботу в умовах NAT завдяки використанню UDP і механізмів keepalive. Серед недоліків варто відзначити обмежену кількість корпоративних функцій, зокрема відсутність розвинених механізмів керування сертифікатами й політиками маршрутизації, а також складність роботи через проксі або системи глибокого аналізу трафіку без додаткових рішень.

V2Ray та XRay належать до екосистем проксі-систем прикладного рівня (L7), орієнтованих насамперед на обходження блокувань, гнучку маршрутизацію трафіку та маскування мережевої активності. Їхня архітектура є модульною та включає окремі транспортні, маршрутизуючі й мережеві компоненти. Підтримуються різні механізми обфускації та транспортування, зокрема mKCP, WebSocket, HTTP/2, TLS, XTLS і ShadowTLS. Такі рішення можуть використовуватися як разом із VPN-тунелями, так і окремо в мережах із жорсткими обмеженнями або DPI. До переваг належать висока гнучкість конфігурації, можливість обходу систем фільтрації та підтримка складних правил маршрутизації. Недоліками є складність налаштування, велика кількість різних реалізацій і форків, а також обмежена придатність для класичних корпоративних VPN-сценаріїв.

З плином часу протоколи ставали дедалі складніше, еволюціонували, тому зрозуміло, що новіші протоколи мають сучасні переваги, тому що базуються на досконаліших технологіях. Побачити еволюцію можно на рисунку 1.7

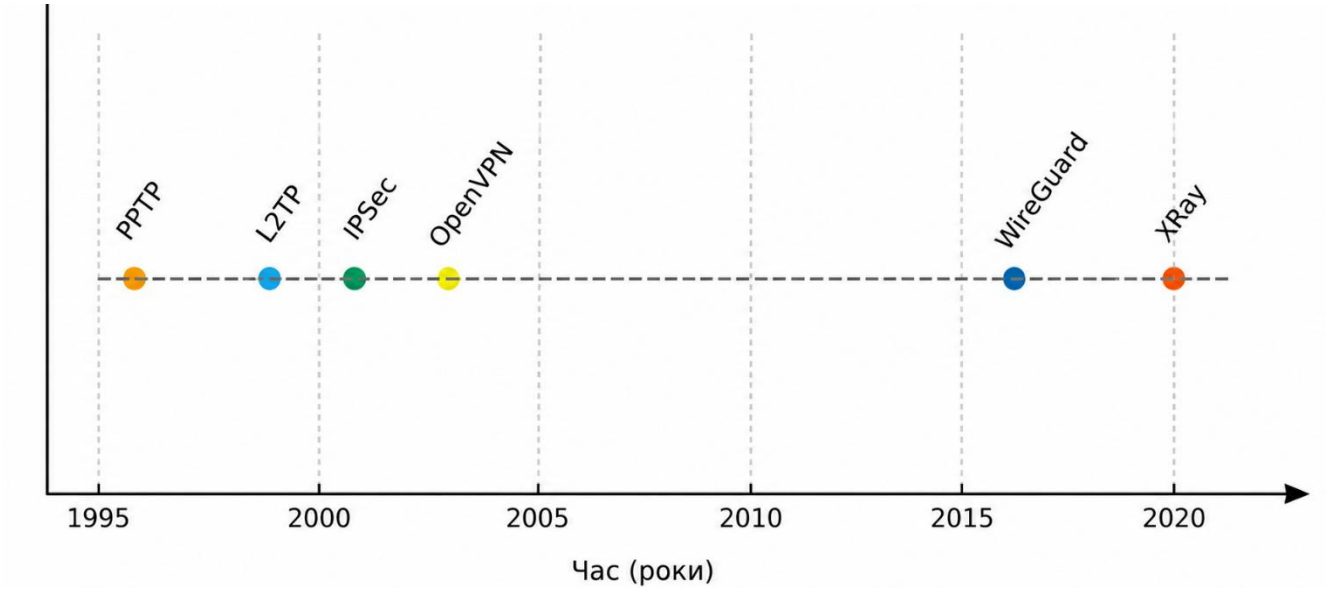


Рисунок 1.7 – Еволюція VPN

Для об’єктивного порівняння сучасних VPN-протоколів у наукових дослідженнях і технічній документації використовують сукупність показників, що характеризують ефективність передавання даних, обчислювальні витрати та рівень захищеності мережевих з’єднань. Аналіз підходів, наведених у специфікаціях IPSec, OpenVPN та WireGuard, а також у роботах, присвячених оцінюванню захищених мережевих технологій, дозволяє виокремити низку ключових метрик продуктивності та безпеки, які доцільно використовувати для подальшого порівняння VPN-рішень.

Метрики продуктивності:

– Throughput (пропускна здатність) – вимірюється в Мбіт/с; залежить від криптографічної продуктивності, накладних заголовків, режиму роботи (UDP vs TCP), та ефективності ядра/користувацького простору. Порівняння по різним протоколам на рисунку 1.8.
– Latency (затримка, RTT) – час першого байта та round-trip time; WireGuard зазвичай демонструє найнижчі затримки завдяки мінімальній обробці в ядрі. Порівняння по різним протоколам на рисунку 1.8.

– Handshake time (час встановлення сесії) – час, необхідний для завершення автентифікації/узгодження ключів (IKEv2 для IPSec проти TLS handshake для OpenVPN та Noise handshake для WireGuard).
– CPU usage / cryptographic load – відсоток завантаження процесора при заданому трафіку; залежить від апаратного прискорення (AES-NI) чи вибору алгоритмів (ChaCha20 краще на CPU без AES-NI).

Метрики безпеки:

– Cryptographic strength – вибрані алгоритми та їхня сучасна стійкість (AES-GCM, ChaCha20-Poly1305, Curve25519 тощо).
– Key management robustness – наскільки складно і безпечно здійснюється обмін ключами (IKEv2 має багатство опцій; WireGuard – прості статичні ключі або протокольні рішення для ротації).
– Resistance to active attacks – MITM, replay, packet injection; IPSec та OpenVPN з TLS/PKI пропонують багаті можливості, WireGuard – простіші, але ефективні сучасні механізми.
– Evasion and anti–censorship – здатність протоколу працювати у середовищах з DPI/блокуваннями; OpenVPN через TCP/443 і XRay/V2Ray з обфускацією часто більш стійкі.

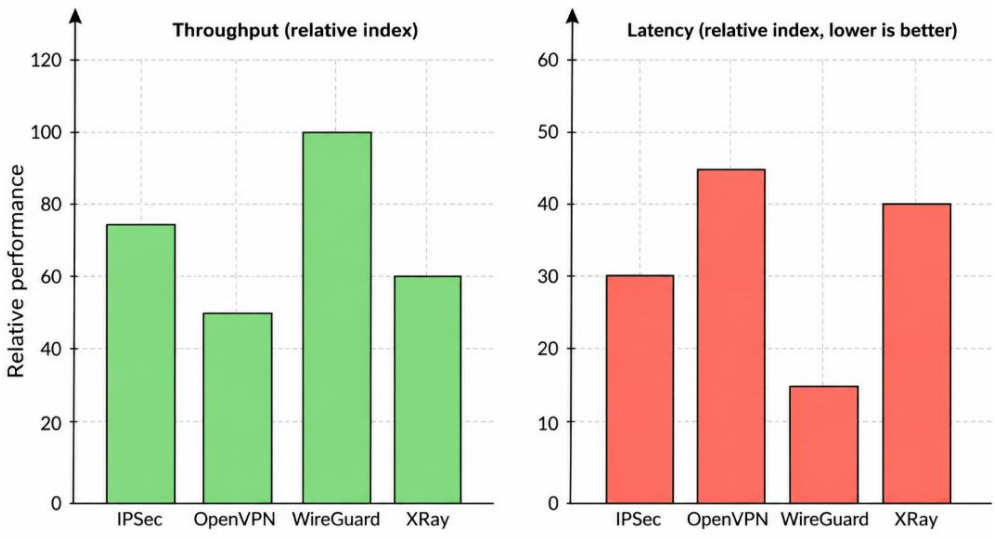


Рисунок 1.8 – Порівняльна продуктивність VPN протоколів

Сучасний розвиток VPN-технологій визначається трьома ключовими векторами: підвищення продуктивності, інтеграція з новими мережевими архітектурами та підготовка до постквантової ери. Традиційні рішення на базі IPSec та OpenVPN продовжують займати значну частку корпоративного ринку завдяки своїй зрілості, однак зростаюча популярність WireGuard і XRay свідчить про потребу у легших, швидших і більш гнучких протоколах.

Одним з основних напрямів еволюції є перехід до постквантових криптографічних алгоритмів. Дослідження Cloudflare та Google показують, що стандартні криптографічні примітиви (RSA, ECDSA, Diffie-Hellman) можуть стати вразливими в умовах розвитку квантових обчислень. У відповідь тестуються гібридні протоколи, які поєднують класичну криптографію та постквантові алгоритми, зокрема CRYSTALS-Kyber для обміну ключами. Це зумовлює появу експериментальних VPN-рішень, здатних забезпечувати стійкість до атак квантових обчислювальних систем.

Другим трендом є інтеграція VPN із SD-WAN та SASE (Secure Access Service Edge). Cisco, Palo Alto Networks та інші виробники наголошують на тому, що класичний підхід до побудови тунелів "точка-точка" поступається місцем динамічним хмарним платформам, які поєднують маршрутизацію, фільтрацію трафіку, DPI та автентифікацію користувачів у єдиній екосистемі. Це дозволяє масштабувати корпоративні мережі без втрати швидкодії та підвищує рівень контролю над потоками даних.

Важливою особливістю сучасного етапу розвитку є розширення сфери застосування VPN у напрямку Zero Trust-архітектур. За даними Forrester, понад 60% компаній у 2023 р. вже поєднували VPN-рішення з Zero Trust Network Access (ZTNA), що зменшує залежність від статичної сегментації мереж і дозволяє впроваджувати політики доступу на основі динамічного аналізу контексту .

З точки зору продуктивності, порівняльні дослідження демонструють значну перевагу WireGuard у швидкості встановлення з’єднання та пропускній здатності.

Наприклад, бенчмарки Phoronix показують, що WireGuard може забезпечувати до 2–5 разів вищу швидкість у порівнянні з OpenVPN при нижчому навантаженні на CPU, тоді як IPSec залишається більш стабільним для масштабних мережевих політик. Протокол XRay демонструє гнучкість у маскуванні трафіку та інтеграції з нестандартними сценаріями обходу цензури, що робить його популярним у країнах із жорсткими обмеженнями доступу до Інтернету.

На рисунку 1.9 представлено інтеграцію VPN у сучасні мережеві архітектури, де класичні тунелі поєднуються з хмарними сервісами безпеки.

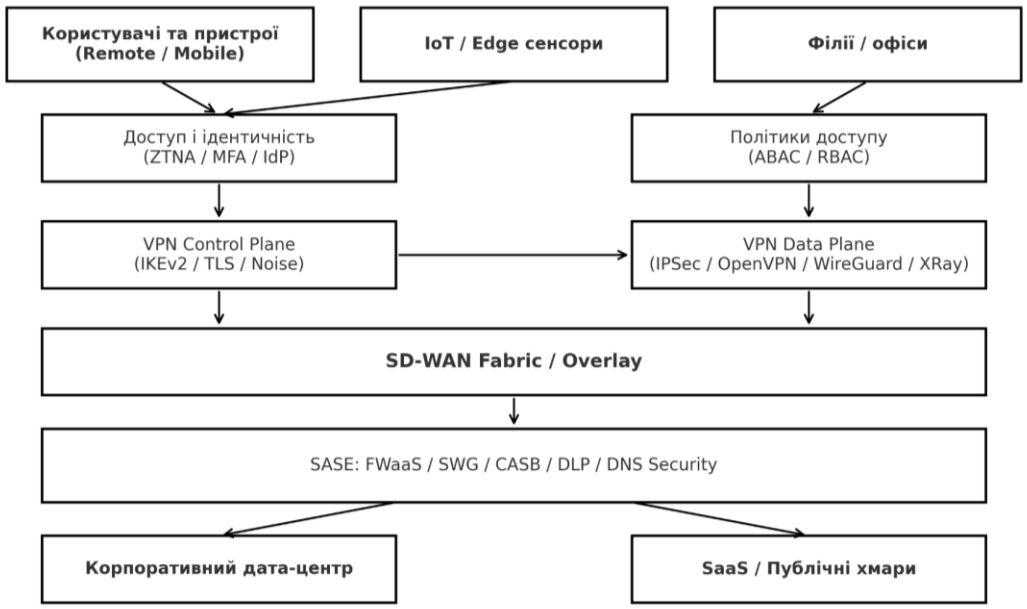


Рисунок 1.9 – Інтеграція VPN-рішень у SD-WAN/SASE-архітектури

На рисунку 1.10 наведено прогноз переходу від традиційних VPN-протоколів до нових рішень, орієнтованих на Zero Trust і постквантову криптографію.

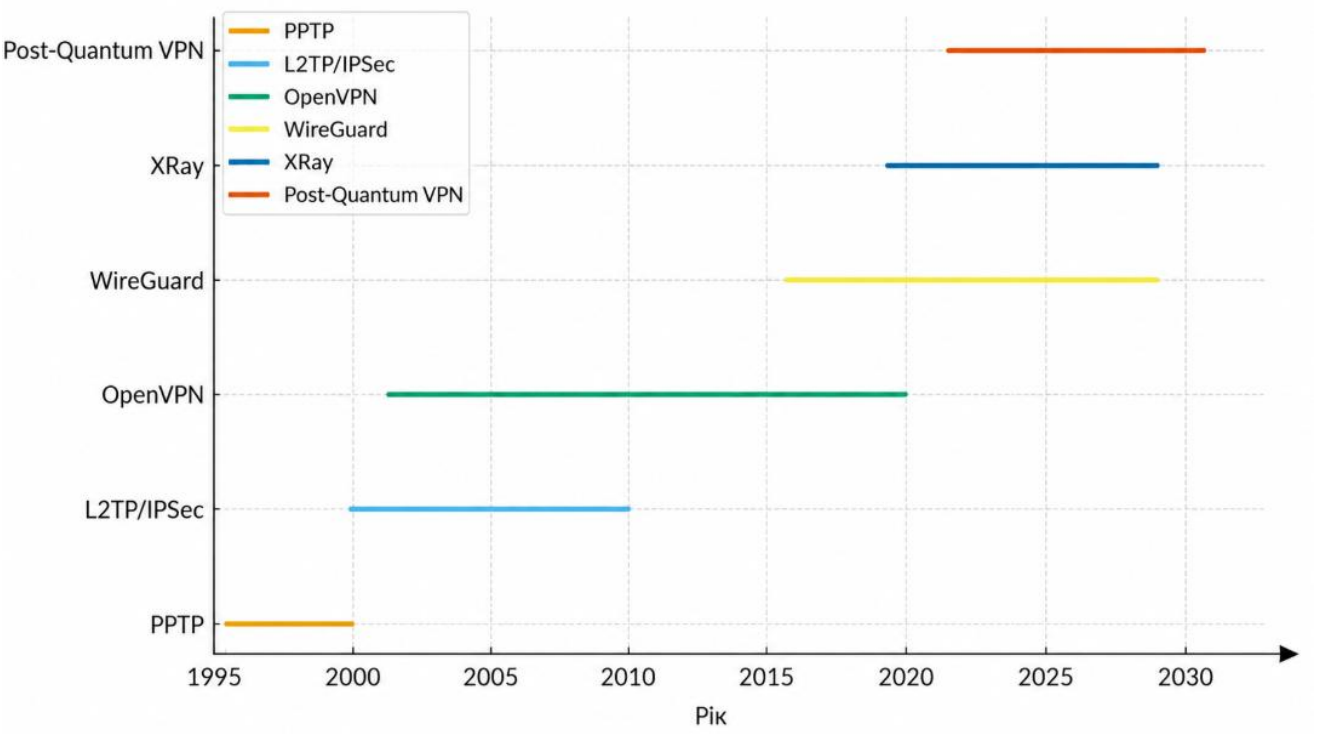


Рисунок 1.10 – Еволюція VPN-технологій: від IPSec до постквантових тунелів

Окремий інтерес становить аналіз ринку. За даними Gartner та IDC, глобальний ринок VPN зростає стабільно: обсяг перевищив $44 млрд у 2022 р. і може досягти понад $77 млрд до 2030 р. Основними драйверами виступають віддалена робота, хмарні обчислення та зростання кіберзагроз. У перспективі найбільш швидко зростатимуть сегменти корпоративних SD-WAN VPN та lightweight-рішень для мобільних пристроїв.

На рисунку 1.11 подано прогноз динаміки ринку VPN за сегментами (корпоративний, споживчий, хмарний) до 2030 року на основі узагальнення прогнозів Fortune Business Insights, Grand View Research та MarketsandMarkets щодо розвитку світового ринку VPN-технологій.

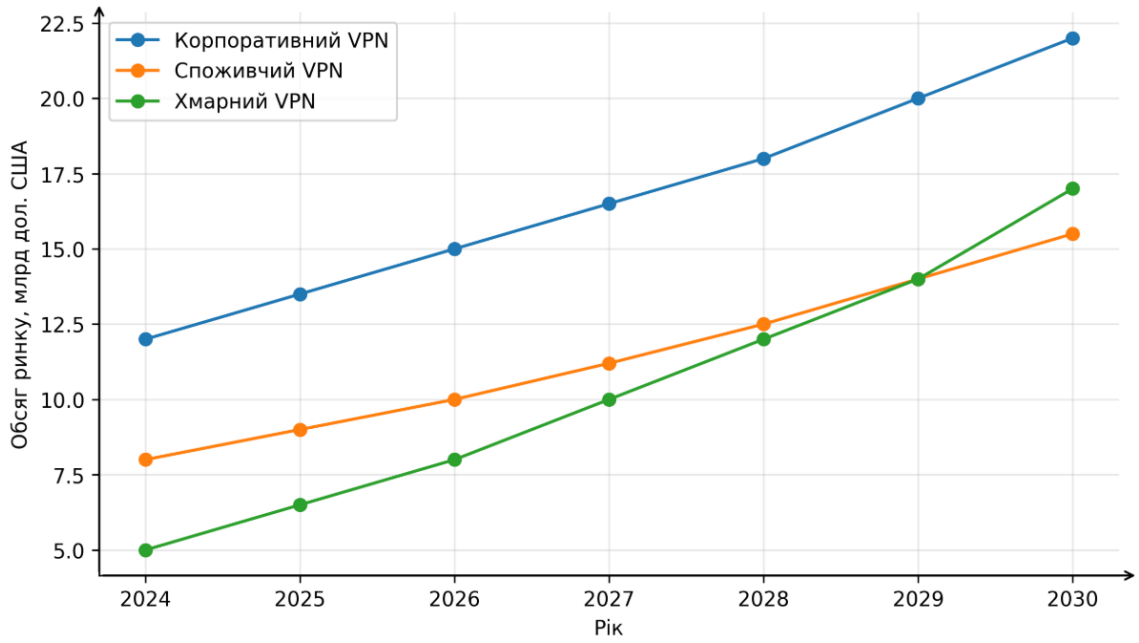


Рисунок 1.11 – Прогноз динаміки світового ринку VPN (млрд USD)

Ще одним показовим аспектом є продуктивність у реальних сценаріях. На рисунку 1.12 наведено результати порівняльних тестів OpenVPN, IPSec, WireGuard і XRay, де WireGuard випереджає конкурентів за latency і throughput, тоді як IPSec забезпечує найбільш передбачувану стабільність, а XRay показує унікальні можливості щодо обходу DPI та гнучкості налаштування.

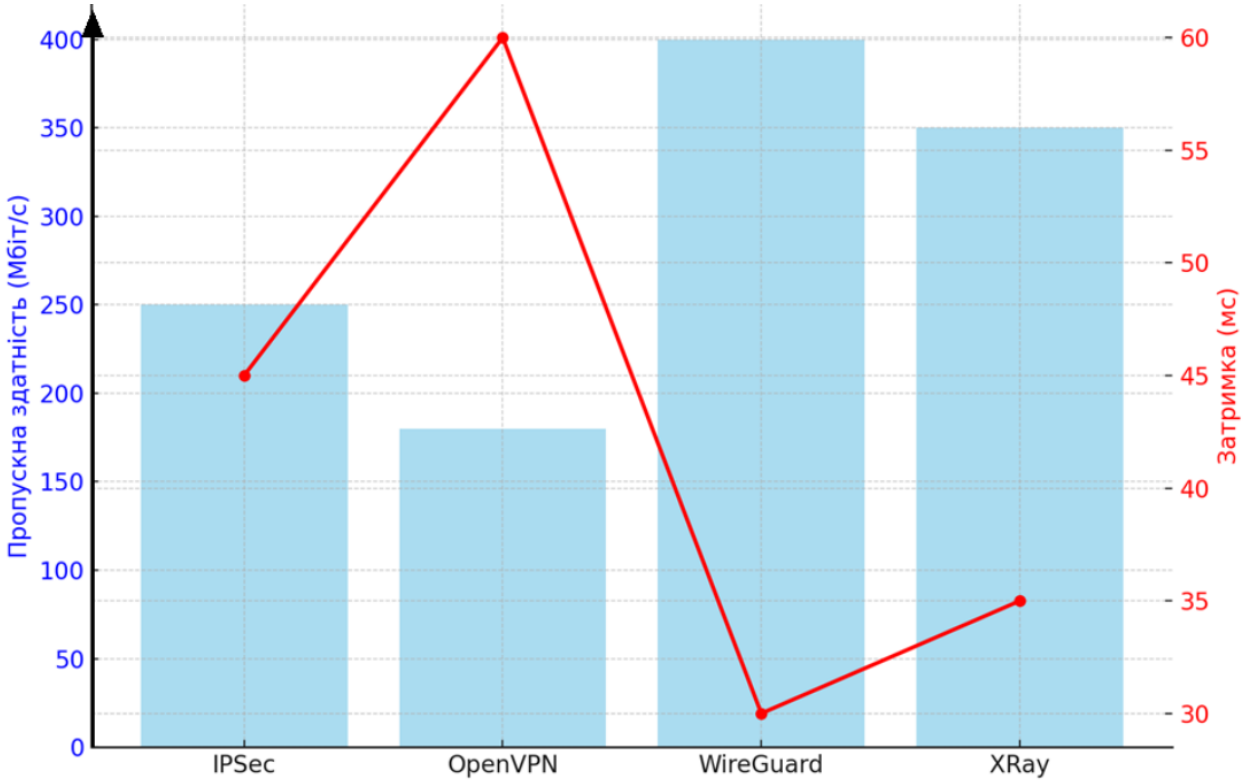


Рисунок 1.12 – Порівняльна продуктивність VPN-протоколів (latency та throughput)

Таким чином, можна зробити висновок, що розвиток VPN-технологій перебуває на межі переходу від класичних протоколів до нових гібридних рішень, які поєднують завадостійкість, гнучкість та постквантову стійкість. Майбутнє VPN лежить у сфері інтеграції з хмарними сервісами, Zero Trust-політиками та впровадженням криптографії наступного покоління, що дозволить підвищити як захищеність, так і ефективність систем передачі даних.

1.6 Обґрунтування побудови багаторівневих моделей захищеності

Сучасні системи передавання даних функціонують у надзвичайно складному середовищі, де одночасно діють як випадкові збої фізичного рівня, так і цілеспрямовані кібератаки на транспортному та прикладному рівнях. Однорівневі підходи, зосереджені виключно на криптографії або лише на завадостійкому кодуванні, довели свою обмеженість: перші захищають від несанкціонованого доступу, проте не гарантують коректності даних у разі збоїв каналу, другі –

забезпечують достовірність передавання, але не протидіють злому чи викраденню інформації. Саме тому актуальним є формування багаторівневих моделей, що інтегрують засоби безпеки кількох рівнів еталонної моделі OSI та моделі TCP/IP.

Одним із перспективних напрямів є синтез інформаційно-аналітичних систем оцінювання рівня захисту каналів передавання інформації [28].

Багаторівневий підхід ґрунтується на принципі «defense in depth» – багатошарової оборони, де кожен рівень накладає власні механізми захисту, що підвищує загальну стійкість системи до різних типів загроз. На фізичному рівні таким механізмом виступає завадостійке кодування (Hamming, Reed-Solomon, LDPC, Polar), яке мінімізує вплив шумів і викривлень сигналу. На мережевому й транспортному рівнях реалізуються VPN-протоколи (IPSec, OpenVPN, WireGuard), які забезпечують криптографічну цілісність, автентифікацію та конфіденційність. На прикладному рівні – додаткові механізми контролю доступу, сегментації трафіку та політик безпеки.

Для аналізу відмов каналів передавання інформації можуть застосовуватись моделі на основі мереж Петрі та імітаційного моделювання [29].

Особливе значення має узгодженість між рівнями: використання надмірного кодування без урахування криптографічних операцій може призвести до зростання затримок, а надмірне навантаження VPN на продуктивність може нівелювати переваги кодування. Тому в обґрунтуванні моделі важливо визначати метрики не окремо для кожного рівня, а як комплексну функцію стійкості, що враховує одночасно BER (bit error rate), latency, throughput і криптографічну стійкість.

Перспективним напрямом також є використання теорії ігор для побудови систем управління інформаційною безпекою [30]. Методи штучного інтелекту також використовуються для підвищення ефективності керування захищеними радіолініями терагерцового діапазону [31].

Дослідження ENISA та NIST підтверджують, що ефективні архітектури безпеки у корпоративних і критичних інфраструктурах вибудовуються саме як багаторівневі системи, де поєднуються механізми кодування, шифрування,

тунелювання та моніторингу. Такі архітектури також відповідають концепціям Zero Trust і SASE (Secure Access Service Edge), які все більше впроваджуються на практиці.

Важливим напрямом сучасних досліджень є впровадження систем одноразового входу (SSO) для підвищення рівня кібербезпеки інформаційних систем [32]. Формалізація концептуальних моделей інформаційної безпеки дозволяє підвищити ефективність побудови комплексних систем захисту [33]. Важливе значення для забезпечення цілісності даних мають методи завадостійкого кодування у пакетних мережах передавання інформації [34].

Таким чином, обґрунтування підходу до побудови багаторівневих моделей захищеності полягає у: поєднанні класичних методів завадостійкого кодування з криптографічними VPN-рішеннями; урахуванні міжрівневої взаємодії для уникнення надмірних затримок та втрати ефективності; визначенні інтегрованих метрик оцінки стійкості; орієнтації на сучасні міжнародні стандарти (NIST, ETSI, ITU-T), що формують основу для практичних рекомендацій.

Цей підхід дозволяє створити єдину інформаційну технологію, яка забезпечує комплексний захист від як фізичних, так і логічних загроз, а також підвищує стійкість системи передачі даних у нестабільних чи ворожих середовищах. Доречно, сучасні дослідження приділяють питанням кібербезпеки технологій Smart City та захисту міської цифрової інфраструктури [35].

1.7 Формалізація вхідних даних

У межах дисертаційної роботи процес передавання даних у захищених мережах розглядається як цілісна функціональна система, що поєднує формування, захист, передавання та відновлення інформації в умовах завад і мережевих обмежень. Для формалізованого подання такої системи доцільно застосувати методологію функціонального моделювання IDEF0, яка дозволяє відокремити вхідні потоки даних, керуючі впливи, механізми реалізації та вихідні результати процесу.

Для послідовного опису такого процесу доцільно попередньо визначити склад вхідних даних, які надходять до системи на початковому етапі та надалі використовуються під час виконання всіх основних функціональних процедур.

У межах цього підрозділу вхідні дані доцільно подати у вигляді трьох узагальнених груп, для яких у подальшому використовуватимуться умовні позначення I1, I2 та I3. Позначення I1 відповідає прикладним даним, що підлягають передаванню. Позначення I2 відповідає службовим даним сеансу передавання. Позначення I3 відповідає початковим параметрам сеансу зв’язку.

До групи I1 належить основне інформаційне наповнення, яке формується джерелом даних і передається через мережеве середовище. Йдеться про користувацькі повідомлення, файли, пакети або інші інформаційні об’єкти, для яких надалі мають бути забезпечені належний рівень цілісності, конфіденційності та доступності. Саме ця група даних становить змістову основу процесу передавання, оскільки визначає, яка саме інформація має бути доставлена від джерела до отримувача.

До групи I2 належать службові дані, що супроводжують процес передавання та забезпечують його організацію. До них можуть бути віднесені службові поля пакетів, ідентифікатори сеансу, адресна інформація, ознаки послідовності, параметри синхронізації, а також інші допоміжні елементи, необхідні для встановлення, підтримання та коректного завершення сеансу обміну. На відміну від прикладних даних, службові дані не визначають зміст повідомлення, однак забезпечують можливість його впорядкованого та коректного транспортування.

До групи I3 належать початкові параметри сеансу зв’язку, які задають загальні умови функціонування системи під час передавання даних. До таких параметрів можуть належати характеристики мережевого середовища, початкові налаштування сеансу, обмеження каналу зв’язку, допустимі режими обміну, а також інші параметри, що визначають контекст подальшої обробки й передавання інформації. Зазначена група не є інформаційним навантаженням у прямому

розумінні, проте вона впливає на спосіб організації всіх наступних етапів передавання.

Запропонований поділ вхідних даних на три узагальнені групи дозволяє впорядкувати початковий опис досліджуваного процесу та уникнути змішування змістових, службових і параметричних складових. У подальшому це створює зручну основу для послідовного переходу до розгляду моделей, методів, обчислювальних засобів і процедур реалізації, не перевантажуючи початковий опис надмірною деталізацією

1.8 Постановка задачі

Розглянувши сучасні виклики інформаційній безпеці, проаналізувавши природу та різновиди кібератак, дослідивши системи виявлення й запобігання інцидентам, а також узагальнивши роль завадостійкого кодування і VPN-протоколів у багаторівневих архітектурах, можна сформулювати наукову задачу даного дослідження.

На сьогодні відсутня інтегрована інформаційна технологія, яка б одночасно враховувала характеристики фізичного рівня (надійність каналу, рівень завадостійкості), транспортного рівня (ефективність криптографічних протоколів і тунелювання) та прикладного рівня (адаптивність VPN-рішень у реальних мережевих сценаріях). Існуючі рішення, як правило, орієнтовані на окремі аспекти забезпечення захищеності або надійності передавання даних: або на підвищення завадостійкості за допомогою кодів корекції помилок, або на криптографічне забезпечення конфіденційності та автентичності інформації. У зв’язку з цим науково-технічна задача полягає у розробленні гібридної інформаційної технології захищеного передавання даних, яка інтегрує механізми завадостійкого кодування та VPN-тунелювання в межах єдиного адаптивного підходу.

Водночас розвиток технологій 5G/6G, збільшення обсягів переданої інформації та поява нових класів атак (наприклад, активних MITM у комбінації з радіочастотними перешкодами) створюють потребу у багаторівневій моделі

захисту, що здатна адаптуватися до змінних умов середовища. Класичні VPN-протоколи, як IPSec чи OpenVPN, забезпечують високий рівень криптографічної безпеки, проте залишаються чутливими до втрат пакетів і високої латентності. З іншого боку, нові рішення (WireGuard, XRay) відзначаються продуктивністю та простотою, але не враховують додаткового шару корекції помилок, необхідного для стабільної роботи у шумних середовищах.

Таким чином, задача дисертаційного дослідження полягає у розробленні гібридної інформаційної технології захищеної передачі даних, яка поєднує методи завадостійкого кодування для підвищення надійності передавання на фізичному рівні, сучасні VPN-протоколи для забезпечення конфіденційності, цілісності та автентифікації інформації, а також систему метрик для комплексного оцінювання ефективності функціонування за сукупністю показників надійності, захищеності та продуктивності.

Метою роботи є підвищиння ефективності, надійності та захищеності передавання даних шляхом розроблення та впровадження інтегрованого підходу до забезпечення їх надійності та захищеності. Для її досягнення необхідно вирішити такі науково-практичні задачі:

1. Провести аналіз сучасних механізмів завадостійкого кодування та VPN-протоколів із позицій їхньої інтеграції.
2. Розробити математичні моделі й методи поєднання кодування та шифрування в єдиній архітектурі.
3. Побудувати алгоритмічне забезпечення реалізації гібридної системи.
4. Виконати верифікацію розробленої технології за допомогою імітаційного моделювання.
5. Оцінити ефективність гібридного підходу шляхом порівняння з існуючими рішеннями.

У результаті дослідження очікується одержати модель, здатну адаптивно поєднувати переваги завадостійкого кодування та сучасних VPN-протоколів, що

дозволить створити новий клас інформаційних технологій для забезпечення надійної й захищеної передачі даних у мережах із високим рівнем загроз.

1.9 Висновки за розділом

У першому розділі проведено аналіз сучасного стану захищеності систем передавання даних у комп’ютерних мережах та визначено основні проблеми забезпечення їх надійності й інформаційної безпеки в умовах дії завад і кіберзагроз.

1. Розглянуто сучасні виклики інформаційній безпеці мережевих систем, пов’язані зі зростанням обсягів передавання даних, розвитком розподілених сервісів і збільшенням кількості потенційних вразливостей.

2. Проаналізовано основні типи кібератак та їх вплив на стабільність функціонування комп’ютерних систем і мереж.

3. Досліджено концептуальні підходи до побудови гібридних моделей забезпечення інформаційної безпеки та визначено доцільність інтеграції механізмів захисту різних рівнів мережевої взаємодії.

4. Розглянуто методи завадостійкого кодування як засоби забезпечення надійності фізичного рівня передавання даних, проаналізовано їх переваги та обмеження при використанні в сучасних мережах.

5. Виконано аналіз сучасних VPN-протоколів, зокрема IPsec, OpenVPN та WireGuard, та визначено особливості їх застосування для забезпечення захищеного передавання даних.

6.Обґрунтовано підходи до побудови багаторівневих моделей захищеності, які передбачають комплексне використання засобів криптографічного захисту та механізмів підвищення надійності передавання даних.

7. Виконано формалізацію вхідних даних, параметрів каналу передавання та показників ефективності функціонування системи.

8. Сформульовано постановку задачі дослідження, визначено основні напрями розроблення моделей, методів та інформаційної технології забезпечення надійності й захищеності передавання даних у комп’ютерних мережах.

Актуальність і доречність розробки і розвитку моделі, методів та інформаційної технології для підвищення надійності й захищеності передачі даних у мережах з часом тільки зростає, про це свідчить сучасна технологічна практика і вектор розвитку наукової думки, що було опробовано і підверджено [36-38].

За результатами проведеного аналізу встановлено, що існуючі підходи до забезпечення захищеності та надійності передавання даних переважно застосовуються ізольовано та не забезпечують необхідного рівня ефективності в умовах комплексного впливу завад і кіберзагроз. Це підтвердило доцільність розроблення інтегрованого підходу, заснованого на поєднанні механізмів завадостійкого кодування та оверлейних технологій у межах єдиної моделі захищеного каналу передавання даних.

РОЗДІЛ 2 ОБҐРУНТУВАННЯ ВИБОРУ МЕТРИК ДЛЯ ОЦІНКИ ГІБРИДНОЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ

2.1 Формалізація керуючих впливів

У підрозділі 1.7 було здійснено формалізацію вхідних даних запропонованої гібридної інформаційної технології, тобто тих інформаційних потоків, які надходять до системи на оброблення та визначають зміст процесу передавання даних. Разом із цим для побудови повної функціональної моделі в нотації IDEF0 необхідно окремо визначити не лише вхідні потоки, а й керуючі впливи, які в межах цієї нотації подаються як верхні входи функції. Саме такі впливи задають правила, межі, логіку та умови функціонування системи, тобто визначають, за якими моделями, методами, критеріями та обмеженнями реалізується процес передавання даних.

У межах даного розділу увага зосереджується саме на формалізації зазначених керуючих впливів. Якщо в першому розділі було визначено, які дані надходять у систему та за яких початкових умов вона функціонує, то в другому розділі розглядаються ті концептуальні та методичні засади, які керують подальшим вибором способів кодування, криптографічного захисту, тунелювання, оцінювання якості функціонування та прийняття рішень щодо допустимості або доцільності тієї чи іншої конфігурації. Такий підхід забезпечує логічне розмежування між формалізацією об’єкта оброблення та формалізацією правил його оброблення.

На верхньому рівні процес передавання даних подається у вигляді узагальненої функції A0, яка відображає цілісний процес реалізації гібридної інформаційної технології підвищення надійності та захищеності передавання даних у мережах. У межах цієї функції вхідні потоки задають прикладні та службові дані, виходи відображають результат їх передавання і відновлення, механізми характеризують програмно-апаратні засоби реалізації, тоді як верхні входи визначають сукупність керуючих впливів, без яких модель не може бути

приведена до формального, алгоритмічного та експериментально відтворюваного вигляду. У загальному вигляді це можна побачити на рисунку 2.1.

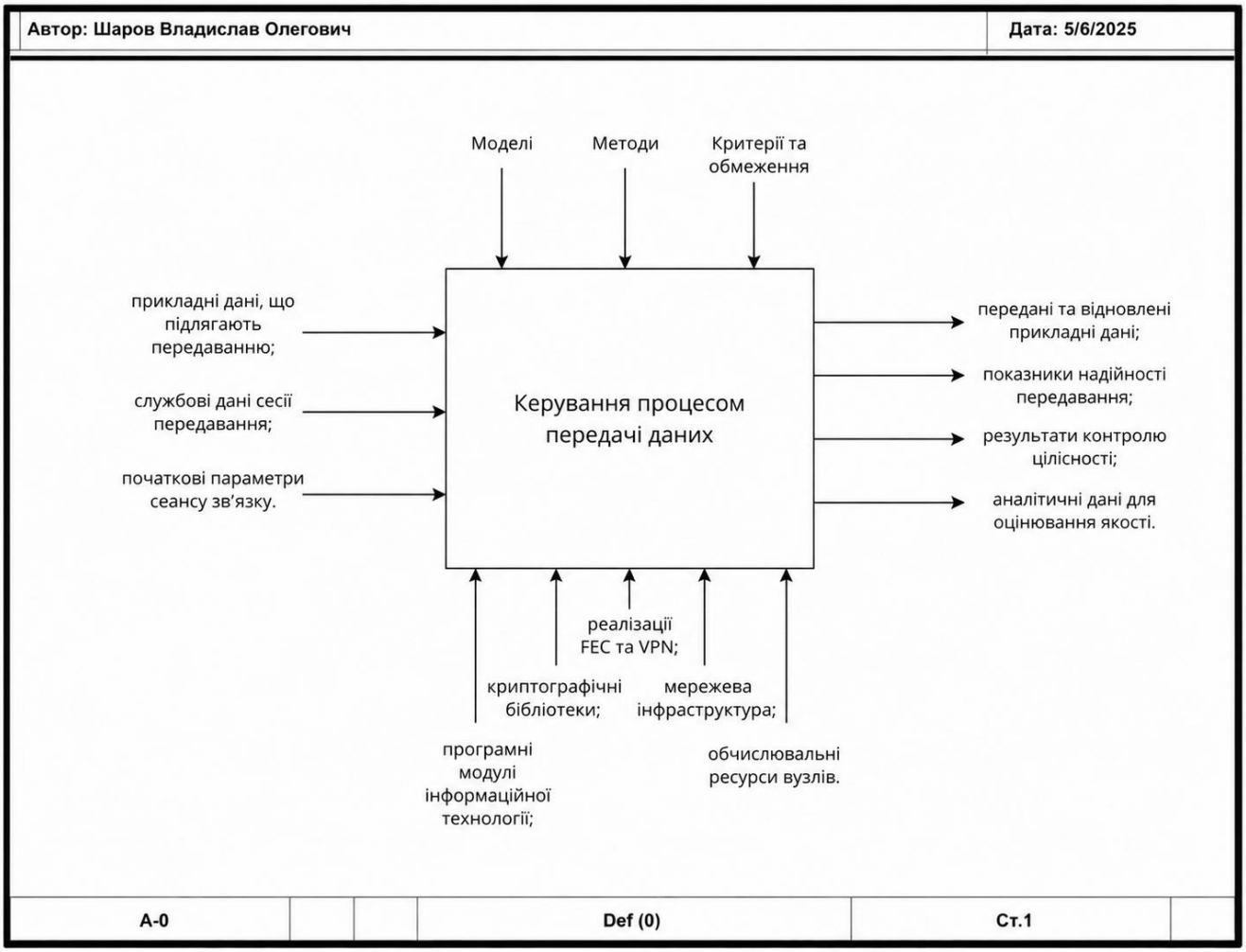


Рисунок 2.1 – Функціональна модель процесу передавання даних у нотації IDEF0

Для переходу від загального уявлення про систему до деталізованого опису окремих етапів її функціонування узагальнена функція A0 підлягає декомпозиції на підфункції A1-A4. Така декомпозиція дозволяє пов'язати функціональну структуру моделі з логікою подальшого викладу матеріалу дисертаційної роботи. У межах цієї декомпозиції окремі підпроцеси відображають підготовку даних до передавання, забезпечення завадостійкості, реалізацію криптографічного захисту і тунелювання, а також приймання та відновлення інформації на стороні одержувача.

При цьому керуючі впливи зберігають системоутворювальну роль, оскільки саме вони визначають, які математичні моделі, методи, критерії та обмеження мають бути застосовані на кожному з етапів. Декомпозований вигляд представлено на рисунку 2.2.

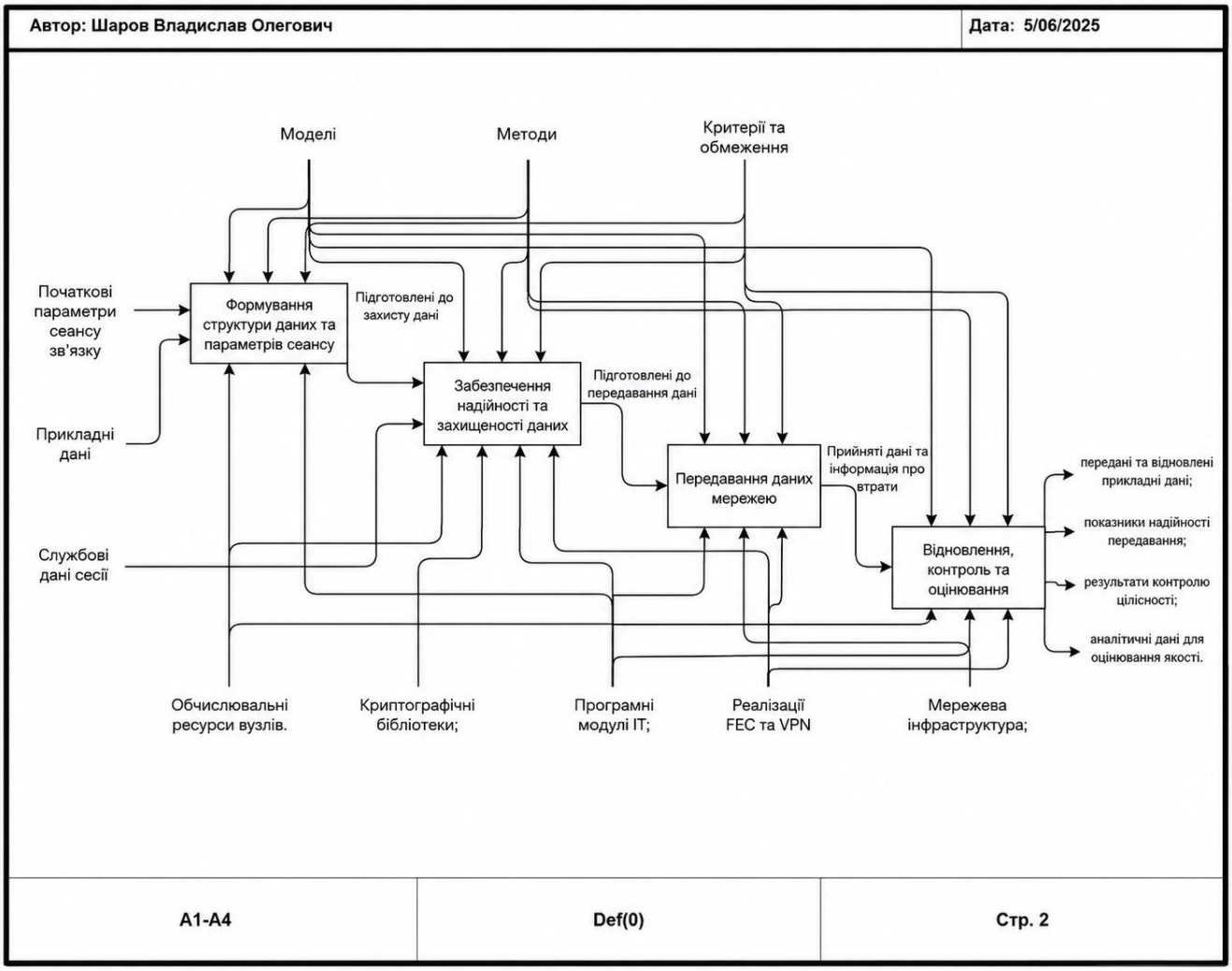


Рисунок 2.2 – Декомпозиція функції на підпроцеси A1-A4 у нотації IDEF0

До верхніх входів моделі в даному дослідженні віднесено чотири взаємопов'язані групи керуючих впливів: моделі, методи, критерії та обмеження. Моделі задають формалізований опис процесів, що досліджуються, і визначають спосіб подання каналу зв'язку, механізмів завадостійкого кодування, криптографічного захисту, тунелювання та наскрізної доставки даних. Методи

визначають практичний інструментарій реалізації цих моделей, тобто способи вибору параметрів, алгоритми оброблення, правила узгодження рівнів захисту та відновлення, а також процедури адаптації системи до умов функціонування. Критерії задають основу для оцінювання ефективності обраних рішень і використовуються для порівняння альтернативних конфігурацій за показниками надійності, затримки, накладних витрат, пропускної здатності та допустимості з погляду безпеки. Обмеження визначають межі застосовності запропонованих рішень і охоплюють ресурсні, часові, мережеві, криптографічні та протокольні умови, у межах яких система повинна залишатися працездатною та ефективною. Аналогічні принципи оцінювання продуктивності каналів передавання використовуються і в сучасних цифрових системах зв’язку [39].

Таким чином, якщо вхідні дані, визначені в підрозділі 1.7, відповідають на питання, що саме надходить у систему, то керуючі впливи, що розглядаються в даному розділі, відповідають на питання, яким чином, за якими правилами та в яких межах ця система повинна функціонувати. Саме тому подальший виклад у розділі 2 спрямовано на обґрунтування складу й змісту цих верхніх входів моделі IDEF0. У наступних підрозділах вони послідовно конкретизуються через систему метрик, критеріїв оцінювання, формалізованих підходів до вибору параметрів і сукупність обмежень, які визначають придатність та ефективність гібридної інформаційної технології в заданих умовах застосування.

2.2 Метрики для єдиної моделі

Запропонований набір метрик будується навколо наскрізного результату: скільки корисних даних доходить коректно, з якою затримкою та з якою «ціною» у вигляді накладних витрат і ресурсоємності. Для читабельності та відтворюваності метрики визначено як конкретні змінні з однозначними формулами і рахунками, а безпека оформлена як перевірювана відповідність профілю, а не як суб’єктивний індекс. Вимоги до метрик як «добре визначених» і «повторюваних» спираються на рамку IPPM, що знижує ризик появи метрик, які неможливо коректно виміряти або

порівняти (IETF (Internet Engineering Task Force) RFC (Request for Comments) 2330). Підходи до оцінювання характеристик цифрових каналів зв’язку та ефективності передавання даних широко розглядаються у класичних роботах з цифрових комунікацій [40].

Єдина модель, що поєднує завадостійке кодування на фізичному рівні, тунелювання VPN і проксі-рівень, повинна оцінюватися метриками, які зберігають сенс при переході між рівнями і не «ламаються» на стиках. На практиці це означає, що бітові помилки та перешкоди на фізиці слід відображати не тільки як BER, а як те, у що вони перетворюються вище: у втрати або недоставку одиниць даних, які перевіряються криптографічною цілісністю та можуть бути відкинуті при прийомі (IETF RFC 4303) [41].

Для частини FEC, орієнтованої на пакети, доречно використовувати пакетні метрики «стірань» і відновлення, оскільки сама рамка FECFRAME визначена як інструмент для захисту від втрат пакетів у довільних потоках поверх ненадійного транспорту (IETF RFC 6363). Якщо у моделі застосовуються віконні (sliding window) схеми, це потрібно відокремити як режим і для нього додатково фіксувати параметри вікна та пов’язану затримку, що прямо узгоджується з розширенням FECFRAME на sliding window коди (IETF RFC 8680).

Для VPN-шару критично відстежувати накладні витрати, ефективний MTU (Maximum Transmission Unit) та фрагментацію, оскільки навіть кілька доданих байтів можуть запускати фрагментацію або проявляти «зламаний» Path MTU Discovery, що призводить до зависань застосунків; NIST прямо описує цей клас проблем і практичні обхідні стратегії на кшталт зменшення MTU або TCP MSS (Maximum Segment Size) clamping (NIST SP 800-77r1). Додатково, сама фрагментація розглядається як джерело крихкості для інтернет-комунікацій, і верхні рівні мають мінімізувати залежність від неї (IETF RFC 8900). Якщо модель включає алгоритм адаптації розміру датаграм або стійку роботу при «black hole», тоді доцільно явно спиратися на DPLPMTUD (Datagram Layer Path MTU Discovery) як робастний підхід для датаграмних транспортів (IETF RFC 8899).

Для метрик затримки та втрат доречно використовувати формулювання IPPM (IP Performance Metrics), оскільки вони задають не лише назви величин, а і параметри вимірювання та принципи звітності. Для затримки базовим є one-way delay як стандартна метрика з визначенням одиниць і параметра «loss threshold waiting time» (IETF RFC 7679). Для втрат базовим є one-way packet loss як однозначно визначена метрика (IETF RFC 7680). Для варіації затримки коректніше використовувати визначення IP Packet Delay Variation, щоб уникнути неоднозначності «jitter» (IETF RFC 3393).

Для пропускної здатності слід розрізняти «що пройшло по дроту» і «що реально доставлено застосунку». У тестуванні TCP throughput окремо підкреслюється чутливість до параметрів на кшталт RTT і Path MTU, тому коректно в моделі явно фіксувати MTU та буферні умови і звітувати goodput як результат наскрізної доставки (IETF RFC 6349). Для загальної дисципліни експериментів корисно узгоджувати постановку з усталеними підходами до бенчмаркінгу throughput, latency та frame loss (IETF RFC 2544).

Безпеку в інтегрованій моделі доцільно задавати як виконувану умову відповідності профілю, що визначається архітектурою IPsec і актуальними вимогами до алгоритмів для IKEv2 та ESP/AH. Архітектурні безпекові послуги IPsec задаються окремо від вибору конкретних алгоритмів (IETF RFC 4301), а вимоги до алгоритмів і їх еволюція винесені у спеціальні документи (IETF RFC 8247, IETF RFC 8221). Практичний зв’язок «профіль алгоритмів – накладні витрати, MTU, CPU, стабільність IKE/ESP» добре підтверджується рекомендаціями NIST (NIST SP 800-77r1).

Для проксі-рівня доцільні метрики, які відображають ціну додаткових рукопотискань і обробки, а саме час готовності сеансу, час до першого корисного байта і накладні витрати на інкапсуляцію. Це узгоджується з тим, що Xray-core є платформою з різними протоколами і транспортами, де вартість «маскування» і транспортного режиму проявляється в затримці, overhead та використанні ресурсів (Project X документація).

У сучасних комп’ютерних мережах процес передавання даних реалізується у вигляді послідовності базових операцій, що включають формування пакета, маршрутизацію, транспортування та приймання даних із подальшою перевіркою їх цілісності на рівні протоколів. У поточній (as-is) конфігурації такі бізнес-процеси не передбачають інтегрованих механізмів підвищення надійності та захищеності. Корекція помилок, шифрування та виявлення аномалій функціонують як незалежні підсистеми, що створює фрагментованість захисту та обмежує ефективність канального контролю.

На канальному рівні застосовуються прості методи контролю цілісності (CRC), які здатні лише фіксувати факт помилки, але не забезпечують її корекцію. На мережевому та транспортному рівнях застосовуються окремі механізми повторної передачі, однак вони не усувають першопричину – нестійкість передавання в умовах завад та атак. Захисні засоби працюють відокремлено: VPN-тунелювання може забезпечувати конфіденційність, але не компенсує канальні помилки, тоді як корекційне кодування не впливає на криптографічну стійкість каналу. Формується інформація щодо результатів контролю цілісності даних у процесі передавання.

Узагальнений бізнес-процес «як є» наведено у вигляді моделі, що відображає основні потоки даних та інформаційну взаємодію між підсистемами мережі.

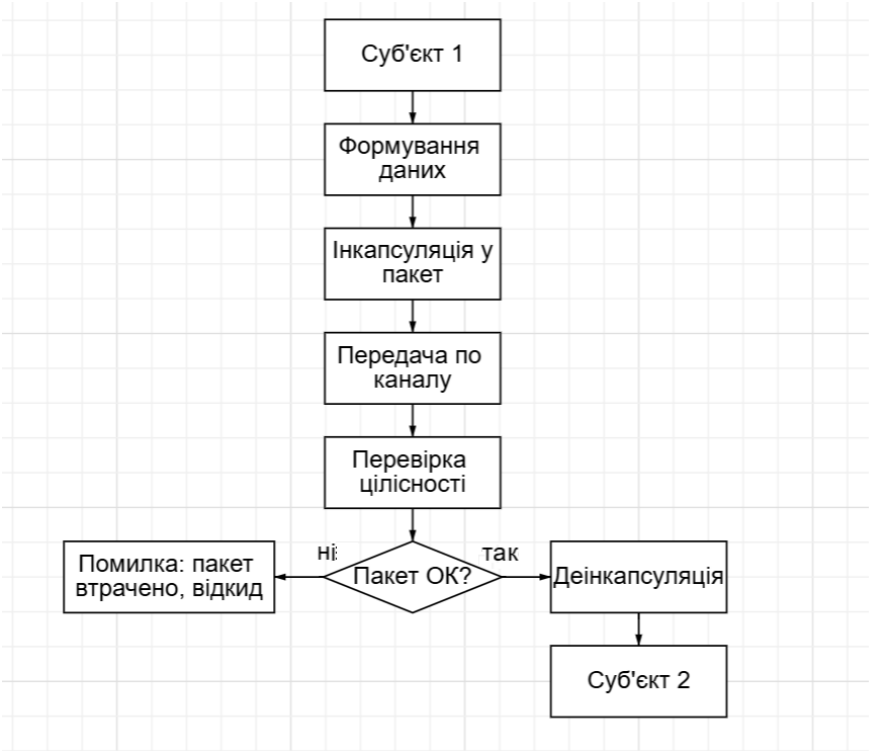


Рисунок 2.3 – Бізнес-процес передавання даних «як є (as-is)»

Вхідним інформаційним потоком запропонованої інформаційної технології є прикладні дані користувача, що надходять з прикладного рівня мережевого стеку та підлягають подальшій структуризації, захисту та передаванню мережею.

Запропонована інформаційна технологія передбачає інтеграцію корекційного кодування, криптографічного захисту та механізмів виявлення аномалій у єдиний технологічний цикл. Така інтеграція усуває фрагментованість, притаманну поточній архітектурі, та забезпечує одночасне підвищення надійності й захищеності передавання даних.

У моделі «як буде (to-be)» корекційне кодування виконується перед застосуванням криптографічних процедур, що гарантує можливість відновлення даних після проходження зашумленого або атакованого каналу. VPN-тунелювання інтегрується до технологічного процесу як механізм захисту від перехоплення та модифікації даних. Засоби виявлення аномалій застосовуються на етапі приймання та аналізу трафіку, що дає змогу фіксувати шкідливу активність і підвищувати операційну стійкість каналу.

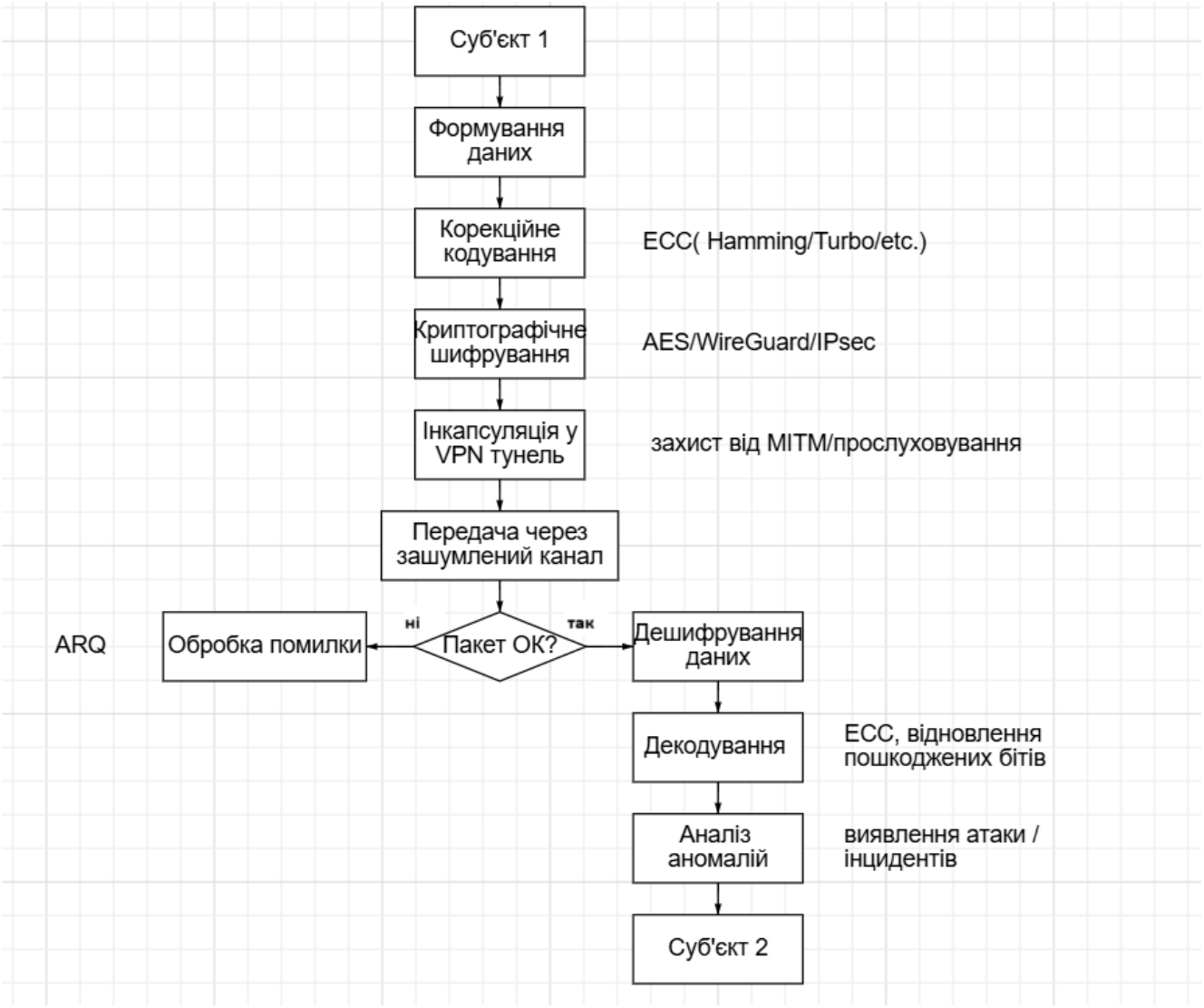


Рисунок 2.4 – Бізнес-процес передавання даних «як буде (to-be)» з інтегрованою інформаційною технологією

2.3 Показники ефективності та методи їх розрахунку

Перш ніж визначати показники ефективності та методи їх розрахунку, необхідно сформулювати критерії оцінювання гібридного захищеного каналу. З огляду на поставлену задачу інтеграції механізмів ЗСК та VPN, основними критеріями є підвищення надійності доставки даних, зменшення втрат і невиправлених помилок, мінімізація затримок передавання, раціональне використання мережевих та обчислювальних ресурсів, а також обмеження надлишковості, що вноситься механізмами захисту та корекції помилок. Для

кількісного оцінювання ступеня досягнення зазначених критеріїв використовується система показників ефективності, наведена нижче.

Швидкість завадостійкого коду визначається як

$$\mathrm{R} = \frac{i}{n}, \tag{2.1}$$

де R– швидкість коду, безрозмірна величина;

n– довжина кодового слова, біт;

i– кількість інформаційних бітів у кодовому слові, біт.

Визначення R як базового параметра кодування є стандартним для теорії та практики завадостійкого кодування.

Частка надлишковості на рівні кодового слова визначається як

$$\rho = 1 - \mathrm{R} = \frac{n-i}{n}, \tag{2.2}$$

де ρ – безрозмірна частка надлишкових бітів.

Якість сигналу на фізичному рівні характеризується відношенням сигнал/шум у лінійному масштабі

$$\gamma = \frac{P_{sig}}{P_{noise}}, \tag{2.3}$$

де P_{sig} – середня потужність сигналу, Вт;

P_{noise} – середня потужність шуму, Вт;

Для подання відношення сигнал/шум у децибелах використовується вираз

$$\Gamma_{dB} = 10 \log_{10} \gamma, \tag{2.4}$$

Бітова ймовірність помилки визначається як

$$P_b = \frac{N_{err}}{N_{bit}}, \tag{2.5}$$

де N_{err} – кількість помилкових бітів у межах спостереження, біт;

N_{bit} – кількість перевірених бітів у межах спостереження, біт.

Імовірність помилки кодового слова визначається як

$$P_w = \frac{E_{cw}}{N_{cw}}, \tag{2.6}$$

де E_{cw} – кількість кодових слів, що після декодування залишилися помилковими;

N_{cw} – кількість перевірених кодових слів.

У моделі вводиться поняття базової одиниці доставки ADU (Application Data Unit), яка відповідає порції даних, що має бути коректно доставлена до рівня застосунку. Кількість ADU, поданих у систему на передаванні, позначається як N_{ADU}^{tx}, а кількість ADU, коректно доставлених на прийманні до рівня застосунку як N_{ADU}^{ok}.

Наскрізна частка успішної доставки визначається як

$$\Pi_{e2e} = \frac{N_{ADU}^{ok}}{N_{ADU}^{tx}}, \tag{2.7}$$

Наскрізна частка недоставки визначається як

$$\lambda_{e2e} = 1 - \Pi_{e2e} = \frac{N_{ADU}^{tx} - N_{ADU}^{ok}}{N_{ADU}^{tx}}, \tag{2.8}$$

де E_{cw} – кількість кодових слів, що після декодування залишилися помилковими.

Параметри FECFRAME на пакетному рівні задаються величинами K_S – кількість вихідних об’єктів (source) у блоці або вікні, од.; K_r – кількість відновлювальних об’єктів (pair), од.; K_t – загальна кількість об’єктів, що

передаються для захисту вихідних даних, од. При цьому $K_t = K_S + K_t$. Пакетна надлишковість FEC визначається як

$$\varphi = \frac{K_r}{K_S}, \tag{2.9}$$

де φ – безрозмірна величина, що характеризує відносний обсяг відновлювального трафіку.

Частка стирань на вході декодера FEC визначається як

$$\varepsilon = 1 - \frac{N_{FEC}^{rx}}{N_{FEC}^{tx}}, \tag{2.10}$$

де ε – безрозмірна частка стирань;

N_{FEC}^{tx} – кількість переданих FEC-захищених об’єктів типу source+repair, од.;

N_{FEC}^{rx} – кількість таких об’єктів, що фактично надійшли на вхід декодера FEC, од.

Емпірична ймовірність успішного декодування FEC визначається як

$$P_{dec} = 1 - \frac{N_{blk}^{ok}}{N_{blk}}, \tag{2.11}$$

де N_{blk} – кількість блоків або інтервалів відновлення, для яких виконувалася спроба декодування, од.;

N_{blk}^{ok} – кількість блоків або інтервалів, для яких відновлення було успішним, од.

Для аналітичного оцінювання в ідеалізованій моделі незалежних стирань може використовуватися вираз

$$P_{dec}^{mdl} = \sum_{k=0}^{K_r} \binom{K_t}{k} \varepsilon^k (1-\varepsilon)^{K_t - k}, \tag{2.12}$$

де P_{dec}^{mdl} – модельна ймовірність успішного декодування, безрозмірна величина;

k – кількість втрачених об’єктів у межах K_t;

$\binom{K_t}{k}$ – біноміальний коефіцієнт, який визначається як $\binom{K_t}{k} = \frac{K_t!}{k!(K_t-k)!}$.

Наведений вираз використовується для оцінювання впливу величини φ за фіксованого значення є на ймовірність відновлення та на обсяг відновлювального трафіку.

Для розділення внеску криптографічних і проксі-механізмів вводиться частка прийняття пакетів VPN-шаром:

$$\Pi_{vpn} = \frac{N_{vpn}^{ok}}{N_{vpn}^{in}}, \tag{2.13}$$

де Π_{vpn} – безрозмірна частка пакетів, коректно прийнятих VPN-шаром;

N_{vpn}^{in} – кількість пакетів, що надійшли на вхід оброблення VPN на приймальній стороні, од.;

N_{vpn}^{ok} – кількість пакетів, що успішно пройшли перевірку цілісності, дешифрування та були прийняті, од.

Для проксі-рівня аналогічно вводиться частка коректного прийняття:

$$\Pi_{prx} = \frac{N_{prx}^{ok}}{N_{prx}^{in}}, \tag{2.14}$$

де Π_{prx} – безрозмірна частка одиниць даних, коректно оброблених проксі-рівнем;

N_{prx}^{in} – кількість одиниць даних, що надійшли на вхід проксі або прикладного транспорту на приймальній стороні, од.;

N_{prx}^{ok} – кількість одиниць даних, що були коректно оброблені та передані до застосунку, од.

Наскрізна затримка для j-тої доставленої одиниці визначається як

$$\tau_j = t_j^{rx} - t_j^{tx}, \tag{2.15}$$

де t_j^{tx} – момент відправлення на передавальній стороні, с;

t_j^{rx} – момент отримання на приймальній стороні на обраному рівні фіксації факту доставки, с.

Квантилі затримки визначаються як

$$\tau_p = \mathrm{Q}_p(\{\tau_j\}), \tag{2.16}$$

де Q_p – оператор p-квантили;

$\{\tau_j\}$ – множина виміряних значень затримки.

Варіація затримки задається як

$$\nu_\tau = \tau_{95} - \tau_{50}, \tag{2.17}$$

Інтервальна пропускна здатність на зовнішньому інтерфейсі визначається як

$$\mathrm{B}_{\mathrm{wire}} = \frac{\mathrm{S}_{\mathrm{wire}}}{\mathrm{T}_{\mathrm{obs}}}, \tag{2.18}$$

де $\mathrm{S}_{\mathrm{wire}}$ – кількість бітів, що пройшли через точку вимірювання за інтервал спостереження, біт;

$\mathrm{T}_{\mathrm{obs}}$ – тривалість інтервалу спостереження, с.

Корисна швидкість доставки застосунку визначається як

$$G_{app} = \frac{S_{app}}{T_{obs}}, \tag{2.19}$$

де S_{app} – кількість корисних бітів, коректно доставлених застосунку за інтервал спостереження, біт.

Коефіцієнт ефективності доставки визначається як

$$\eta = \frac{G_{app}}{B_{wire}}, \tag{2.20}$$

Суммарні накладні витрати в байтах на одиницю даних визначаються як

$$h_{tot} = L_{wire} - L_{app}, \tag{2.21}$$

де L_{app} – розмір корисного навантаження, байт;

L_{wire} – розмір відповідної одиниці даних на зовнішньому інтерфейсі після додавання заголовків, службових полів, інкапсуляцій і padding, байт.

Мультиплікативний overhead визначається як

$$\Omega_{tot} = \frac{L_{wire}}{L_{app}} = 1 + \frac{h_{tot}}{L_{app}}, \tag{2.22}$$

де Ω_{tot} – безрозмірний коефіцієнт сумарних накладних витрат.;

Для аналізу внеску окремих рівнів сумарні накладні витрати подаються як

$$h_{tot} = h_{net} + h_{fec} + h_{vpn} + h_{prx}, \tag{2.23}$$

де h_{net} – накладні витрати базового мережевого стека, байт;

h_{fec} – лужбові поля та відновлювальні дані FEC, байт;

h_{vpn} – заголовки та службові поля VPN, байт;

h_{prx} – накладні витрати проксі-протоколу і транспорту, байт.

Path MTU позначається як M_{PMTU}, це – максимальний розмір пакета на шляху без фрагментації, байт).

Максимально допустимий корисний розмір без фрагментації визначається як

$$L_{max} = M_{PMTU} - h_{tot}, \quad (2.24)$$

Частка фрагментованих пакетів визначається як

$$\xi_{frag} = \frac{N_{frag}}{N_{plt}^{wire}}, \quad (2.25)$$

де N_{frag} – кількість випадків фрагментації;

N_{plt}^{wire} – кількість переданих пакетів зовнішнього IP-рівня.

Ефективно знайдений розмір для режиму робастного керування MTU визначається як

$$M_{eff} = max\{L_{app}: \text{доставка тестових датаграм без деградації}\}, \quad (2.26)$$

де M_{eff} – ефективно знайдений розмір корисного навантаження, байт.

Час готовності VPN-шару визначається як

$$T_{vpn} = t_{vpn}^{ready} - t_{vpn}^{start}, \quad (2.27)$$

де t_{vpn}^{start} – момент початку встановлення тунелю, с;

t_{vpn}^{ready} – момент, коли тунель здатний передавати коректно захищені пакети, с.

Час переукладання ключового матеріалу визначається як

$$T_{rekey} = t_{rekey}^{ready} - t_{rekey}^{start}, \quad (2.28)$$

де t_{rekey}^{start} – момент початку процедури rekey;

t_{rekey}^{ready} – момент готовності нового криптографічного контексту, с.

Показник часу підготовки захищеного каналу визначається як

$$\tau_{\text{setup}} = t_{\text{ready}} - t_{\text{start}}, \tag{2.29}$$

де t_{rekey}^{start} – момент початку процедури rekey;

Час до отримання першого корисного байта застосунку визначається як

$$T_{\text{ttfb}} = t_{first\_byte}^{rx} - t_{session}^{start}, \tag{2.30}$$

де $t_{session}^{start}$ – момент ініціації прикладного сеансу, с;

t_{rekey}^{ready} – момент отримання першого корисного байта на приймальній стороні, с.

Завантаження процесора визначається як

$$u_{\text{cpu}} = \frac{T_{cpu}}{T_{obs}}, \tag{2.31}$$

де T_{cpu} – сумарний процесорний час, витрачений компонентами моделі за інтервал спостереження, с.

Питома вартість оброблення в циклах на байт визначається як

$$c_{\text{cpu}} = \frac{C_{cpu}}{S_{app}^{B}}, \tag{2.32}$$

де c_{cpu} – кількість процесорних циклів на один корисний байт, цикл/байт;

C_{cpu} – загальна кількість процесорних циклів, витрачених на оброблення трафіку, цикл;

S_{app}^{B} – кількість корисних байтів, доставлених застосунку, байт.

Пікове споживання пам’яті визначається як

$$\mathrm{m_{peak}} = \max_{t} m(t), \tag{2.33}$$

де $m(t)$ – обсяг пам’яті, споживаний компонентами моделі в момент часу t, байт;

Відповідність профілю безпеки задається індикатором

$$\sigma_{\mathrm{sec}} = \begin{cases} 1, \text{протоколи відповідають політиці безпеки;} \\ 0, \text{у інших випадках} \end{cases}, \tag{2.34}$$

За потреби ранжування конфігурацій одним числом може використовуватися допоміжний утилітарний показник

Оцінювання ефективності конфігурацій у запропонованій моделі виконується за сукупністю показників надійності, часових характеристик, накладних витрат, ресурсного навантаження та безпеки. При цьому результати аналізуються як багатокритеріальна система показників без зведення їх до єдиного інтегрального індексу, що дозволяє уникнути суб’єктивного вибору вагових коефіцієнтів та забезпечує прозору інтерпретацію результатів.

У подальших методах запропоновані метрики використовуються не ізольовано, а як узгоджена система обмежень, критеріїв оптимізації та діагностичних індикаторів причин деградації. На етапі моделювання фізичного рівня показники якості каналу γ і Γ_{dB}, а також імовірності помилки P_b і P_w застосовуються для параметризації умов передавання та переходу до пакетної моделі втрат або стирань ε. Такий перехід відповідає загальноприйнятому зв’язку між характеристиками фізичного каналу та показниками помилок у цифрових системах зв’язку.

На етапі FEC підбираються параметри R, ρ, а також пакетні параметри K_s, K_r і φ таким чином, щоб за заданого значення ε забезпечити необхідний рівень P_{dec} і, як наслідок, підвищити наскрізну частку успішної доставки Π_{e2e} за контрольованого зростання Ω_{tot} та зниження η. Така постановка узгоджується з

підходом FECFRAME, у межах якого надлишковий FEC-трафік розглядається як цілеспрямований механізм компенсації втрат пакетів.

На рівні VPN і proxy принциповим є те, що криптографічні перевірки перетворюють частину пошкоджених даних на безумовно відкинуті пакети. Саме тому показники Π_{vpn}і Π_{proxy} є критично важливими для локалізації причин деградації та пояснення того, на якому етапі тракту втрачається трафік. Для IPsec така поведінка безпосередньо випливає з правила відкидання датаграми у разі невдалого проходження перевірки цілісності. Метрики h_{tot}, Ω_{tot}, M_{MTPU}, L_{max}, ξ_{frag} використовуються для того, щоб методи керування пакетизацією та вибору профілю шифрування не призводили до фрагментації та порушення коректної роботи механізмів PMTU discovery. Такий зв'язок має не лише теоретичний, а й прикладний характер, оскільки накладні витрати ESP можуть збільшувати розмір пакетів до рівня, що перевищує MTU, провокувати фрагментацію та викликати проблеми з визначенням допустимого розміру датаграм; серед практичних заходів протидії таким ситуаціям розглядаються, зокрема, зменшення MTU та TCP MSS clamping. Додатково крихкість фрагментації як мережевого механізму підтверджується відповідними рекомендаціями IETF. Якщо в методі передбачено робастне керування розміром датаграм, то показник M_{eff} набуває значення вихідної метрики ефективності алгоритму PMTU-адаптації, узгодженої з підходом DPLPMTUD.

У часовому аналізі показники τ_p і v_τ використовуються для кількісного оцінювання критеріїв якості обслуговування та стабільності функціонування системи. Зокрема, значення τ_p характеризує рівень затримки передавання даних, а показник v_τ відображає варіацію затримки та ступінь нестабільності часових характеристик каналу. Відповідно, методика вимірювання затримки та втрат має бути відтворюваною і узгодженою з підходами IPPM, а визначення односпрямованої затримки та варіації затримки доцільно спирати на профільні документи IETF.

У дослідженнях пропускної здатності показники B_{wire}, G_{app} і η дозволяють розмежувати валовий мережевий трафік і корисний результат доставки, а також кількісно оцінити ціну використання FEC і багатошарової інкапсуляції. За таких умов контроль сценаріїв throughput-вимірювань із фіксацією Path MTU є необхідним, а самі процедури вимірювання та подання результатів доцільно узгоджувати з підходами до TCP throughput testing і загального мережевого бенчмаркінгу.

Безпекова частина моделі виконує функцію фільтра конфігурацій. Значення $\sigma_{sec} = 0$ означає, що відповідна конфігурація не підлягає подальшому порівнянню за продуктивністю, тоді як значення $\sigma_{sec} = 1$ допускає її до профілювання та експериментального аналізу. Вибір алгоритмів IKEv2 і ESP/AH доцільно задавати через вимоги та рекомендації профільних RFC, що дає змогу уникнути фіксації в тексті дисертації застарілих або надмірно жорстко прив’язаних до часу наборів криптографічних механізмів . Водночас архітектурна роль IPsec та IKE має визначатися базовими документами, а практичний зв’язок між вибором алгоритмів, накладними витратами та процесорним навантаженням додатково підтверджується рекомендаціями NIST.

Для порівняння альтернативних VPN-підходів у межах єдиної моделі можуть застосовуватися ті самі метрики часу, ресурсних витрат і накладних витрат. Зокрема, для WireGuard як тунелю мережевого рівня з акцентом на продуктивність, простоту реалізації та прозорість механізму обміну ключами змістовними є показники T_{vpn}, T_{recey}, u_{cpu}, Ω_{tot} і G_{app}, які відображають практичні наслідки вибраного протокольного дизайну. Аналогічно, для proxy-рівня на базі XRay найбільш інформативними вихідними показниками є T_{ttfb}, Π_{prx}, Ω_{tot} і η, оскільки саме вони відображають часову, транспортну та ресурсну ціну застосування відповідних протоколів у реальних сценаріях передавання [42]. Окрему проблему для стабільності передавання створює фрагментація IP-пакетів у сучасних мережевих середовищах [43].

2.4 Концептуальна модель гібридного захищеного каналу даних

Гібридний захищений канал розглядається як наскрізний тракт, у якому надійність формується поєднанням завадостійкого кодування (на фізичному та/або пакетному рівні), а захищеність забезпечується криптографічним оверлеєм і проксі-платформою з функціями віртуальної маршрутизації трафіку. Концептуально ця декомпозиція узгоджується з багаторівневим поданням мережевих систем, яке задає базова модель OSI, де фізичні впливи на сигнал відокремлено від механізмів тунелювання, маршрутизації та прикладної логіки.

Щоб уніфікувати об’єкт оцінювання між рівнями, базовою «одиницею доставки» приймається ADU (Application Data Unit). Саме ADU є логічним об’єктом, який має бути доставлений коректно до рівня застосунку незалежно від того, як саме він пакетується, кодується або інкапсулюється.

Функціонально тракт складається з таких підсистем. На передавальній стороні дані застосунку перетворюються у послідовність ADU, після чого виконується пакетизація та накладання надлишковості. Надлишковість може реалізовуватися двома способами: як канальне/фізичне завадостійке кодування з параметрами (n, i) та як пакетне FEC у термінах FECFRAME, де формуються FEC Source Packets і FEC Repair Packets та задається «protection amount» як відносне збільшення обсягу переданих даних [44-47].

Якщо в моделі використовується «ковзне вікно» для FEC поверх пакетного потоку, то воно розглядається як окремий режим кодування. Для цього режиму потрібні ідентифікатори положення ADU у потоці (Source FEC Payload ID) та зв’язку repair-символів із вихідними символами (Repair FEC Payload ID), що задається розширенням FECFRAME на sliding window коди. Теоретичні основи сучасних схем FEC та ітеративного декодування детально розглянуті у роботах з сучасної теорії кодування [48-50]. Особливо важливу роль такі механізми відіграють у космічних системах зв’язку з високим рівнем завад [51]. У стандартах 3GPP аналогічні підходи використовуються для мереж нового покоління NR [52]. Тому також доречно зазначити, що LDPC-коди також широко застосовуються у

системах космічного зв’язку CCSDS [53]. Окрему увагу сучасні дослідження приділяють стійкості VPN-тунелювання до постквантових загроз [54]. Практичні експерименти із постквантовими VPN-підходами також активно проводяться провідними IT-компаніями [55]. Перехід до quantum-safe криптографії розглядається як один із ключових напрямів розвитку захищених мережевих систем [56].

Далі дані потрапляють до захищеного оверлею. Для протоколів сімейства IPsec ключовим поняттям є Security Association як односпрямоване логічне з’єднання, у межах якого застосовується однакове безпекове перетворення (AH/ESP) та підтримується стан безпеки. Встановлення і підтримання цього стану у масштабованому режимі виконується протоколом IKEv2, який структурно містить IKE_SA_INIT, IKE_AUTH, а також обміни CREATE_CHILD_SA для створення та rekey як IKE SA, так і Child SA [57-59].

Проксі-рівень (V2Ray/XRay) в моделі трактується не як «ще один VPN», а як програмована платформа маршрутизації з множинними inbound/outbound і внутрішнім диспетчером, який обирає outbound для з’єднання на підставі правил. У документації V2Ray це описано як внутрішню архітектуру inbound → Dispatcher/Router/DNS → outbound, а також як механізм routing на базі правил і balancer-ів. Аналогічно для XRay routing-модуль визначається як механізм, що спрямовує inbound-дані через різні outbound за правилами, реалізуючи «on-demand proxying».

У межах запропонованої концептуальної моделі профіль гібридного каналу характеризується набором параметрів, що визначають режими функціонування підсистем завадостійкого кодування, FEC та захищеного оверлею. Для подальшої формалізації профіль каналу доцільно подати у вигляді конфігураційного вектора p:

$$p = (\mathrm{n}, \mathrm{i}, \varphi_{\mathrm{FEC}}, \mathrm{W}_{\mathrm{FEC}}, \mathrm{L}_{\mathrm{ADU}}, \mathrm{P}_{\mathrm{ovl}}, \mathrm{R}_{\mathrm{route}}), \tag{2.35}$$

де φ_{FEC} – відносний обсяг repair-пакетів у механізмі FECFRAME;

W_{FEC} – параметр вікна для режиму sliding window;

L_{ADU} – розмір ADU або корисного навантаження після пакетизації;

P_{ovl} – тип захищеного оверлею (IPsec, OpenVPN, WireGuard, V2Ray/XRay як proxy-оверлей);

R_{route} – правило або політика маршрутизації.

Важливо, що p повинен бути достатньо повним, аби з нього однозначно обчислювалися всі метрики, введені у 2.1-2.3, та перевірялися обмеження допустимості.

Для узгодження з IDEF0-логікою тракт коректно описується як функція перетворення: входи I1 (прикладні дані), I2 (службові дані сеансу), I3 (початкові параметри), керування C (політика безпеки, SLA, обмеження ресурсів), механізми M (кодер/декодер, VPN-стек, proxy-платформа, апаратна платформа), виходи O (відновлені ADU, журнали вимірювань, значення метрик для зворотного зв'язку). Блок-схема тракту представлена на рисунку 2.5. Така форма подання потрібна, щоб забезпечити логічну трасованість між розділами: у 3-му розділі реалізуються механізми M, у 4-му перевіряються виходи O та виконання керуючих обмежень. Відображення інтерфейсів між рівнями та потоки метрик представлені на рисунку 2.6.

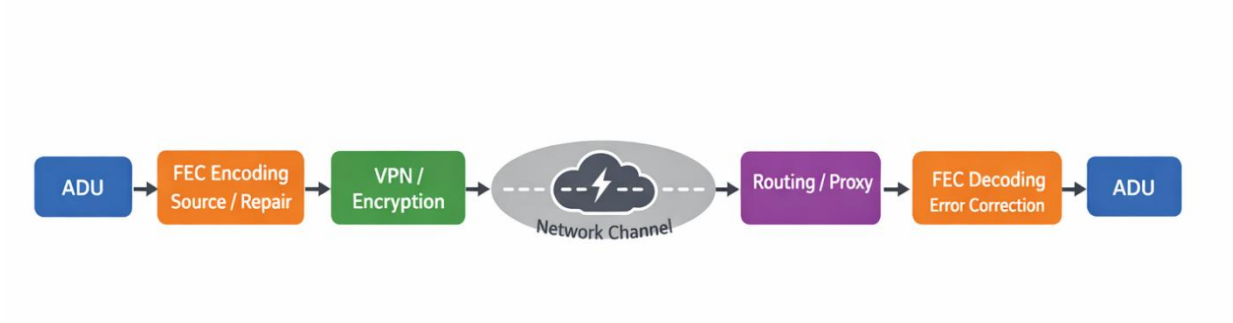


Рисунок 2.5 – Блок-схема наскрізного тракту

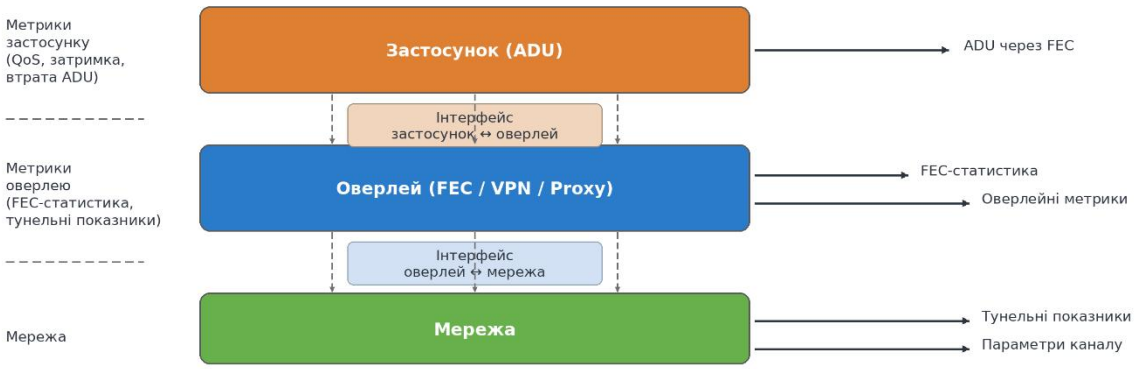


Рисунок 2.6 – Відображення інтерфейсів між рівнями та потоки метрик

Для узгодженого кількісного подання складової захищеності в межах інтегрованої оцінки доцільно ввести інтегральний індекс захищеності I_{sec}, який відображає рівень реалізації базових властивостей безпеки захищеного каналу. На відміну від метрик надійності та продуктивності, що характеризують якість функціонування системи в умовах завад і обмежень середовища, індекс I_{sec} узагальнює результати перевірки автентифікації, контролю цілісності, стійкості до replay-впливів та стабільності підтримання захищеної сесії.

Безпекова складова в моделі розглядається не як безперервний індекс якості, а як множина обов'язкових вимог до криптографічного профілю. Тому для оцінювання використовується індикатор відповідності профілю безпеки σ_{sec}.

2.5 Метод синтезу профілю гібридного захищеного каналу

Метод синтезу профілю призначений для вибору конфігурації p до початку сеансу або для формування «базового профілю» під заданий клас умов. Його роль у дисертації полягає в тому, щоб перетворити перелік метрик у формальну задачу вибору параметрів і забезпечити наукову новизну через системне поєднання шарів: завадостійкого кодування, VPN-захисту та програмованої proxy-маршрутизації.

На першому етапі задається політика безпеки та довіри, яка визначає допустимі протоколи й режими оверлею. Для IPsec це означає наявність керування станом через SA та ключового обміну через IKEv2. Для OpenVPN політика довіри

може формулюватися через PKI з сертифікатами та CA, де сервер і клієнти мають власні пари ключів і здійснюють взаємну перевірку сертифікатів. Для WireGuard політика задається відповідністю публічного ключа пира і «ідентичності тунелю», що є принципом дизайну протоколу та дозволяє компактно формалізувати аутентифікацію як перевірку відповідного ключа.

На другому етапі формується множина кандидатних профілів P_{adm} як декартів добуток допустимих значень параметрів кодування та оверлею, але з попереднім відсіканням конфігурацій, які суперечать вимогам сучасної криптографічної практики. Для IPsec це доцільно обґрунтовувати тим, що для ESP і AH існує окреме керівництво з актуалізації криптографічних алгоритмів і принципу «encryption must be authenticated», тобто шифрування має бути автентифікованим, а набори алгоритмів мають підтримувати актуальність у часі.

На третьому етапі для кожного кандидата p оцінюється пакетизаційна придатність. Тут важливий акцент роботи: багатошарова інкапсуляція (FEC + VPN + proxy) збільшує накладні витрати й підвищує ризик фрагментації, а фрагментація вважається крихким механізмом, що вводить fragility в інтернет-комунікацію і має уникатися або контролюватися. У межах методу це оформлюється як перевірка умов на ефективний максимальний розмір корисної частини та як рекомендація застосування робастного PMTU-підходу. Саме DPLPMTUD формалізує ідею пробінгу, виявлення «black hole» і вимогу, що upper layer має коригувати максимальний розмір повідомлення з урахуванням додаткового overhead, який цей рівень додає.

На четвертому етапі виконується надійнісне узгодження. Для кожного p оцінюється, яка надлишковість потрібна на пакетному рівні для досягнення цільової ймовірності успішної доставки ADU, а також яка «ціна» цього рішення у вигляді втрати goodput та збільшення затримки. Тут застосовується апарат FECFRAME: ADU групуються у блоки або вікна, генеруються source/repair пакети, а «protection amount» виступає керованою змінною, яку можна напряму пов’язувати з витратами трафіку.

П’ятий етап є власне оптимізаційним вибором. У найпростішому вигляді синтез можна записати як задачу: знайти

$$p^* = \arg\min_{p \in \mathrm{P_{adm}}} J(p), \tag{2.36}$$

де p – профіль гібридного каналу;

$J(p)$ – скалярний критерій ранжування допустимих рішень;

Множина допустимих профілів визначається системою порогових обмежень на метрики, введені у підрозділах 2.1–2.3

$$\mathrm{P_{adm}} = (\mathrm{p} \in P | \Pi_{\mathrm{e2e}} \geq \Pi_{\min}, \tau_{95}(\mathrm{p}) \leq \tau_{max}, \mathrm{G}_{app}(\mathrm{p}) \geq \mathrm{G}_{min},$$

$$\Omega_{tot}(\mathrm{p}) \leq \Omega_{max}, \xi_{frag} = 0), \tag{2.37}$$

де P – повна множина розглядуваних профілів;

$\Pi_{\min}, \tau_{max}, \mathrm{G}_{min}, \Omega_{max}$ – гранично допустимі значення відповідних метрик.

За такого підходу критерій J(p) не замінює обмеження допустимості, а використовується лише для ранжування тих профілів, які вже задовольняють базові вимоги. Це зменшує суб’єктивність вибору та забезпечує відтворюваність результатів експериментального дослідження. Одразу можна звернути увагу на Залежність надійності доставки від відносного обсягу repair-пакетів рисунок 2.7, а також залежність відносного службового залишку відрозміру ADU рисунок 2.8.

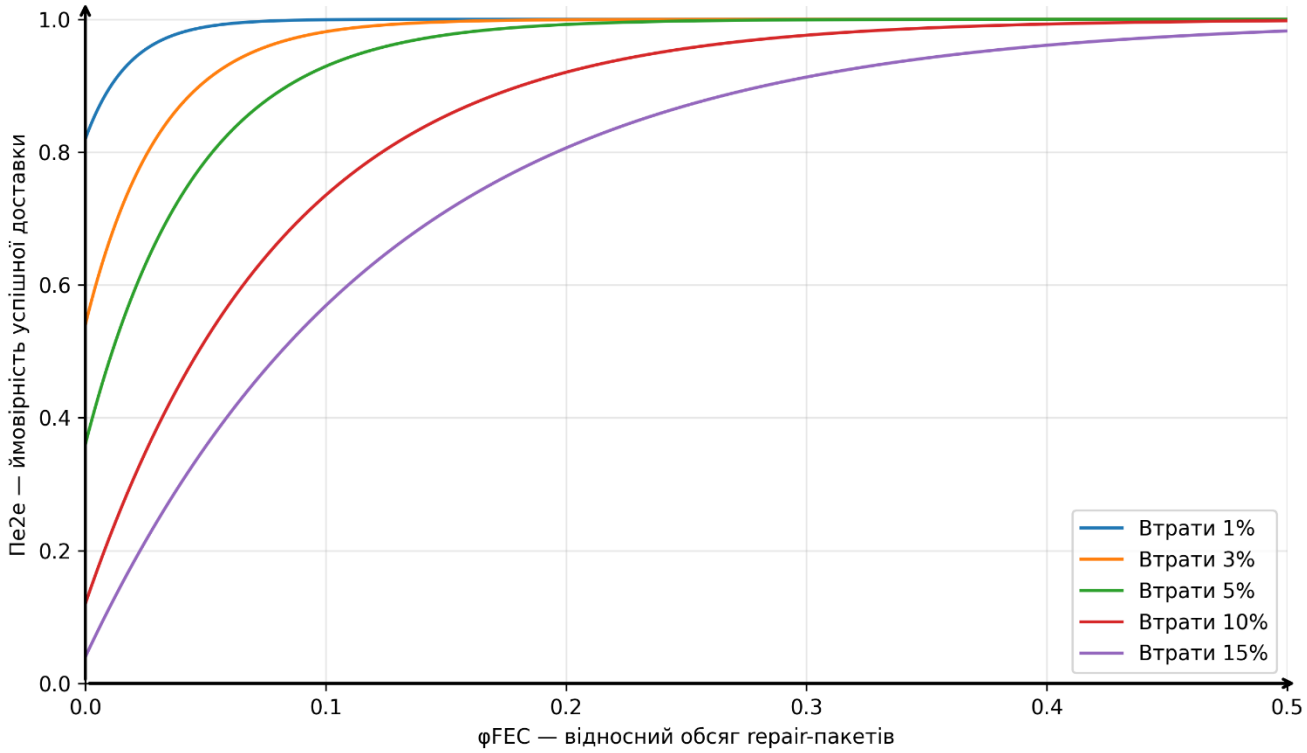


Рисунок 2.7 – Надійність доставки залежно від відносного обсягу repair-пакетів

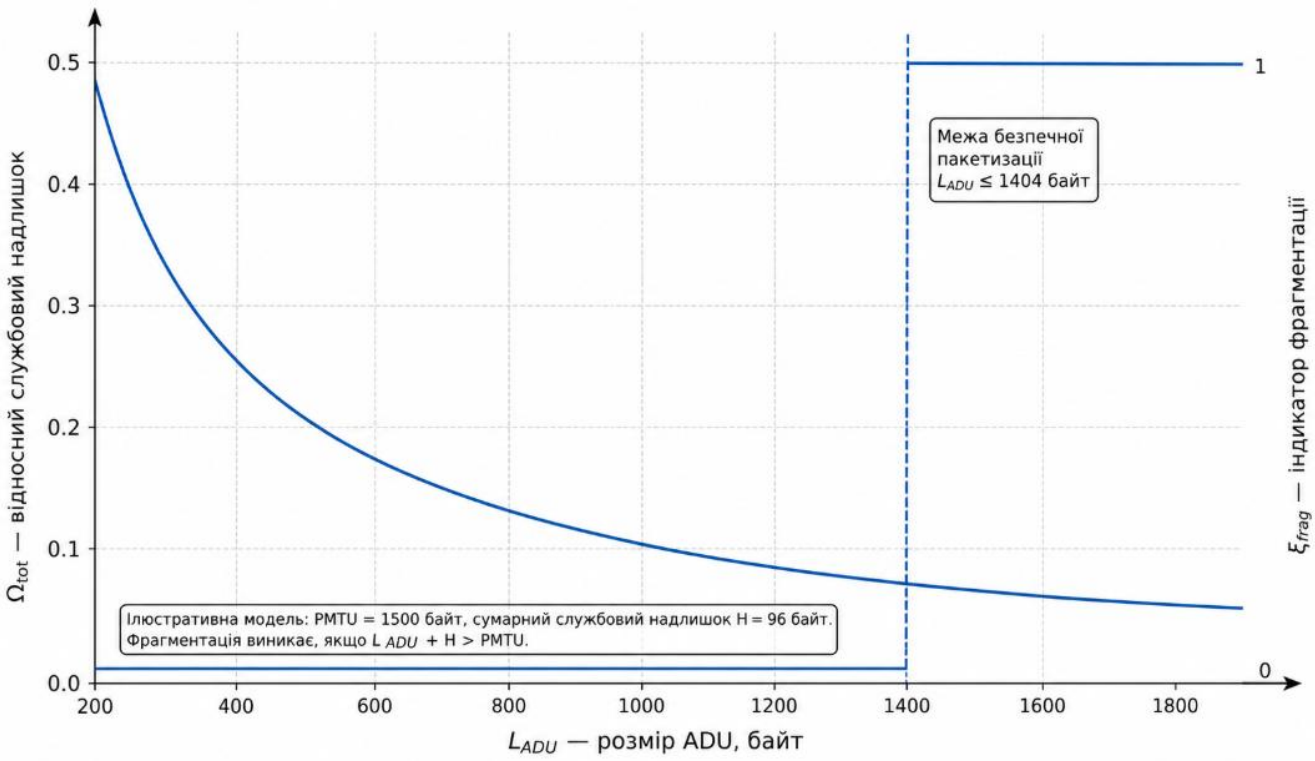


Рисунок 2.8 – Ω_{tot} і ξ_{frag} залежно від L_{ADU}

2.6 Метод адаптивного керування параметрами FEC оверлею

Метод адаптивного керування вводиться як замкнений контур, у якому система під час сеансу вимірює поточні значення метрик (втрати, затримку, goodput, накладні витрати, фрагментацію) та змінює керовані параметри p так, щоб підтримувати виконання SLA і вимог безпеки. На відміну від «одноразового налаштування», адаптація робить модель придатною для динамічних каналів і середовищ, де параметри мережі та умови протидії змінюються в часі.

При цьому показник SNR доцільно розглядати не лише як параметр початкового сценарію, а і як поточну вимірювану характеристику фізичного каналу, що змінюється в часі в процесі сеансу. У межах запропонованої інформаційної технології значення γ використовується як вхід телеметричного контуру для інтерпретації причин деградації передавання та для відокремлення погіршення, зумовленого саме фізичним середовищем, від наслідків фрагментації, втрат пакетів, зміни маршруту або криптографічного відкидання пошкоджених пакетів. Це дає змогу пов’язати поточний стан каналу зі змінами показників Π_{e2e}, λ_{e2e}, τ_{95}, G_{app}, Ω_{tot} BER, FER, та і, відповідно, коригувати значення φ, L_{adu} та параметри захищеного оверлею не за наперед заданим профілем, а відповідно до фактичної динаміки каналу.

Оцінювання стану каналу в режимі реального часу здійснюється на основі телеметричних даних, які збираються у ковзному часовому вікні спостереження. До складу телеметрії входять оцінки BER, FER, частки втрачених пакетів, рівня фрагментації, затримки τ_{95}, goodput та службових подій захищеного оверлею. Для підвищення стійкості до випадкових коливань рішення про адаптацію приймається не за миттєвими значеннями метрик, а за їх усередненими або квантильними оцінками у межах вікна спостереження.

Особливу увагу приділено реакції на імпульсні (бурстові) завади. Якщо в межах одного або кількох послідовних вікон спостереження фіксується різке зростання FER, серії втрат пакетів або погіршення показника Π_{e2e}, система інтерпретує таку ситуацію як короткочасну деградацію каналу та тимчасово

переходить до профілю з підвищеною надлишковістю FEC. Після стабілізації показників протягом заданого інтервалу часу виконується повернення до базового профілю. Такий підхід дозволяє уникнути надмірної кількості реконфігурацій і водночас забезпечує швидке реагування на короткочасні збурення каналу.

Ключова наукова ідея адаптації полягає в узгодженні двох контурів керування. Перший контур відповідає за завадостійкість: змінюється надлишковість FEC (φ_{fec}), режим формування ремонтних пакетів (блоковий або sliding window) та, за потреби, політика пакетизації L_{adu}. Другий контур відповідає за оверлей: змінюється транспортний режим або конфігурація оверлейного з'єднання у V2Ray/XRay через правила routing та вибір outbound-вузлів, а також враховуються події керування ключами (handshake, rekey), що можуть короткочасно впливати на затримку і пропускну здатність.

Адаптація FEC у віконному режимі має окреме обґрунтування: sliding window підхід передбачає маркування позицій ADU та зв'язків repair-даних, що дозволяє більш гнучко реагувати на поточні втрати без необхідності чекати завершення великого блоку. Це формалізовано в розширенні FECFRAME для sliding window кодів, де визначено вимоги до payload ID та процедурні аспекти роботи.

Адаптація пакетизації і MTU у методі трактується як обов'язковий елемент, оскільки для багатошарових інкапсуляцій саме «невдалий розмір» часто є причиною деградації. Фрагментація розглядається як крихка й небажана, тому адаптація має підтримувати розмір корисного навантаження у зоні, де фрагментація не виникає або є контрольованою. Для UDP-орієнтованих протоколів і proxy-транспортів доцільно спиратися на DPLPMTUD, який визначає робастний спосіб виявлення підтримуваного розміру датаграми та зменшення розміру при «black hole», а також прямо вимагає врахування overhead верхніх рівнів у виборі MPS.

Адаптація маршрутизації в V2Ray/XRay формалізується як зміна R_route, тобто як зміна набору правил, outboundTag або використання balancer-ів на підставі

вимірюваної якості для класів трафіку. У класичному VPN маршрутизація обмежена «тунель є або немає», тоді як V2Ray/XRay дозволяє керувати вибором вихідного з'єднання на рівні правил для кожного inbound-з'єднання.

Окремо в методі враховуються події керування криптографічним станом. Для IPsec це треба пояснювати через модель IKEv2: початкові обміни IKE_SA_INIT та IKE_AUTH устанавливають IKE SA і перший Child SA, а CREATE_CHILD_SA використовується для створення нових Child SA та rekey. Тому в адаптивному керуванні корисно трактувати rekey як подію, що змінює часові характеристики та може вимагати тимчасового підсилення FEC або зміни маршруту для критичних потоків. Особливу увагу треба звертати на події у збурених каналах під час адаптивного керування. Часові ряди по метрикам представлені на рисунку 2.9.

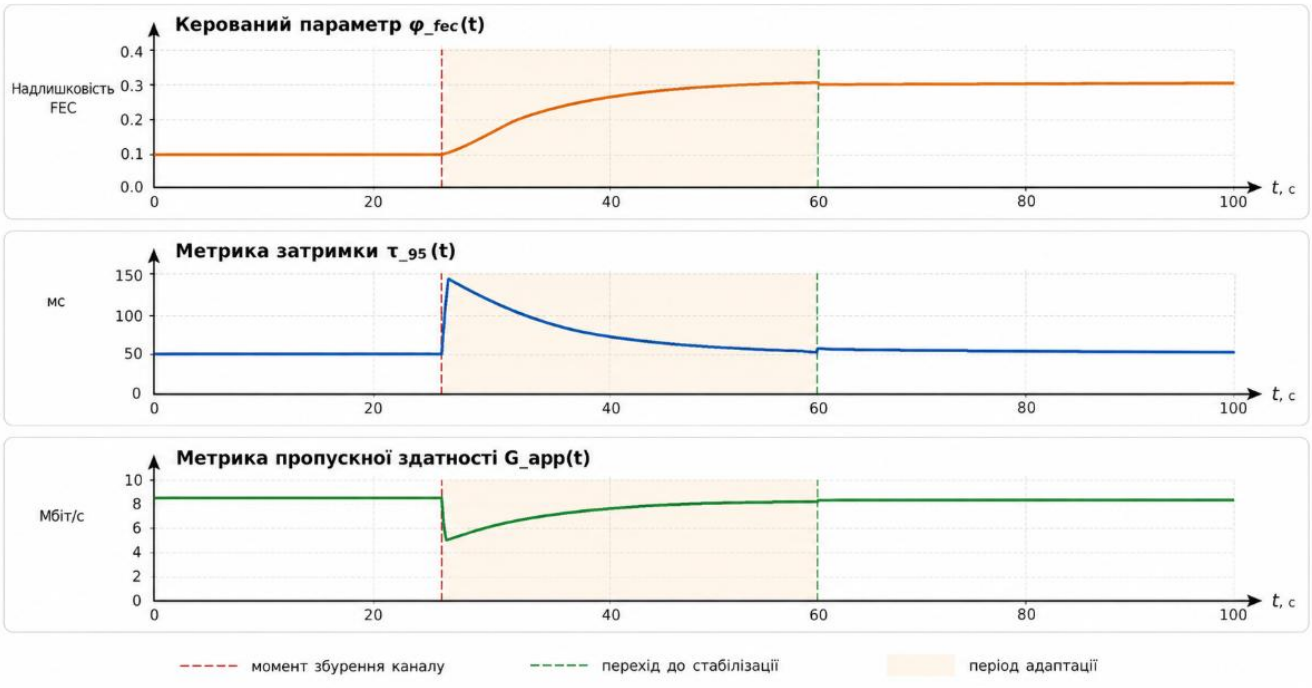


Рисунок 2.9 – Часові ряди метрик і керованих параметрів, наприклад «$\varphi_{fec}(t)$, $\tau_{95}(t)$, $G_{app}(t)$»

2.7 Критерії оптимізації й обмеження профілю гібридного каналу

Критерії оптимізації задаються так, щоб кожен критерій був вимірюваний у майбутньому розділі експериментів і не вимагав «напівформальних» індексів.

Базова ідея полягає в тому, що оцінка ведеться за наскрізними метриками доставки, часу та ефективності, а безпека задається як обмеження допустимості конфігурації, а не як довільний числовий «індекс».

Інтегральний показник захищеності в подальшому використовується не як самостійна ціль оптимізації, а як допоміжний діагностичний показник для порівняння допустимих профілів. На етапі синтезу профілю першочергово перевіряється виконання обмежень допустимості за показниками надійності, затримки, фрагментації та ресурсного навантаження. Лише в межах множини допустимих профілів виконується ранжування за функцією корисності, що враховує ефективну швидкість, накладні витрати та обчислювальну ціну реалізації.

У якості основного результатного критерію використовується ймовірність коректної доставки ADU до застосункуП$_{e2e}$, оскільки саме вона узгоджує фізичні завади, втрати пакетів, дію FEC та поведінку криптографічного оверлею. Ця позиція логічно випливає з постановки FECFRAME, де FEC накладається на потік ADU і повертає відновлені ADU при наявності достатньої кількості source/repair даних.

Другий ключовий критерій пов’язаний із затримкою. Для дисертації доцільно використовувати не тільки середнє значення, а квантили (наприклад, τ_{95}), оскільки саме хвости затримки визначають якість сервісу у присутності фрагментації, retransmit-подій, rekey-подій і змін маршруту. У цій постановці τ_{95} є критерієм мінімізації або критерієм порогового обмеження, який перевіряється в експерименті.

Третій критерій описує ефективність використання мережевого ресурсу як корисну швидкість доставки G_{app} або, якщо у вас уже введено окремо throughput і goodput, як goodput на рівні застосунку. Сенс цього критерію для новизни в тому, що FEC і оверлей одночасно збільшують трафік і навантаження, а отже оптимальне рішення має показувати, що підвищення П$_{e2e}$ досягнуте не «заливанням каналу» repair-даними, а керованим компромісом.

Окремою групою критеріїв вводиться «вартість профілю». Вона включає мультиплікативний overhead Ω_{tot}, обчислювальну вартість (наприклад, u_{cpu}), а також частку фрагментації ξ_{frag}. Для фрагментації потрібне окреме обґрунтування: RFC 8900 визначає фрагментацію як джерело fragility і надає рекомендації розробникам і операторам щодо альтернатив та зменшення залежності від фрагментації. Для керування MTU у дейтаграмних транспортів доцільно включати робастність до PMTU black hole і принцип урахування overhead, тобто можливість застосувати DPLPMTUD або сумісний механізм у рівні пакетизації.

Обмеження допустимості профілю формуються як набір умов, які мають бути виконані до оптимізаційного ранжування. Обмеження безпеки задаються через відповідність протоколів і алгоритмів політиці. Для IPsec поняття SA та керування ключами через IKEv2 є обов'язковими елементами коректної побудови безпечного оверлею. Додатково для ESP/AH існує окремий документ з вимогами й рекомендаціями до алгоритмів, що прямо підкреслює необхідність «up to date» алгоритмів і принцип «encryption must be authenticated».

Пакетизаційні обмеження формулюються як умова відсутності або мінімізації фрагментації: L_{adu}+ h_{tot} <= M_{pmtu}, де h_{tot} є сумарним overhead від FEC, VPN та proxy, а M_{pmtu} є доступним MTU тракту. Якщо закладається динамічне визначення M_{pmtu}, воно має бути узгоджене з принципами DPLPMTUD і забороною виходити за поточний PLPMTU для не-probe пакетів .

Обмеження якості сервісу задаються як пороги: Π_{e2e} >= Π_{min}, τ_{95}<= τ_{max}, G_{app} >= G_{min}. Обмеження ресурсу задаються як u_{cpu}<= u_{max} і, за потреби, як Ω_{tot} <= Ω_{max}. У такій формі постановка зберігає прямий зв'язок із метриками 2.1-2.3 і дозволяє у 4-му розділі проводити верифікацію без заміни вимірювань на суб'єктивні інтегральні шкали. Корисно буде розглянути графік Парето «τ_{95} (t) проти G_{app} (t)» для різних класів оверлею рисунок 2.10, а також теплову карту залежності фрагментації по Ω_{tot} та L_{ADU}

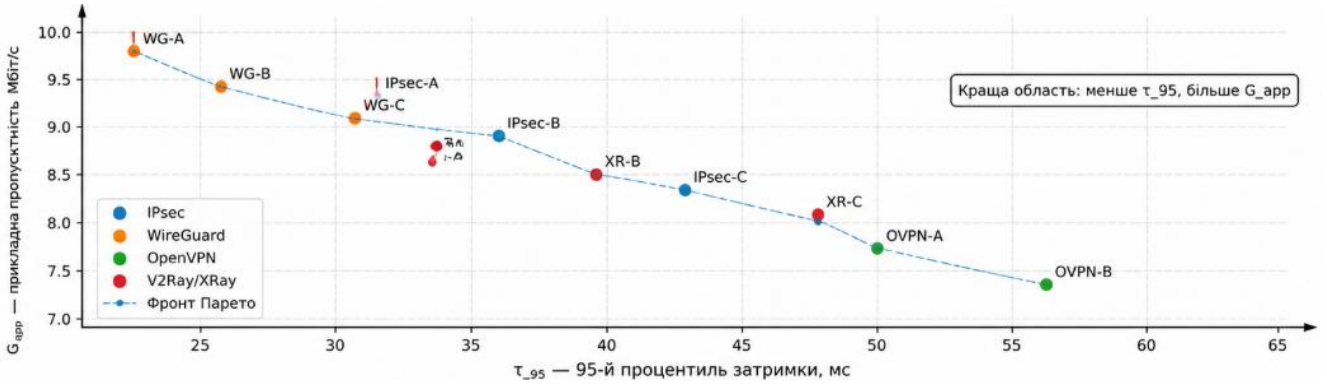


Рисунок 2.10 – Графік Парето «$\tau_{95}(t)$ проти $G_{app}(t)$» для різних класів оверлею

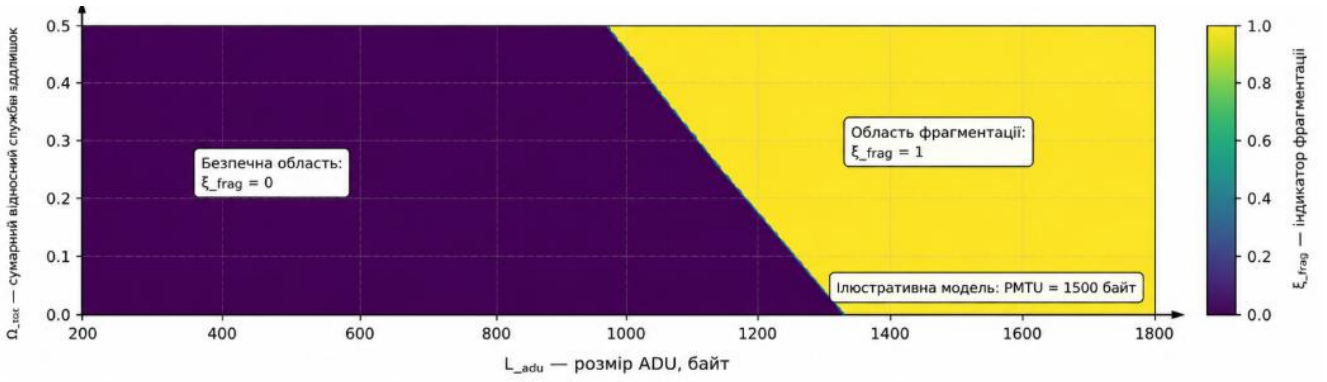


Рисунок 2.11 – Теплова карта, що показує область виконання обмеження фрагментації

2.8 Висновки за розділом

У другому розділі обґрунтовано вибір метрик та показників оцінювання ефективності гібридної інформаційної технології забезпечення надійності й захищеності передавання даних.

1. Виконано формалізацію керуючих впливів, що визначають параметри функціонування системи передавання даних, з урахуванням характеристик мережі, параметрів завадостійкого кодування та особливостей використання захищених оверлейних протоколів.

2. Ввизначено систему метрик для єдиної моделі захищеного каналу передавання даних, що дозволяє комплексно оцінювати показники надійності, захищеності та ефективності функціонування системи.

3. Сформовано набір метрик і відповідних формул для оцінювання характеристик каналу передавання даних, включаючи показники втрат пакетів, імовірності помилки, затримки передавання та ефективності використання ресурсів мережі.

4. Розроблено концептуальну модель гібридного захищеного каналу передавання даних, яка поєднує механізми завадостійкого кодування та VPN-тунелювання в межах єдиного підходу.

5. Запропоновано метод синтезу профілю гібридного захищеного каналу, що забезпечує формування параметрів системи з урахуванням умов функціонування мережі та вимог до якості передавання даних.

6. Розроблено метод адаптивного керування параметрами завадостійкого кодування та захищеного оверлею, який забезпечує зміну конфігурації системи залежно від стану мережі та значень показників ефективності.

7. Визначено критерії оптимізації та обмеження допустимості профілю гібридного каналу, що дозволяють оцінювати доцільність використання певних конфігурацій системи в різних умовах функціонування.

Базу для обраних показників, їх зумовленість та практичність засновано в тому числі за рахунок апробації і розвитку роботи щодо проблематики у каналах зв’язку і методів, що допомагають боротись із завадами [60-62].

За результатами розділу сформовано систему показників, методів та моделей, необхідних для побудови гібридної інформаційної технології забезпечення надійності й захищеності передавання даних. Отримані результати створюють основу для реалізації інтегрованого підходу до адаптивного керування параметрами системи та подальшого дослідження ефективності запропонованих рішень.

РОЗДІЛ 3 РОЗРОБКА МОДЕЛЕЙ ТА МЕТОДІВ ПОБУДОВИ ГІБРИДНИХ ЗАХИЩЕНИХ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

3.1 Загальна архітектура реалізації гібридної технології

Реалізація запропонованої гібридної інформаційної технології ґрунтується на багаторівневій архітектурі, у межах якої механізми завадостійкого кодування, криптографічного захисту, тунелювання, проксі-маршрутизації та моніторингу функціонують не як ізольовані компоненти, а як узгоджена система наскрізного передавання прикладних даних. Така архітектура забезпечує практичне втілення моделей і методів, розроблених у другому розділі, та створює програмно-технічну основу для подальшої експериментальної перевірки у четвертому розділі. Її побудова спирається на сучасні підходи до багаторівневого захисту даних, використання завадостійкого кодування в пакетних потоках, реалізацію захищених оверлеїв та віртуалізацію мережевих функцій.

Архітектурно система організована як послідовність функціональних рівнів, кожен з яких виконує окрему роль у спільному контурі оброблення. На вході технології перебувають прикладні дані, що надходять від сервісів верхнього рівня у вигляді ADU, а також службові параметри сесії, до яких належать вимоги до якості обслуговування, обраний профіль безпеки, допустимі затримки, політики маршрутизації, початкові параметри FEC і правила роботи оверлею. Тим самим вже на етапі входу задається не лише потік корисного навантаження, а й сукупність керувальних впливів, які визначають спосіб його подальшого перетворення. У термінах архітектури це означає, що технологія працює не просто з пакетами, а з прикладними одиницями даних, для яких одночасно мають бути забезпечені доставка, відновлюваність, криптографічний захист і контроль експлуатаційних характеристик.

Перший функціональний рівень архітектури утворює підсистема формування та підготовки потоку даних. На цьому рівні виконується прийом ADU від прикладного джерела, нормалізація їхнього формату, початкова пакетизація та

зіставлення потоку з профілем передавання. Саме тут визначається, які параметри надалі мають бути застосовані до конкретної сесії: який рівень надлишковості допустимий, який клас оверлею використовується, які правила маршрутизації є пріоритетними, чи потребує потік підвищеної стійкості до втрат, а також чи належить він до класу трафіку з жорсткими вимогами до затримки. Таким чином, на верхньому рівні архітектури формується логічний контекст сеансу, а сам потік набуває ознак керованого об’єкта, параметри якого надалі можуть бути змінені в межах механізмів синтезу профілю та адаптивного керування.

Другий рівень утворює FEC-підсистема, яка забезпечує додавання контрольованої надлишковості до потоку даних і реалізує процедури кодування та подальшого декодування. У межах запропонованої архітектури цей рівень не обмежується лише класичним фізичним кодуванням, а розглядається ширше – як програмно реалізований механізм підвищення ймовірності успішного відновлення ADU в пакетному середовищі. Для цього передбачено використання як блокових схем, так і схем із ковзним вікном, узгоджених із підходами FECFRAME. На передавальному боці FEC-підсистема формує source-пакети та repair-пакети, веде облік їхнього взаємозв’язку, підтримує ідентифікацію елементів потоку та передає сформовану послідовність до наступного рівня. На приймальному боці цей самий архітектурний рівень виконує зворотне перетворення: аналізує втрати, визначає можливість відновлення відсутніх елементів і реконструює вихідні ADU. Важливо, що в межах загальної архітектури FEC-підсистема виступає не допоміжним доповненням до VPN, а окремим рівнем керованої надійності, параметри якого узгоджуються з параметрами захищеного оверлею.

Третій рівень архітектури становить криптографічний оверлей, призначений для забезпечення конфіденційності даних, автентифікації учасників обміну та контролю цілісності інформації. У запропонованій реалізації він охоплює класи VPN- та proxy-орієнтованих засобів захисту, зокрема IPsec, OpenVPN, WireGuard, а також екосистемні рішення типу V2Ray/XRay, які поєднують функції тунелювання, маскування та гнучкого керування потоками [63,64]. Для архітектури

принципово важливо, що оверлейний рівень розглядається у двох взаємопов’язаних аспектах. Водночас під час реалізації VPN-модулів необхідно враховувати історично відомі криптографічні вразливості ранніх протоколів тунелювання, зокрема PPTP та MS-CHAPv2 [65]. Перший аспект пов’язаний зі встановленням і підтриманням криптографічного стану: ініціалізацією тунелю, автентифікацією сторін, створенням асоціацій безпеки, зміною ключів, періодичними подіями handshake і rekey. Другий аспект стосується вже власне транспортування захищеного трафіку після встановлення цього стану. Таке розмежування є суттєвим, оскільки саме службові події криптографічного рівня можуть викликати короткочасні сплески затримки, зниження goodput або додаткові накладні витрати, а отже мають бути видимими для контуру керування та системи моніторингу.

Четвертий рівень утворює програмований маршрутизувально-проксійний контур, реалізований на базі V2Ray/XRay. На відміну від класичного VPN-підходу, де переважає модель «єдиний тунель для всього потоку», ця архітектурна складова забезпечує більш гнучкий спосіб організації передавання. Внутрішня логіка такого контуру включає вузли приймання вхідних з’єднань, диспетчеризацію, оброблення правил маршрутизації, вибір outbound-напрямку, балансування між доступними маршрутами та підтримку різних режимів транспортування. Завдяки цьому оверлей у запропонованій архітектурі виконує не лише функцію шифрованої оболонки, а й функцію програмованого середовища керування траєкторією потоку. Це має принципове значення для реалізації методу адаптації, оскільки дозволяє змінювати не тільки параметри надлишковості FEC, а й маршрутні правила, outboundTag, пріоритети каналів та політики оброблення окремих класів трафіку.

Наступним рівнем є середовище передавання, яке в архітектурі розглядається як зовнішнє мережеве оточення з керованими або некерованими деградаціями. У межах експериментального й прикладного контурів це середовище може бути представлене як реальним мережевим сегментом, так і емуляційним каналом із заданими втратами, затримками, варіацією затримки, обмеженнями пропускної

здатності та умовами фрагментації. На цьому рівні проявляються всі негативні ефекти, для компенсації яких і призначена гібридна технологія: випадкові та пачкові втрати, нестабільність затримки, деградація goodput через службовий overhead, проблеми з path MTU, чорні діри PMTU та крихкість фрагментації. Саме тому архітектура має враховувати не лише логіку кодування і шифрування, а й сумарний пакетний бюджет, щоб розмір корисного навантаження, FEC-надлишковість і інкапсуляційні заголовки залишалися узгодженими між собою.

На приймальному боці реалізація архітектури відтворює зворотну послідовність перетворень. Спочатку виконується прийом потоку з мережевого середовища та його передавання до відповідного inbound-модуля оверлею. Далі здійснюються дешифрування, деінкапсуляція, перевірка службових атрибутів сесії, реконструкція source- і repair-компонентів, після чого FEC-декодер відновлює втрачений або пошкоджений обсяг інформації в межах допустимого профілю кодування. Заключний етап полягає у відновленні вихідних ADU та передаванні їх до прикладного рівня. Таким чином, наскрізний тракт реалізації набуває завершеного вигляду: від формування ADU до їх захищеного транспортування, відновлення та доставки у відтвореному вигляді. Саме така композиція рівнів і є практичним втіленням гібридної моделі, у якій захищеність і надійність забезпечуються спільно, а не окремими, неузгодженими засобами.

Окреме місце в архітектурі посідає підсистема моніторингу, телеметрії та зворотного зв’язку. Її призначення полягає у зборі, нормалізації та передаванні метрик між рівнями системи. Точки спостереження доцільно розміщувати перед FEC-кодуванням, після формування repair-потоку, на вході та виході криптографічного оверлею, на межі оверлею й мережі, а також після FEC-декодування на приймальному боці. Це дозволяє отримувати не лише загальну інтегральну оцінку роботи системи, а й локалізувати джерело деградації. Наприклад, з боку FEC можуть зніматися показники втрат, частка успішного відновлення, використаний рівень надлишковості та режим роботи вікна; з боку оверлею – затримка встановлення тунелю, події handshake і rekey, тунельний

overhead, зміни маршруту та стани outbound-каналів; з боку прикладного рівня – goodput, інтегральна затримка, варіація затримки та факт доставки ADU. Саме через таку систему спостереження архітектура набуває властивості керованості, оскільки значення виміряних метрик надалі використовуються в алгоритмах синтезу профілю та адаптивної перебудови параметрів.

У межах запропонованої архітектури система спостереження повинна формувати не лише показники надійності та продуктивності, а і часткові компоненти інтегрального індексу захищеності I_{sec} введеного у підрозділі 2.4. Зокрема, на основі подій автентифікації, відхилення модифікованих пакетів, виявлення повторних передавань та результатів процедур handshake/rekey доцільно обчислювати показники $A_{auth}, A_{int}, A_{rep}, A_{stab}$. Це забезпечує безпосередній зв’язок між концептуально визначеною інтегрованою метрикою захищеності та програмною реалізацією системи, у якій зазначені події вже спостерігаються на рівні телеметричного контуру.

Програмна реалізація архітектури доцільно організовується за модульним принципом, де кожна функціональна підсистема представлена окремим сервісом або групою сервісів із чітко визначеними інтерфейсами взаємодії. Такий підхід узгоджується з практиками NFV, контейнеризації та хмарно-орієнтованого розгортання мережевих функцій. У межах запропонованої архітектури логічно виділяються менеджер сесії, модуль FEC-оброблення, модуль оверлейного захисту, маршрутизувальний проксі-модуль, модуль керування MTU і пакетизацією, а також модуль збору телеметрії. Менеджер сесії координує створення профілю передавання, ініціалізацію потрібних підсистем і передавання їм узгоджених параметрів. FEC-модуль працює з потоками source і repair-пакетів. Оверлейний модуль відповідає за криптографічний контур і параметри тунелю. Маршрутизувальний модуль реалізує правила вибору шляху. Телеметричний модуль накопичує дані для зворотного зв’язку та експериментального аналізу.

Коефіцієнт надлишковості FEC φ у межах запропонованої архітектури розглядається як один із керованих параметрів профілю передавання. Значення φ

визначає співвідношення між обсягом repair-пакетів і source-пакетів та безпосередньо впливає на імовірність відновлення даних, накладні витрати, затримку й корисну пропускну здатність. Саме тому φ має використовуватися як вхідний параметр у процедурах синтезу профілю гібридного каналу та в контурі адаптивного керування поряд із вибором захищеного оверлею та маршруту передавання.

До складу телеметричного модуля доцільно включити засоби вимірювання τ_{setup}, що фіксують час від ініціації захищеного каналу до переходу системи у стан готовності до передавання корисних даних. Значення τ_{setup} використовуються для порівняння часових витрат входу системи у захищений режим для профілів IPsec, OpenVPN, WireGuard та XRay.

У складі телеметричного модуля доцільно передбачити підсистему оцінювання бітової помилки BER, яка визначається шляхом зіставлення еталонної та прийнятої бітових послідовностей на контрольних точках передавання. Така підсистема дозволяє оцінювати рівень деградації фізичного каналу до та після застосування FEC-оброблення, а також відокремлювати вплив завад середовища від впливу тунелювання, пакетизації та маршрутизаційного профілю. Значення BER надалі використовуються разом із показниками $П_{e2e}$, τ_{95}, G_{app} та Ω_{tot} для аналізу ефективності сформованого профілю передавання в умовах різної якості каналу.

На основі отриманих залежностей BER(SNR) та FER(SNR) у складі аналітичного контуру доцільно також визначати виграш кодування G_{code} як зсув за віссю SNR між профілем без FEC та профілем із FEC, за якого досягається однаковий цільовий рівень помилок. Такий показник дозволяє подати ефект застосування завадостійкого кодування у компактному вигляді та безпосередньо оцінити, наскільки використання FEC зменшує вимоги до якості фізичного каналу. Значення G_{code} є похідною характеристикою від BER і FER, проте саме воно забезпечує зручне порівняння різних профілів кодування та захищеного оверлею в узагальненій форм

До складу телеметричного модуля доцільно включити засоби формування часткових показників $A_{auth}, A_{int}, A_{rep}, A_{stab}$, на основі яких надалі визначається інтегральний індекс захищеності I_{sec}. Такий підхід дозволяє узгодити програмну реалізацію системи з формалізованими метриками другого розділу та забезпечує підготовку чисельних даних для експериментального оцінювання захищеності у четвертому розділі.

До складу телеметричного модуля також доцільно включити засоби фіксації τ_{SA} для первинного встановлення тунелю та для подій повторного узгодження ключового матеріалу. Це дозволяє розмежувати часові витрати на запуск захищеного каналу та часові характеристики передавання в усталеному режимі, які описуються метрикою τ_{95}. До складу телеметричного модуля доцільно включити підсистему спостереження за поточним значенням SNR, яка фіксує зміну γ у часі та узгоджує ці дані з часовими рядами. Така синхронізація дає змогу оцінювати не лише статичний вплив окремих значень SNR, а і динамічний вплив коливань якості каналу на поведінку всієї системи. У результаті SNR використовується як спостережувана метрика стану фізичного середовища, за якою пояснюється момент переходу системи до режиму підвищеної надлишковості, зміни параметрів пакетизації або вибору іншого захищеного профілю. Така декомпозиція не лише спрощує реалізацію й супровід, а й дозволяє масштабувати окремі частини системи залежно від сценарію застосування, апаратних ресурсів і вимог до продуктивності.

Окремою складовою телеметричного модуля є підсистема вимірювання показників BER, FER та виграшу кодування (coding gain). Зазначена підсистема виконує зіставлення еталонної та прийнятої бітової послідовності на контрольних точках до FEC-кодування, після проходження каналу та після FEC-декодування, а також формує оцінку частки кадрів, у яких після відновлення збереглися помилки. Це дає змогу відокремити вплив фізичних завад і втрат каналу від впливу тунелювання, фрагментації та зміни маршруту. Виграш кодування визначається як зсув за SNR між профілем без FEC та профілем із FEC, за якого досягається однаковий цільовий рівень BER або FER. Сформовані оцінки передаються до

підсистеми аналізу та адаптивного керування і надалі використовуються разом із показниками Π_{e2e}, λ_{e2e}, τ_{95}, G_{app}, Ω_{tot} та ξ_{frag} для вибору раціональних значень φ, L_{adu} і профілю захищеного оверлею.

Важливою особливістю архітектури є її сумісність зі стандартним мережевим стеком і можливість роботи без радикального порушення існуючої інфраструктури. Запропонована технологія не потребує повної заміни транспортних механізмів або перебудови прикладних сервісів. Її інтеграція здійснюється шляхом введення узгодженого контуру між прикладним рівнем і середовищем передавання, у межах якого пакетизація, FEC, інкапсуляція, шифрування, вибір маршруту та контроль метрик здійснюються як єдина послідовність операцій. Саме ця властивість робить архітектуру придатною не лише для лабораторного моделювання, а й для створення відтворюваного програмного прототипу, здатного працювати в контейнеризованому або віртуалізованому середовищі, а також у сценаріях гібридних захищених каналів у розподілених мережах.

Отже, загальна архітектура реалізації гібридної технології являє собою багаторівневу модульну систему, у якій прикладні дані перетворюються у керований захищений потік, проходять через контури FEC, оверлейного захисту та програмованої маршрутизації, піддаються впливу мережевого середовища, після чого відновлюються і доставляються у вигляді вихідних ADU. Її принципова відмінність полягає в тому, що завадостійке кодування, криптографічний оверлей і маршрутизація розглядаються як частини єдиного технологічного контуру з уніфікованими інтерфейсами керування й моніторингу. Саме така архітектура створює необхідний базис для подальшої програмної реалізації методу синтезу профілю гібридного каналу та методу адаптивного керування його параметрами.

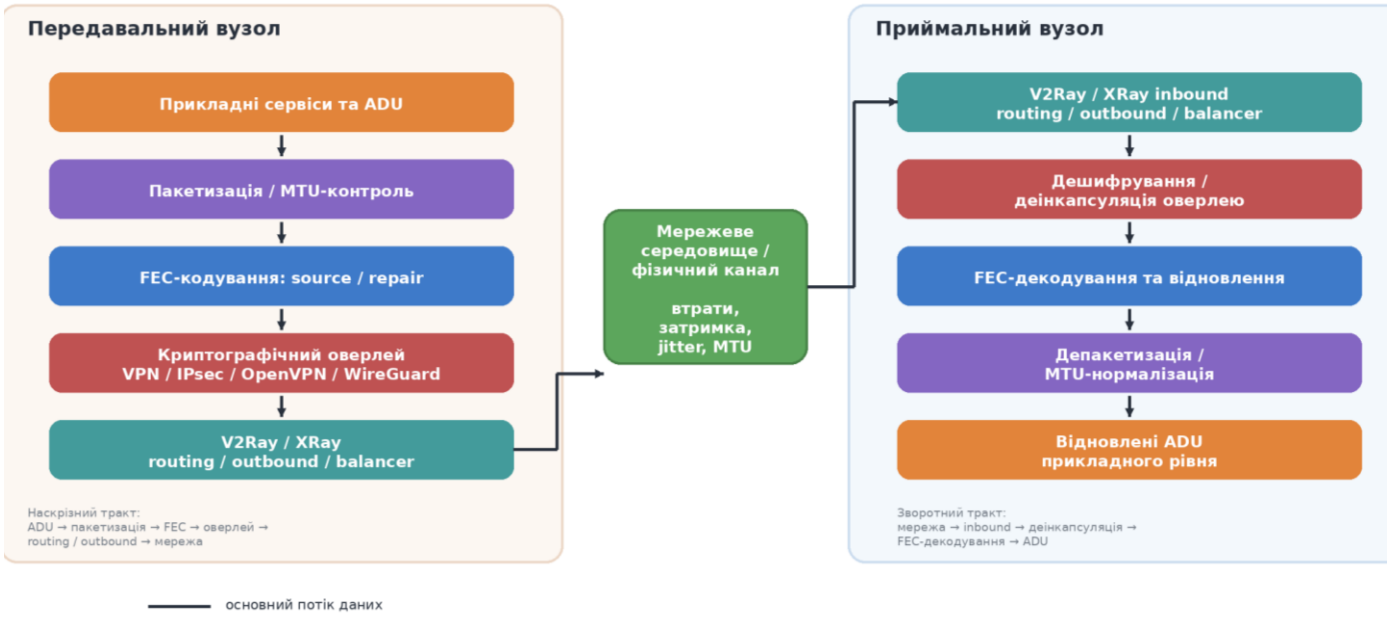


Рисунок 3.1 – Узагальнена блок-схема архітектури

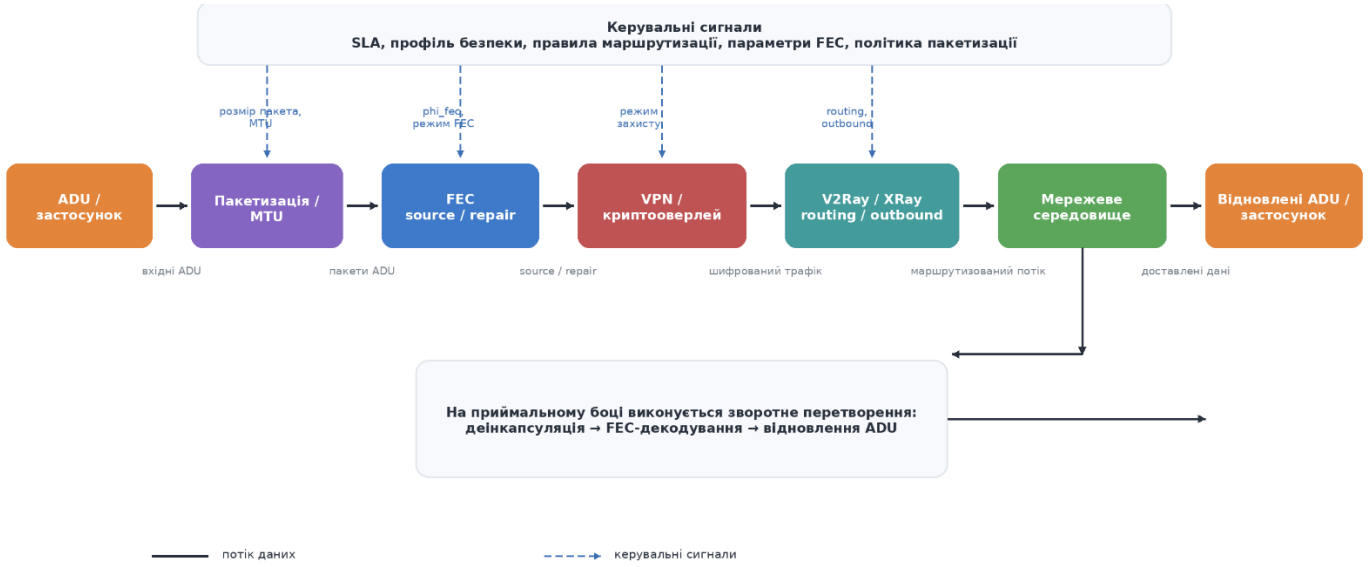


Рисунок 3.2 – Схема потоків даних і керувальних сигналів між рівнями

3.2 Програмна реалізація методу синтезу профілю гібридного каналу

У межах запропонованої гібридної інформаційної технології синтез профілю каналу розглядається як процедура вибору такої конфігурації параметрів передавання, яка за поточного стану середовища та заданих вимог забезпечує узгоджене досягнення потрібного рівня надійності, затримки, продуктивності, накладних витрат і криптографічної допустимості. Якщо в підрозділі 3.1 було

задано загальну архітектуру багаторівневої системи, склад її функціональних підсистем, а також точки спостереження, в яких накопичуються телеметричні дані, то в даному підрозділі ці положення конкретизуються у вигляді методу прийняття рішення щодо вибору профілю передавання. Його призначення полягає в тому, щоб перетворити множину можливих налаштувань FEC, оверлейного захисту, пакетизації та маршрутизації на одну узгоджену конфігурацію, придатну для практичного використання в межах сесії зв'язку.

Необхідність такого методу зумовлена тим, що жоден окремий механізм – ані завадостійке кодування, ані VPN-тунелювання, ані проксі-маршрутизація – не забезпечує оптимального результату сам по собі. Підвищення надлишковості покращує відновлюваність даних, але водночас збільшує транспортне навантаження. Використання більш захищеного оверлею підвищує криптографічну стійкість, але може погіршувати часові характеристики. Зміна маршруту або типу вихідного каналу здатна знизити втрати, однак іноді призводить до зростання latency або службового overhead. Отже, побудова гібридного каналу вимагає не локального, а саме багатокритеріального вибору, в якому всі основні параметри розглядаються спільно.

У програмній моделі профіль каналу формується як впорядкований набір параметрів, що охоплює FEC-режим, параметри надлишковості, правила пакетизації, тип криптографічного оверлею та логіку маршрутизації. Узагальнено це подається у вигляді

$$p = (\, p_{\mathrm{fec}}, \mathrm{p}_{\mathrm{ovl}}, r, \mathrm{L}_{\mathrm{adu}}), \tag{3.1}$$

Тут важливим є не стільки детальне перерахування всіх складових, скільки сам принцип: профіль розглядається як єдиний об'єкт синтезу, а не як набір незалежних налаштувань різних модулів. Саме така інтерпретація узгоджується з концептуальною моделлю 3.1, де FEC-модуль, оверлейний модуль, маршрутизувальний проксі та телеметричний контур функціонують як пов'язані елементи однієї системи.

Початковим етапом синтезу є формування множини кандидатних профілів. Вона створюється комбінуванням допустимих значень параметрів FEC, доступних оверлейних протоколів, варіантів outbound-маршрутизації та допустимих розмірів ADU. У загальному вигляді така множина подається як P_{cand}. На цьому етапі відсіюються явно непридатні конфігурації, для яких заздалегідь відомо, що вони суперечать технічним або безпековим вимогам. Таким чином, задача синтезу від самого початку не зводиться до повного перебору всіх теоретично можливих комбінацій, а обмежується лише практично допустимою областю рішень.

Особливе місце на етапі формування кандидатів займає перевірка обмежень, пов’язаних із пакетизацією та недопущенням фрагментації. З огляду на висновки другого розділу, а також на роль MTU-контролю в архітектурі 3.1, до множини кандидатів включаються лише ті профілі, для яких сумарний розмір сформованого пакета не перевищує допустиму межу шляху передавання. Це обмеження є принциповим, оскільки в гібридному каналі загальний розмір пакета визначається не лише довжиною корисних даних, а і FEC-надлишковістю, оверлейними заголовками та службовими полями маршрутизації. Відповідно, навіть ефективний з точки зору відновлення профіль не може вважатися допустимим, якщо його застосування систематично призводить до фрагментації або до зростання пов’язаних із нею втрат.

Після побудови множини кандидатів виконується їх оцінювання за системою метрик, обґрунтованих у другому розділі. На цьому етапі вже не вводяться нові критерії, а використовуються ті самі показники, що були прийняті як змістовні для оцінювання якості гібридної інформаційної технології. Для кожного профілю визначається очікувана імовірність доставки та відновлення ADU, оцінюється рівень затримки, обчислюються накладні витрати й ефективна швидкість прикладного передавання.

Принципово важливо, що в запропонованому методі ці метрики не аналізуються ізольовано. Окремий профіль може демонструвати високе значення Π_{e2e}, але виявлятися неприйнятним через завелику τ_{95}. Інший профіль може

забезпечувати добрий $\mathrm{G}_{\mathrm{app}}$, однак досягати цього за рахунок недостатньої стійкості або неприпустимого зростання Ω. Саме тому оцінювання виконується в межах інтегрованої цільової функції, яка дозволяє перейти від набору окремих показників до єдиної процедури ранжування. У найпростішому вигляді така функція може бути подана як

$$J(p) = w_1\big(1 - \Pi_{\mathrm{e2e}}(\mathrm{p})\big) + w_2 \frac{\tau_{95}(p)}{\tau_{95}^{max}} + w_3(\Omega(\mathrm{p}) - 1) - w_4 G_{\mathrm{app}}(p), \quad (3.2)$$

Ця функція використовується не як самодостатня математична конструкція, а як інструмент впорядкування допустимих профілів згідно з пріоритетами конкретного сценарію. Відповідно, зміна вагових коефіцієнтів дає змогу реалізувати різні режими синтезу: від консервативного, орієнтованого насамперед на надійність і безпеку, до продуктивного, у якому більша увага приділяється затримці та goodput.

Окремо слід підкреслити, що використання цільової функції не скасовує жорстких обмежень. Перед ранжуванням відсіюються профілі, які не досягають мінімально допустимого рівня доставки, порушують часові межі, виходять за межі дозволених накладних витрат або суперечать вимогам безпеки. Тому задача синтезу фактично зводиться до вибору найкращого елемента не з усієї множини P_{cand}, а лише з множини допустимих профілів P_{adm}. Оптимальний профіль каналу обирається з множини допустимих профілів P_{adm}, сформованої відповідно до обмежень з формули (2.39).

$$p^* = arg \min_{p \in P_{\mathrm{adm}}} J(p), \quad (3.3)$$

Саме така постановка є найбільш логічною для дисертаційної моделі, оскільки вона поєднує два рівні відбору: спочатку перевірку принципової допустимості, а вже потім – оптимізаційне порівняння всередині допустимої області.

Безпековий контур у цьому методі не винесено в окремий зовнішній етап, а інтегровано безпосередньо в процедуру синтезу. Для цього використовується модуль політики безпеки, який перевіряє відповідність профілю вимогам до криптографічних режимів, типів оверлею та заборонених поєднань механізмів. Такий підхід є методично важливим, оскільки не допускає ситуації, коли конфігурація визнається оптимальною лише з погляду продуктивності, але при цьому суперечить вимогам сучасної криптографічної практики. Отже, синтез профілю в запропонованій моделі відбувається лише в межах простору безпеково допустимих рішень, а не поверх нього.

Із програмної точки зору ця логіка реалізується як окремий керувальний модуль, пов’язаний із телеметричним контуром та менеджером сесії. Враховуючи модульну архітектуру, описану в 3.1, метод синтезу виконує роль зв’язувальної ланки між підсистемою спостереження, FEC-обробленням, оверлейним захистом і маршрутизувальним модулем. На практиці це означає, що результати вимірювання втрат, затримки, подій handshake/rekey, змін outbound-каналів та факту доставки ADU не лише накопичуються для подальшого аналізу, а і безпосередньо використовуються для побудови або перегляду профілю передавання. У цьому полягає одна з ключових відмінностей запропонованого підходу від статичних схем налаштування: профіль не задається один раз, а формується на основі поточного стану системи.

У реалізації метод доцільно подати через клас ProfileSynthesizer, який виконує три основні функції: генерування множини кандидатних профілів, їх оцінювання та вибір найкращого варіанта. Метод generateProfiles() формує множину кандидатів з урахуванням технічних і безпекових обмежень. Метод evaluateProfile(profile) обчислює для кожного кандидата вектор оцінок і значення цільової функції. Метод selectBest() виконує остаточний вибір конфігурації, яка найбільшою мірою відповідає поточному сценарію застосування. Така декомпозиція добре узгоджується з модульною структурою програмної

архітектури, описаною в 3.1, і водночас створює основу для подальшої адаптивної перебудови параметрів у наступних підрозділах.

З методичного погляду важливо й те, що синтез профілю може використовуватися у двох режимах. Перший режим відповідає початковому вибору конфігурації перед стартом сеансу. У цьому випадку метод працює з апріорними оцінками параметрів каналу та доступних ресурсів. Другий режим відповідає повторному синтезу в процесі роботи, коли телеметрія вказує на деградацію умов передавання або на зміну характеристик шляху. Саме такий підхід робить синтез профілю не разовою оптимізаційною процедурою, а елементом загального адаптивного контуру керування, який було концептуально закладено в попередньому підрозділі.

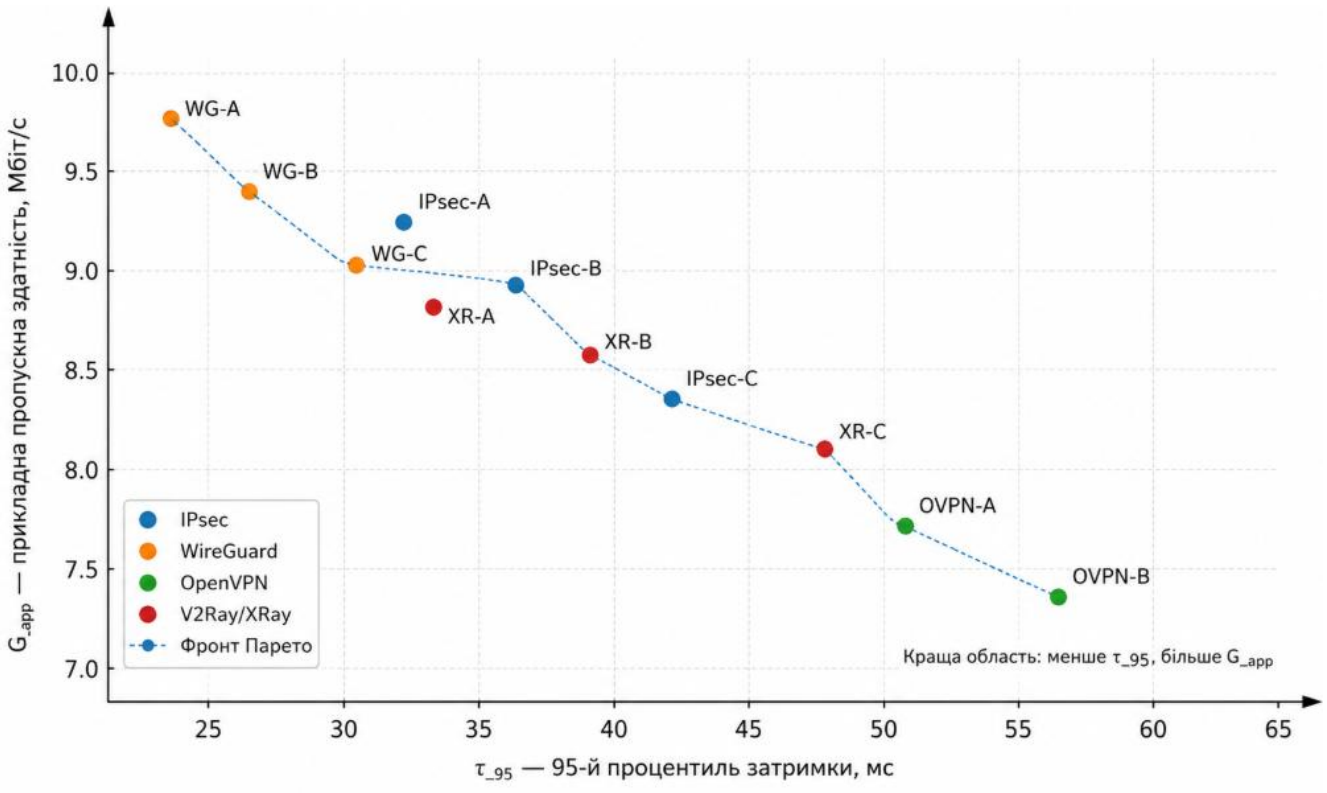


Рисунок 3.3 – Pareto-діаграма вибору профілю

3.3 Програмна реалізація адаптивного керування FEC та оверлеєм

Практична цінність запропонованого методу визначається не лише тим, наскільки коректно він формалізований на рівні моделей і метрик, а й тим, яким чином він може бути реалізований у програмному середовищі без порушення цілісності мережевого стеку та без втрати керованості всієї системи. Саме тому метод адаптивного керування параметрами FEC та оверлею доцільно розглядати не як окремий алгоритм у вузькому розумінні, а як координаційний програмний механізм, вбудований у життєвий цикл сеансу передавання даних. Його призначення полягає в тому, щоб у процесі роботи системи безперервно співвідносити поточний стан каналу, параметри криптографічного тунелю, доступні ресурси вузла та вимоги до якості сервісу, після чого приймати рішення про зміну робочого профілю без повної зупинки передавання.

У програмній архітектурі такий метод доцільно реалізовувати у вигляді окремого керувального модуля, який взаємодіє з підсистемами кодування, тунелювання, пакетизації та збору телеметрії. Центральним елементом виступає клас AdaptiveController, який не виконує кодування чи шифрування безпосередньо, а координує дії інших модулів, приймаючи рішення на підставі поточного стану середовища. Такий підхід є принципово важливим, оскільки дозволяє розмежувати функції спостереження, аналізу, вибору рішення та його застосування. У результаті система набуває модульності: FEC-підсистема відповідає за надлишковість і відновлення, VPN/оверлей – за конфіденційність і спосіб транспортування, а адаптивний контролер – за узгодження цих двох площин у межах єдиної політики.

Початковою фазою роботи контролера є отримання й агрегація телеметрії. Для цього використовується модуль збору показників, який у програмній реалізації може бути представлений класом MetricsCollector. Його завдання полягає не лише в накопиченні сирих значень, а у формуванні цілісного знімка стану каналу за певне часове вікно. До такого знімка входять показники втрат пакетів, затримки, її квантильні оцінки, goodput, частота повторних передач, ознаки фрагментації, а також індикатори навантаження на процесор і пам’ять вузла. Принципово важливо,

що рішення не повинні прийматися за одиничним сплеском або випадковою аномалією. Тому телеметрія спершу проходить етап згладжування, фільтрації та короткострокової агрегації. Це дозволяє відокремити нестійкі коливання від реального погіршення умов передавання й уникнути ситуації, коли система починає надто часто перебудовувати власну конфігурацію.

Після отримання узагальненого стану середовища запускається етап аналітичної оцінки. На цьому етапі контролер не просто порівнює поточні значення з наперед заданими порогами, а інтерпретує їх у контексті обраного профілю сеансу. Один і той самий рівень втрат може мати різне значення для різних режимів роботи: для коротких інтерактивних сесій критичним буде зростання затримки, тоді як для потокового або пакетного передавання більш істотним стане падіння goodput чи зростання частки невідновлених ADU. Саме тому модуль PolicyEngine доцільно реалізувати не як жорсткий набір if-else правил, а як механізм профільного узгодження, де кожне рішення приймається з урахуванням пріоритетів поточного сценарію. У найпростішому випадку це може бути система ваг і порогів, а в розширеному – багатокритеріальний вибір допустимого профілю з множини наперед підготовлених конфігурацій.

Окремий контур керування стосується параметрів FEC. У програмному сенсі це означає, що контролер повинен мати можливість змінювати рівень надлишковості без перебудови всієї системи з нуля. Якщо телеметрія вказує на стабільне зростання втрат або на появу пачкових стирань, контролер може збільшувати φ_{fec}, коригувати W_{fec} або змінювати режим роботи між більш простим блоковим підходом і більш гнучким віконним підходом. Таке рішення має прийматися поступово, невеликими кроками, із перевіркою ефекту після кожної зміни. Інакше надмірність почне зростати швидше, ніж цього вимагає канал, що призведе до зайвих накладних витрат і погіршення корисної пропускної здатності. У програмній реалізації це означає, що метод adjustFec() повинен не просто “підняти резерв”, а змінити активний FEC-профіль, передати оновлені параметри модулю кодування, зафіксувати момент зміни у журналі подій та тимчасово

перевести систему у режим спостереження, коли нові рішення не приймаються доти, доки не стане зрозумілим ефект від щойно застосованої конфігурації.

Не менш важливим є керування пакетизацією. На практиці саме невдале співвідношення між розміром корисного навантаження, заголовками тунелю та допустимим MTU часто створює додаткові проблеми, які зовні виглядають як погіршення якості каналу, хоча насправді їх джерелом є фрагментація. З цієї причини адаптивний контролер повинен відстежувати не лише втрати, а й непрямі ознаки того, що частина трафіку розбивається на фрагменти або не проходить через окремі ділянки шляху. У програмній реалізації для цього доцільно передбачити окремий керувальний компонент, пов’язаний з effectiveMtu() та логікою MTU-clipping. Якщо виявляється нестабільність проходження пакетів, контролер зменшує L_adu або коригує верхню межу корисного навантаження для поточного тунелю. Така зміна має особливе значення у гібридній системі, тому що надлишковість FEC і параметри тунелювання сумарно формують реальний розмір пакета, а отже, без урахування цього чинника навіть добре підібрана схема кодування може працювати неефективно.

Другий великий контур адаптації пов’язаний з оверлеєм. Якщо FEC компенсує втрати та підвищує ймовірність відновлення даних, то оверлей визначає, яким маршрутом, через який транспорт і в якому форматі ці дані будуть проходити мережею. У випадку V2Ray/XRay програмна реалізація отримує додаткову гнучкість, оскільки один і той самий сеанс може мати кілька можливих outbound-профілів, що відрізняються транспортом, маскуванням, параметрами маршрутизації та стійкістю до блокування. Тому метод adjustOverlay() повинен виконувати не механічне перемикання між тегами, а виважений вибір нового шляху за умов, коли поточний режим перестає відповідати вимогам до затримки, стабільності або надійності доставки. У цьому випадку контролер порівнює активний маршрут з альтернативними профілями, оцінює вартість переходу та приймає рішення лише тоді, коли очікувана користь перевищує ризики, пов’язані з перебудовою тунелю.

Особливістю адаптації оверлею є те, що вона завжди дорожча за локальну перебудову FEC. Зміна параметрів кодування може бути майже прозорою для користувача, тоді як зміна оверлейного маршруту, транспортного режиму або outbound-профілю нерідко супроводжується короткочасною деградацією, повторною ініціалізацією службових структур або накопиченням буферів. Саме тому в програмній моделі доцільно використовувати ієрархію реакцій: спочатку система намагається виправити ситуацію менш інвазивними засобами – підлаштуванням FEC і пакетизації, і лише в разі недостатності цього переходить до зміни оверлею. Така послідовність має не лише практичне, а й методичне обґрунтування: вона дозволяє зберегти стабільність сеансу і водночас уникнути зайвих перепідключень, які самі по собі можуть погіршувати спостережувані метрики.

Окремої уваги потребує обробка службових подій криптографічного тунелю, насамперед handshake та rekey. У реальних системах саме ці події часто стають джерелом короткочасних, але відчутних змін затримки та пропускної здатності. Якщо адаптивний контролер не враховує такого типу подій, він може хибно інтерпретувати службовий сплеск затримки як деградацію каналу та почати непотрібну перебудову профілю. Щоб цього уникнути, у програмній реалізації доцільно передбачити спеціальний обробник handleRekeyEvent(), який переводить систему у режим контекстного спостереження. У цьому режимі зміни метрик аналізуються з поправкою на те, що відбувається службова криптографічна операція. За потреби контролер може короткочасно збільшити запас відновлювальної надлишковості, посилити буферування або тимчасово знизити інтенсивність нових керувальних рішень. Після завершення handshake система повертається до стандартного режиму оцінювання.

Ще один важливий аспект реалізації пов’язаний із ресурсними обмеженнями вузла. Гібридна інформаційна технологія одночасно використовує криптографічні операції, механізми кодування, буферизацію, моніторинг та логіку прийняття рішень. Усе це створює навантаження на процесор, пам’ять і мережевий стек. Якщо

контролер орієнтуватиметься лише на показники каналу, але ігноруватиме стан самого вузла, то в окремих ситуаціях він може “покращувати” надійність ціною перевантаження системи. Саме тому програмна реалізація має включати ресурсний зворотний зв’язок. Якщо навантаження на CPU зростає до меж, що загрожують стабільності роботи, контролер не повинен безумовно нарощувати надлишковість чи запускати важкі сценарії зміни тунелю. Натомість він має обирати серед допустимих конфігурацій ті, що зберігають баланс між стійкістю передавання та обчислювальною вартістю. При цьому всі рішення повинні залишатися в межах політик безпеки, тобто спрощення обробки не може порушувати базові вимоги до криптографічного захисту.

З програмної точки зору важливо також забезпечити безпечне застосування нових параметрів. Недостатньо лише обчислити кращий профіль – необхідно коректно ввести його в дію. Для цього доцільно використовувати поетапну процедуру: підготовка нового профілю, перевірка його сумісності з поточним станом сеансу, застосування змін у визначеному порядку, фіксація контрольної точки та спостереження за результатом. Наприклад, перед зміною outbound-профілю спершу потрібно перевірити доступність нового каналу, потім скоригувати MTU-обмеження, після цього активувати новий маршрут і лише далі адаптувати FEC під оновлені умови. Така послідовність зменшує ризик того, що система одночасно змінить кілька критичних параметрів і втратить керованість. У разі невдалого застосування профілю повинен існувати механізм rollback, який дозволяє повернутися до останньої стабільної конфігурації.

Для запобігання осциляціям доцільно вводити гістерезис, мінімальний інтервал між перебудовами та поняття “зони нечутливості”. Це означає, що не кожне незначне відхилення від цільових метрик повинно викликати реакцію. Якщо, наприклад, затримка зросла незначно і не виходить за межі допустимого діапазону, система має зберігати поточний профіль. Лише стійке та статистично підтверджене погіршення повинно призводити до зміни параметрів. Таке рішення має особливе значення для мереж із природною варіативністю, де мікроколивання є нормою. У

програмній реалізації це можна оформити через cooldown-інтервали, фіксацію часу останнього переключення та обов’язкове підтвердження тенденції на кількох послідовних вікнах спостереження.

Узагальнюючи, програмна реалізація методу адаптивного керування параметрами FEC та оверлею являє собою не ізольований алгоритм, а багатокомпонентний керувальний контур, що поєднує спостереження, інтерпретацію, вибір рішення та його контрольоване застосування. Саме така реалізація забезпечує практичну придатність запропонованої інформаційної технології в динамічних умовах мережевого середовища. Її перевага полягає в тому, що система не обмежується одноразовим синтезом профілю до початку сеансу, а зберігає здатність коригувати свої параметри в процесі роботи, не руйнуючи при цьому архітектурної узгодженості між рівнем кодування, рівнем захищеного тунелю та рівнем прикладного передавання даних.

Рисунок 3.4 – Послідовність зміни профілю сеансу при погіршенні стану каналу: збір метрик, вибір рішення, коригування FEC, MTU та outbound-маршруту

3.4 Реалізація модулів завадостійкого кодування та відновлення даних

Практична придатність запропонованої гібридної інформаційної технології значною мірою визначається тим, наскільки послідовно реалізовано модулі завадостійкого кодування та відновлення даних у складі загальної програмної архітектури. Якщо в попередніх підрозділах було обґрунтовано вибір моделей, параметрів і принципів поєднання FEC із криптографічним оверлеєм, то на цьому

етапі основна увага зосереджується вже на структурі програмних компонентів, їхній взаємодії та порядку проходження даних через модулі ЗС кодування і декодування. Такий перехід від моделі до реалізації є принциповим, оскільки саме в програмному модулі абстрактні параметри надлишковості, довжини блоку, режиму роботи вікна та профілю коду набувають конкретної функціональної форми.

Програмна реалізація доцільно організовується за модульним принципом, коли підсистема FEC виділяється в окремий функціональний контур із чітко визначеними інтерфейсами входу, виходу та керування. Такий підхід узгоджується з уже закладеною у файлі логікою пакетної структури, де модулі ЗСК зосереджуються в зоні ua.securehybrid.fec, а взаємодія з політикою керування, каналом, VPN-рівнем і телеметрією винесена в окремі пакети. Це дозволяє уникнути надмірного зв’язування компонентів між собою та забезпечує замінність конкретної сім’ї кодів без перебудови всієї системи. У такій архітектурі модуль ЗСК не повинен залежати від конкретного VPN-протоколу, а модуль декодування не повинен бути жорстко прив’язаний до певної транспортної реалізації. Відповідно, FEC-контур виступає як самостійний обчислювальний шар, що працює з підготовленими до передавання кадрами та повертає або успішно відновлені ADU, або ознаки неможливості відновлення.

Базою такої реалізації є уніфікований програмний інтерфейс для ЗС кодування та декодування. Його доцільно подавати через абстракції IBlockEncoder та IBlockDecoder, які визначають єдиний API для роботи незалежно від того, яка саме сім’я кодів використовується в конкретному профілі. Така уніфікація має істотне значення, оскільки в межах однієї інформаційної технології можуть застосовуватися різні варіанти реалізації завадостійких кодів: блокове кодування, укорочені схеми, пунктурування, а в окремих сценаріях і віконні механізми відновлення. Єдиний інтерфейс дозволяє зберегти сталість зовнішньої логіки, тоді як внутрішня реалізація коду може змінюватися залежно від вимог сеансу. У програмному сенсі це означає, що вищий рівень працює не з конкретним кодом

Хеммінга, Reed-Solomon чи LDPC, а з абстрактною операцією формування FEC-кадру та подальшого відновлення корисного навантаження. Саме через це підсистема FEC інтегрується в архітектуру як сервіс, а не як жорстко вбудований фрагмент окремого алгоритму.

На передавальному боці основною функцією модуля є перетворення вхідної послідовності ADU у структуру, придатну для стійкого проходження через канал із втратами. Цей процес не зводиться лише до механічного додавання надлишкових пакетів. Спочатку виконується нормалізація даних: корисне навантаження приводиться до формату, сумісного з поточним профілем ЗСК, з урахуванням обмежень MTU, обраної схеми пакетизації та службових полів. Далі формується група source-пакетів, яка становить базову множину для подальшого породження repair-пакетів. На цьому етапі особливо важливо зберегти стабільне відображення між порядком вихідних ADU, їхніми локальними ідентифікаторами та позиціями у кодувальній структурі. Без цього приймальна сторона не зможе коректно визначити, які саме елементи були втрачені й які позиції мають бути відновлені.

Після формування вихідної групи активується власне ЗСК механізм. У програмному відношенні він реалізується у вигляді окремого класу, умовно позначеного як FecEncoder або FecEngine, який працює з поточним профілем FEC та формує repair-потік у тому обсязі, який визначено параметрами сеансу. Важливо, що цей модуль не повинен зберігати зайву прив’язку до мережевої підсистеми. Його завдання полягає не у відправленні пакетів, а у породженні стійкої надлишкової структури, де кожний вихідний кадр містить як корисне навантаження, так і достатню службову інформацію для подальшого складання кодувальної групи на приймальному боці. Саме тому до складу FEC-кадру доцільно включати ідентифікатор сесії, номер кодувальної групи, локальний номер елемента в межах групи, тип пакета та ознаки профілю, за яким було здійснене ЗСК. Така побудова суттєво спрощує відновлення даних у разі перестановки пакетів, часткових втрат або повторного надходження окремих кадрів.

У реалізації необхідно передбачити щонайменше два режими роботи модуля ЗСК. Перший – блоковий, коли надлишковість формується для завершеної групи з наперед визначеною кількістю source-елементів. Саме цей режим є найбільш прозорим для експериментального аналізу, оскільки він дозволяє чітко пов’язати параметри профілю з результативністю відновлення. Другий режим – потоковий або віконний, коли ЗСК виконується не для жорстко ізольованого блоку, а для рухомого вікна пакетів. Такий підхід є складнішим у реалізації, однак краще відповідає динамічним мережевим сценаріям, де неприпустимо очікувати повного накопичення блоку перед передаванням. У програмному модулі обидва режими доцільно підтримувати в межах спільного інтерфейсу, а різницю між ними приховувати на рівні конкретної реалізації профілю. Завдяки цьому зовнішня логіка оркестрації не змінюється, тоді як внутрішній спосіб побудови repair-потоку вибирається залежно від характеристик каналу та вимог до затримки.

Принциповим для гібридної інформаційної технології є те, що ЗСК застосовується не до відкритого прикладного тексту, а до вже підготовлених захищених кадрів. У поточній структурі файлу ця логіка вже зафіксована: FEC накладається на послідовність зашифрованих та автентифікованих пакетів, а відновлення виконується на рівні цілих пакетів, не втручаючись у криптографічну цілісність AEAD. Це має важливе методичне значення. По-перше, така побудова не порушує межу відповідальності між криптографічним і корекційним рівнями. По-друге, вона усуває ризик того, що декодер працюватиме з частково пошкодженими криптографічними блоками, які все одно не можуть бути коректно використані після втрати автентичності. По-третє, відновлення на рівні цілих пакетів добре узгоджується з моделлю packet erasure, на якій базується значна частина FEC-підходів у мережевих системах.

На приймальному боці основним елементом виступає модуль FecDecoder, який приймає набір отриманих кадрів, реконструює структуру відповідної кодувальної групи та визначає, чи достатньо наявної інформації для відновлення втрачених елементів. На відміну від передавального модуля, декодер працює в

умовах неповноти та невизначеності. Він може отримати не всі source-пакети, частину repair-пакетів, а також зіткнутися з перестановкою порядку надходження. Тому його першим завданням стає не відразу відновлення, а впорядкування й верифікація вхідної множини. Для цього в структурі декодера повинні підтримуватися буфери збору, таблиці відповідності ідентифікаторів сесії та групи, а також механізми контролю тайм-аутів. Якщо набір кадрів виявляється достатнім для декодування, запускається обчислювальна процедура відновлення; якщо ні, група утримується в буфері до досягнення граничного часу очікування або до надходження нових repair-елементів.

Успішне відновлення можливе лише за умови, що декодер не змішує між собою різні логічні групи. Саме тому велике значення мають службові поля FEC-заголовка, які не несуть прикладного змісту, але забезпечують цілісність процедури реконструкції. Після того як декодер визначив склад групи, виконується побудова локальної матриці або іншої внутрішньої структури, потрібної для конкретної схеми ЗСК, після чого обчислюються відсутні елементи. У випадку блокових кодів це може бути розв’язання системи співвідношень над скінченним полем, у випадку ітеративних кодів – послідовна процедура уточнення оцінок. Однак незалежно від конкретного алгоритму зовнішній результат повинен бути уніфікований: декодер повертає відновлене корисне навантаження, ознаку успішності операції та статистичні характеристики процесу. Саме така модель вже передбачена у твоїй схемі інтерфейсів, де decode(frame) повертає не лише payload, а й стан ok та блок stats.

Наявність статистичного результату декодування є не другорядною, а концептуально важливою частиною реалізації. Йдеться не лише про внутрішні лічильники помилок. Дані про кількість успішно відновлених елементів, число ітерацій, частку невідновлених груп, частоту тайм-аутів і співвідношення source/repair-пакетів становлять основу для подальшого керування профілем сеансу. Інакше кажучи, модуль FEC має не тільки виконувати корекцію, а й продукувати інформацію про власну результативність. Через це він тісно

пов’язується з підсистемою телеметрії. Після завершення кожного циклу ЗС кодування або декодування відповідні події передаються в MetricsCollector, який агрегує їх у вікна спостереження та формує узагальнений знімок стану системи. У перспективі саме на основі цих знімків PolicyEngine або адаптивний контролер приймають рішення щодо зміни рівня надлишковості, режиму вікна чи допустимого розміру корисного навантаження.

Значну роль у практичній реалізації відіграє обробка граничних випадків. У реальному мережевому середовищі далеко не кожна втрата є ізольованою, а надходження кадрів не гарантує ані їхньої повноти, ані правильного порядку. З цієї причини модулі кодування та відновлення повинні підтримувати механізми повторного впорядкування, контроль дублювання, відбракування прострочених груп та безпечне завершення декодування у разі недостатності інформації. Ігнорування таких деталей призвело б до того, що реалізація залишалася б працездатною лише в лабораторному середовищі, але втрачала б стійкість при реальних мережевих аномаліях. Саме тому в декодері необхідно передбачити окрему логіку життєвого циклу кодувальної групи: створення контексту, накопичення елементів, спроба відновлення, передавання результату нагору або закриття контексту з фіксацією невдачі.

Окремо слід підкреслити роль канального емулятора в перевірці працездатності FEC-модулів. У поточній архітектурі вже передбачено інтерфейс IChannelModel, який повертає або модифікований кадр, або ознаку стирання. Це дозволяє відділити власне корекційну логіку від конкретного способу ін’єкції завад та моделювати різні типи деградації каналу без змін у FEC-модулі. Така ізоляція є надзвичайно корисною в науковому та експериментальному сенсі. Вона дає змогу перевіряти поведінку одного й того ж механізму ЗСК за різних профілів втрат, бурстів і шумів, зберігаючи тотожну логіку верхнього рівня. У результаті стає можливим порівнювати не лише ефективність окремих кодів, а й стійкість усієї підсистеми до різних класів порушень у мережі.

З точки зору інтеграції з рештою системи модулі ЗСК та відновлення не повинні працювати ізольовано. На передавальному боці вони взаємодіють із підсистемою підняття тунелю та оцінки ефективного MTU, щоб розмір кодувальної групи та службового заголовка не призводив до фрагментації. На приймальному боці вони повинні бути узгоджені з логікою прийому з VPN-адаптера, який подає вже отримані тунельовані кадри у відповідний буфер обробки. Між цими рівнями має існувати не пряме жорстке злиття, а контрактна взаємодія через інтерфейси. Саме така побудова забезпечує масштабованість архітектури: заміна реалізації WireGuard на IPsec або OpenVPN не потребує переписування FEC-декодера, а зміна сім'ї коду не змінює логіку тунелювання. Усе це підтримує ключову для дисертації ідею про багаторівневу, але узгоджену інтеграцію різних захисних механізмів у межах однієї інформаційної технології.

У програмній реалізації доцільно також розділяти "швидкий" і "повільний" контур роботи FEC-модулів. До швидкого контуру належать власне операції ЗСК, маркування кадрів, буферизація та відновлення в межах поточного сеансу. До повільного – зміна профілю, переналаштування параметрів надлишковості, перемикання між блоковим і віконним режимом, а також узгодження нового FEC-профілю з каналом і оверлеєм. Таке розмежування дозволяє не змішувати обчислювальні процедури реального часу з процедурою керування політикою. Практично це означає, що модуль FecEncoder не приймає стратегічних рішень самостійно: він виконує профіль, отриманий від PolicyEngine або адаптивного контролера. Аналогічно декодер не змінює параметри системи напряму, а лише повідомляє про результативність своєї роботи через статистику та події. Саме це розмежування робить архітектуру прозорою, передбачуваною та придатною до подальшого масштабування.

Таким чином, реалізація модулів завадостійкого кодування та відновлення даних у межах запропонованої інформаційної технології має розглядатися як самостійний програмний контур із чітко визначеними функціями підготовки кадрів, породження надлишковості, буферизації, реконструкції втрачених

елементів та формування телеметрії. Важливою перевагою такого підходу є його сумісність із модульною архітектурою всієї системи та відсутність жорсткої залежності від конкретного VPN-протоколу або окремої сім'ї кодів. Саме це забезпечує можливість поєднати в одній реалізації різні профілі корекційного захисту, адаптувати їх до стану каналу та зберегти керованість процесу передавання в умовах втрат, бурстових завад і обмежень мережевого середовища.

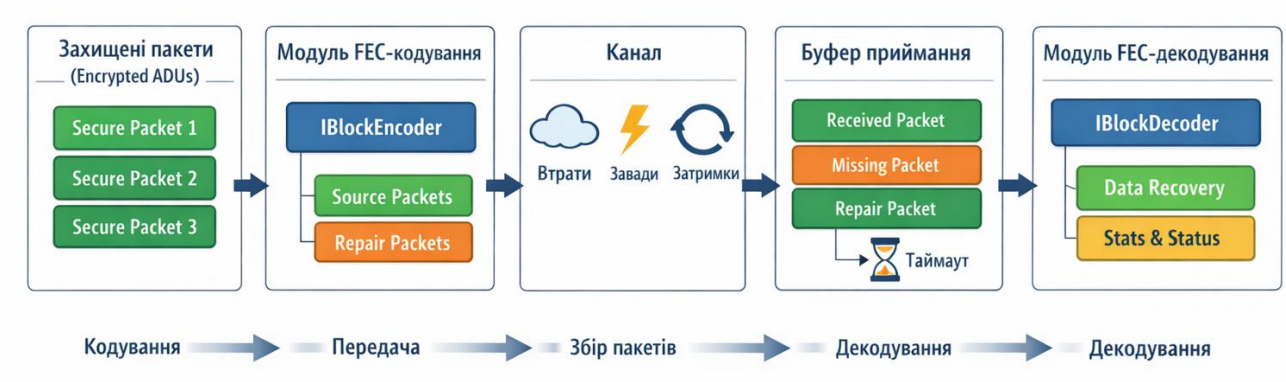


Рисунок 3.5 – Послідовність проходження даних через модулі FEC-кодування, канал, буфер приймання та FEC-декодування

Рисунок 3.6 – Послідовність проходження даних через модулі FEC-кодування, канал, буфер приймання та FEC-декодування

3.5 Реалізація модулів VPN, V2Ray/XRay та криптографічного захисту

Програмна реалізація криптографічного захисту та тунелювання в межах гібридної інформаційної технології організовується як окремий функціональний контур, який відповідає за встановлення захищеної сесії, шифрування і дешифрування пакетів, маршрутизацію трафіку через оверлей та підтримання актуального стану криптографічних параметрів. На відміну від FEC-модулів, що працюють із надлишковістю та відновленням даних, VPN-модулі забезпечують конфіденційність, цілісність і автентичність передавання [66]. Їх доцільно реалізовувати у вигляді окремих адаптерів із єдиним зовнішнім інтерфейсом, що дозволяє змінювати конкретний механізм тунелювання без перебудови верхнього рівня системи. Такий підхід відповідає модульній структурі прототипу та спрощує інтеграцію WireGuard, IPsec, OpenVPN і XRay у єдину систему керування.

Модуль IpsecModule реалізує функції побудови захищеного каналу на основі Security Association. На етапі ініціалізації він виконує створення та узгодження параметрів SA, після чого забезпечує інкапсуляцію, шифрування й перевірку цілісності пакетів у режимі AH/ESP. У межах програмної реалізації доцільно виділити методи initSa(), ikeInit(), ikeAuth(), encrypt(packet) і decrypt(packet). Перші два відповідають за запуск процедури узгодження ключів і параметрів сеансу, а два останні – за безпосередню обробку трафіку. Такий поділ дозволяє чітко

відокремити життєвий цикл тунелю від обробки корисних даних. На практиці інтеграція цього модуля може виконуватися через strongSwan/swanctl, що узгоджується із загальною адаптерною моделлю системи.

З метою узгодження розділу з обраними у підрозділі 2.2 метриками доцільно ввести окрему часову характеристику встановлення захищеної асоціації τ_{SA}, під якою розуміється інтервал від моменту ініціації процедури узгодження параметрів захищеного сеансу до моменту переходу тунелю в стан готовності до передавання корисних даних. Для IPsec значення τ_{SA} охоплює виконання етапів initSa(), ikeInit() та ikeAuth(), для OpenVPN – виконання startTlsHandshake(), а для WireGuard – завершення початкового handshake. В архітектурі прототипу цю величину доцільно фіксувати телеметричним модулем окремо від τ_{95}, оскільки τ_{SA} характеризує не затримку вже встановленого каналу, а часові витрати на переведення системи у стан захищеної готовності. Значення τ_{SA} повинно використовуватися разом із τ_{95}, G_{app}, $П_{e2e}$ та Ω_{tot} при порівнянні різних типів захищеного оверлею, оскільки надмірно велика тривалість встановлення SA знижує оперативність початку сесії та може погіршувати інтегральну ефективність гібридної інформаційної технології.

Модуль OpenVpnModule призначений для реалізації захищеного тунелю на основі TLS. Його ключова особливість полягає в тому, що криптографічний контур і транспортна логіка тут тісно пов’язані з TLS-сесією, тому основну увагу слід приділити процедурі встановлення каналу та подальшому керуванню параметрами шифрування. У складі модуля доцільно виділити метод startTlsHandshake(), який виконує ініціалізацію захищеної сесії, а також методи encrypt(packet) і decrypt(packet) для обробки даних після встановлення тунелю. Для практичної реалізації доцільно використовувати OpenSSL або сумісну бібліотеку, що дозволяє не дублювати низькорівневі криптографічні процедури й зосередити увагу на інтеграції модуля з рештою системи. У прототипі зовнішнє керування таким модулем може здійснюватися через management-сокет OpenVPN.

Модуль WireGuardModule реалізує більш компактну модель захищеного тунелю. Його структура є простішою, оскільки значна частина складності винесена

у фіксований набір криптографічних примітивів та короткий handshake. У програмній реалізації доцільно виділити метод handshake(), який виконує узгодження ключів, метод wrap(packet) для шифрування вихідного пакета та метод unwrap(packet) для його розкриття на приймальному боці. Додатково потрібна функція queuePacketUntilHandshake(), що тимчасово буферизує трафік до завершення первинного встановлення захищеного стану. Така логіка особливо важлива для коротких сесій або при повторному перевстановленні ключів. У межах прототипу модуль може взаємодіяти із зовнішнім інструментом wg/wg-quick або з API-обгорткою, якщо потрібно забезпечити програмне перемикання профілів.

Окреме місце посідає XRayModule, який виконує не стільки криптографічну, скільки оверлейно-маршрутизувальну функцію. Його завдання полягає у прийманні локального трафіку від застосунку, передачі його на обраний транспорт і перемиканні між outbound-профілями залежно від активної політики. У структурі цього модуля доцільно виділити три основні частини: inbound, який приймає локальний трафік; router, який визначає потрібний маршрут; outbound(tag), який забезпечує фактичне передавання через відповідний транспортний профіль. Для адаптивної системи особливо важливим є метод changeOutbound(tag), оскільки саме він дозволяє змінювати активний маршрут без зупинки всього сеансу. Таким чином, XRayModule виступає точкою узгодження між локальною сесією, політикою маршрутизації та зовнішнім мережевим середовищем.

Для уніфікації криптографічних операцій доцільно ввести абстрактний інтерфейс CryptoEngine, який надає єдині методи encrypt(), decrypt(), sign(), verify() або їх мінімально необхідний піднабір залежно від обраного протоколу. Конкретні реалізації цього інтерфейсу можуть використовувати AES-GCM, ChaCha20-Poly1305, HMAC, RSA або ECC, однак для верхнього рівня вони мають виглядати однаково. Завдяки цьому класи IpsecModule, OpenVpnModule і WireGuardModule не дублюють криптографічну логіку, а звертаються до єдиного шару обробки. Така централізація спрощує контроль версій бібліотек, аудит безпеки та подальшу зміну криптографічного профілю без переписування модулів тунелювання.

Стан захищеної сесії повинен зберігатися в окремому класі SecurityAssociation. У ньому доцільно розміщувати ідентифікатор сесії, параметри ключів, nonce, SPI, часові мітки, режими шифрування та службові ознаки стану тунелю [67]. Це дозволяє відокремити короткочасні криптографічні дані від логіки самих модулів і спростити процедури rekey, перевстановлення тунелю та коректного завершення сесії. Після завершення роботи відповідні об’єкти повинні бути знищені або очищені, щоб уникнути повторного використання службових параметрів і зменшити ризик витоку чутливих даних.

У результаті програмна реалізація модулів VPN, V2Ray/XRay та криптографічного захисту формує окремий, але тісно інтегрований рівень гібридної інформаційної технології. Його функція полягає не лише у шифруванні пакетів, а й у підтриманні захищеного стану сесії, керуванні маршрутами, обліку службових параметрів тунелю та узгодженні роботи з підсистемами пакетизації, FEC і адаптивного керування. Саме така побудова дозволяє поєднати в межах однієї архітектури кілька VPN-підходів і забезпечити їхню спільну роботу з механізмами завадостійкого кодування та динамічної адаптації.

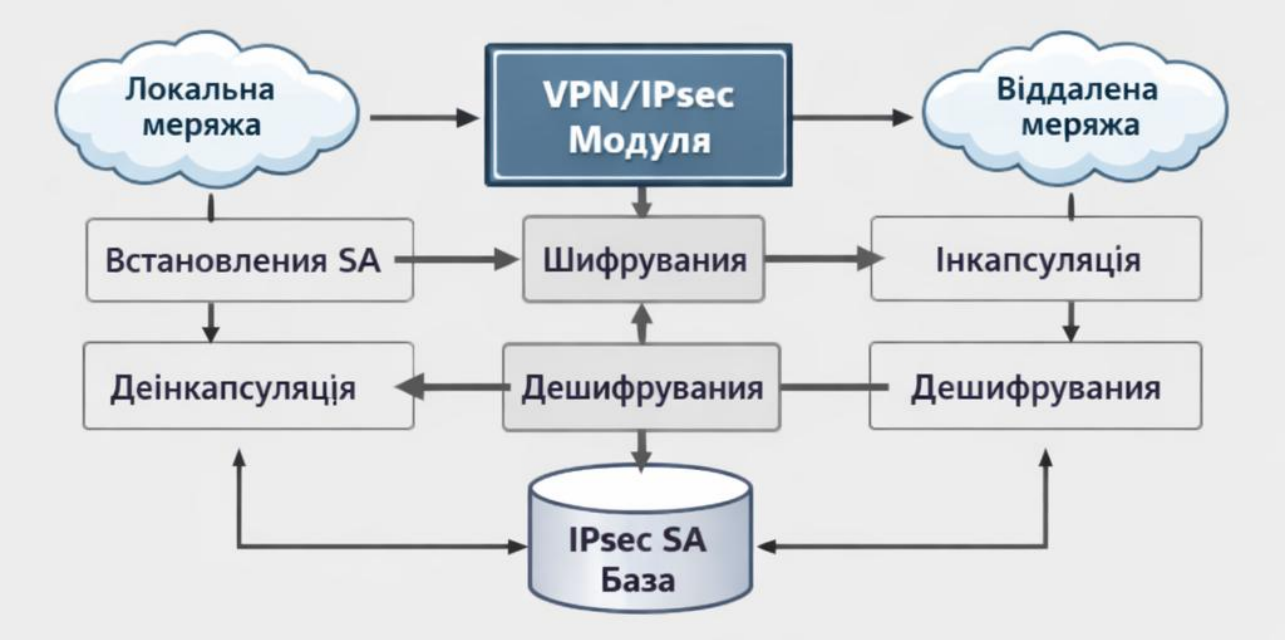


Рисунок 3.7 – Структурна схема модуля VPN/IPsec

Архітектурні принципи побудови IPsec-модулів відповідають рекомендаціям RFC 4301 [68]. Узгодження параметрів SA та обмін ключами реалізуються відповідно до механізмів IKEv2 [69].

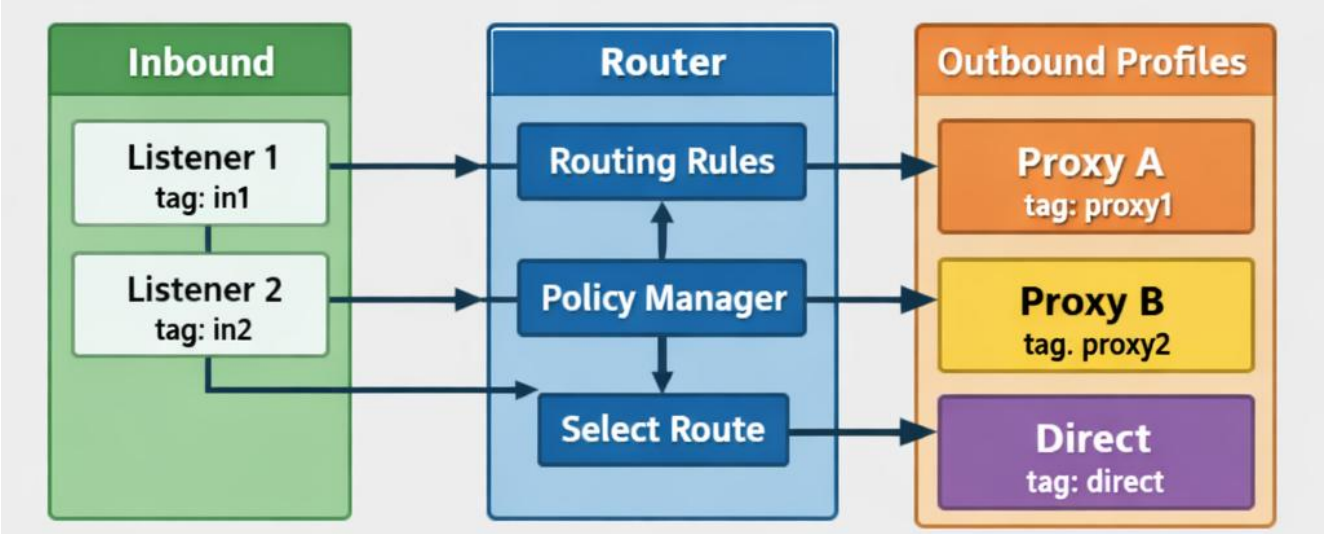


Рисунок 3.8 – Структурна схема модуля XRay із компонентами inbound, router та outbound-профілями з тегами

Архітектура XRay та принципи організації inbound/outbound-маршрутизації відповідають офіційній документації проєкту V2Ray/Xray [70].

3.6 Інтеграція модулів, мережа та обчислювальні ресурси

Інтеграція розроблених модулів виконується у межах єдиної програмної системи, де підсистеми FEC, VPN, оверлейної маршрутизації, моделювання каналу та збору телеметрії працюють як узгоджені компоненти з чітко визначеними інтерфейсами взаємодії [71]. Такий підхід відповідає концепції virtualized network functions та cloud-native VPN, запропонованій ETSI [72]. Базовими точками інтеграції є модулі IBlockEncoder/IBlockDecoder, IVpnAdapter, IChannelModel, PolicyEngine та MetricsCollector, що дозволяє об’єднати кодування, тунелювання, ін’єкцію втрат, погодження профілів і збір показників у межах єдиного контуру керування. IVpnAdapter відповідає за підняття та контроль тунелю, а також за

оцінку ефективного MTU, IChannelModel моделює втрати та спотворення, PolicyEngine узгоджує параметри FEC і VPN, а MetricsCollector накопичує події та формує знімки стану системи. Централізоване погодження політик безпеки також використовується у SASE-архітектурах [73].

Функцію зв’язування компонентів доцільно покласти на клас SessionManager. Саме він ініціалізує екземпляри модулів, задає активний профіль сеансу, піднімає VPN-тунель, запускає FEC-кодування та забезпечує передавання кадрів між підсистемами через внутрішні черги або сокети. У такій побудові SessionManager не реалізує криптографію чи декодування самостійно, а виконує роль координатора, який підтримує правильний порядок проходження даних: прикладне навантаження → VPN/оверлей → FEC → модель каналу → буфер приймання → FEC-відновлення → передавання на прикладний рівень. Такий підхід відповідає модульній архітектурі прототипу і забезпечує можливість заміни окремих реалізацій без зміни верхнього рівня керування.

Тестове середовище доцільно реалізовувати у вигляді набору контейнерів або віртуальних машин, які моделюють кінцеві вузли зв’язку. На одному вузлі можуть розміщуватися модулі FEC-кодування та VPN-адаптер, на іншому – модулі приймання, декодування і збору результатів. Мережеве середовище між ними може відтворюватися засобами Mininet, OpenStack або аналогічних платформ віртуалізації мережевих функцій. Така побудова дозволяє відокремити логіку застосунку від логіки каналу та створити відтворювані експериментальні умови для перевірки різних комбінацій FEC, VPN і мережевих параметрів.

Система моніторингу охоплює кілька точок вимірювання. На рівні модулів кодування та декодування фіксуються події fec-encode і fec-decode, що дають змогу оцінювати час обробки та частку успішних декодувань. На рівні VPN-модуля фіксуються події vpn-up, vpn-down і rekey, які характеризують стабільність тунелю та інтервали перевстановлення ключів. На мережевому рівні збираються події drop, erase, frag, reasm і latency-sample, що дозволяють оцінювати втрати, фрагментацію, медіанну затримку та 95-й процентиль затримки. Додатково окремо відстежується

cpu-sample, який показує навантаження на процесор. Агреговані результати можуть експортуватися у форматах CSV і JSON для подальшого аналізу.

Для оцінювання обчислювальних ресурсів кожному віртуальному вузлу доцільно задавати обмеження CPU та RAM, що імітують роботу реальних пристроїв із різною продуктивністю. Обмеження на процесор можуть встановлюватися через cgroups, а під час кожної серії експериментів фіксується CPU-профіль і статус апаратного прискорення, зокрема AES-NI або ARM CE. Це важливо, оскільки висновки щодо співвідношення між затримкою, пропускною здатністю і навантаженням на процесор мають розглядатися лише в межах конкретної апаратної конфігурації.

Проведення серії випробувань доцільно організувати через клас ExperimentRunner. Його завдання полягає у запуску експериментів за наперед визначеною матрицею сценаріїв, зміні параметрів середовища та збереженні результатів. У межах таких сценаріїв можуть варіюватися тип VPN-протоколу, наявність або відсутність FEC, параметри каналу, effective MTU, кількість outbound-профілів XRay та інтенсивність трафіку. Результатом роботи ExperimentRunner є набір структурованих журналів і файлів експорту, придатних для подальшого статистичного аналізу та побудови графіків.

Важливою складовою інтеграції є також вимоги до безпеки самої програмної реалізації. VPN-адаптери повинні працювати з мінімально необхідними привілеями, ключові та тимчасові конфігураційні дані мають очищуватися після використання, а система повинна підтримувати контрольовані повторні спроби, тайм-аути та деградаційний режим роботи у випадку відмови окремого тунельного модуля. Це підвищує стійкість експериментального стенду та робить результати перевірки ближчими до реальних умов експлуатації.

Отже, інтеграція модулів у межах гібридної інформаційної технології базується на модульному принципі, віртуалізованій мережевій інфраструктурі та контрольованому розподілі обчислювальних ресурсів. Клас SessionManager забезпечує зв’язування компонентів у межах окремого сеансу, а ExperimentRunner

– проведення відтворюваних серій випробувань. Така організація дозволяє досліджувати ефективність поєднання FEC, VPN і оверлейної маршрутизації в умовах змінного каналу, обмеженого CPU та різних конфігурацій мережевого середовища. Актуальність розвитку гібридних VPN-рішень підтверджується сучасними аналітичними дослідженнями Gartner [74]. За прогнозами IDC очікується подальше зростання використання VPN та захищених оверлейних мереж у корпоративному секторі [75]. Одним із перспективних напрямів розвитку є інтеграція VPN-рішень із концепцією Zero Trust [76].

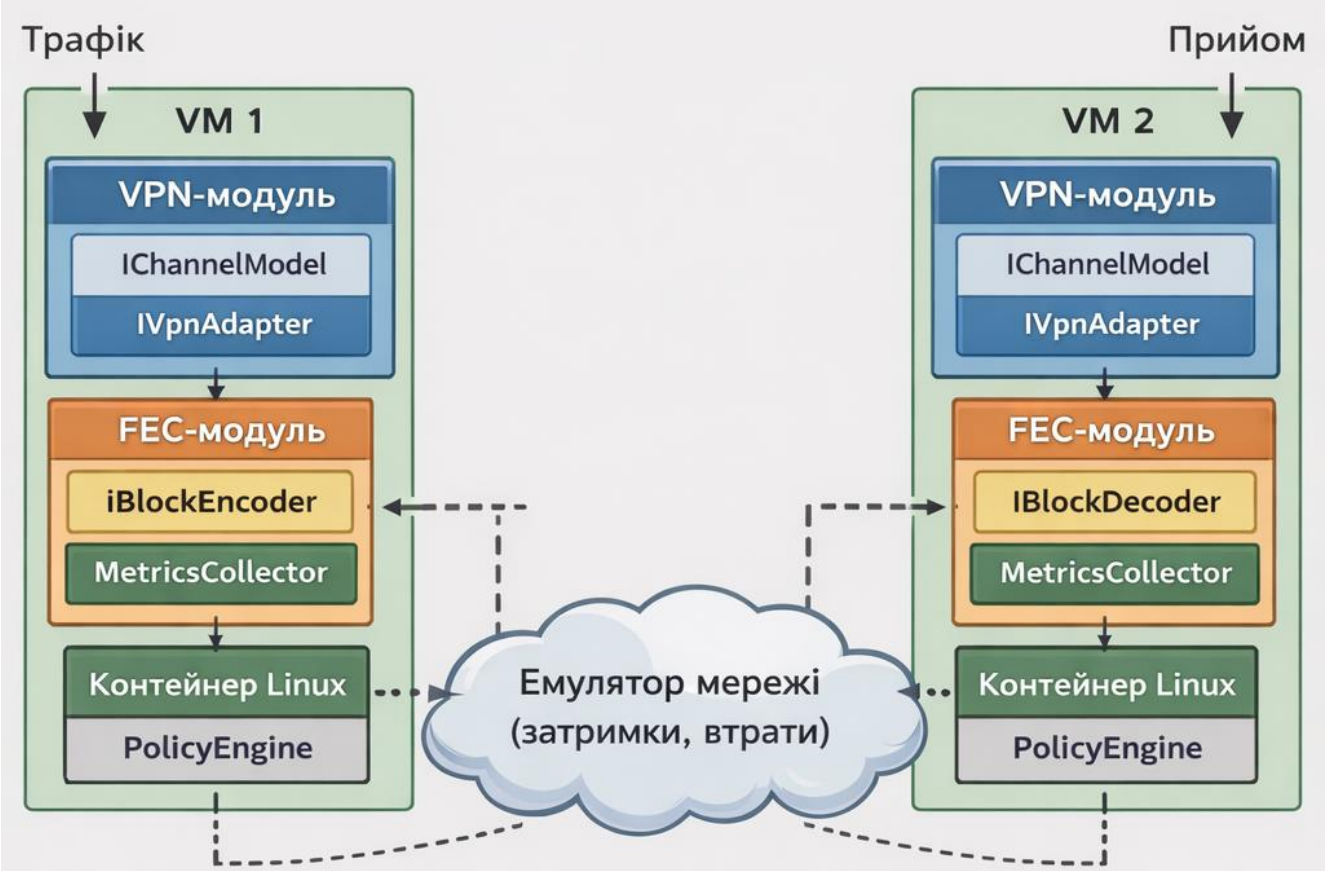


Рисунок 3.10 – Фізична схема тестового стенду з віртуальними вузлами, VPN-модулями, FEC-модулями та емулятором мережі

3.7 Критерії валідації та план експериментів

Критеріями ефективності при цьому є максимізація надійності доставки даних і пропускної здатності, а також мінімізація затримки, накладних витрат,

фрагментації та обчислювального навантаження. Кількісне оцінювання досягнення зазначених критеріїв виконується за допомогою відповідних показників та обмежень прийнятності. Аналогічні критерії використовуються і в сучасних comparative benchmark-дослідженнях VPN-рішень [77]. Порівняльний аналіз продуктивності WireGuard та OpenVPN наведено у праці панів Mackey та Mihov [78]. Результати оцінювання відкритих VPN-рішень також представлені у праці панів Anyam, Singh, Larijani, Philip [79]. Ефективність WireGuard та OpenVPN у віртуалізованих середовищах підтверджується сучасними експериментальними дослідженнями [80]. Порівняння реалізацій IPsec, WireGuard та OpenVPN також наведено у праці пана Dekker [81]. Такий підхід є доцільним, оскільки окреме покращення лише одного показника, наприклад ймовірності відновлення, не може вважатися достатнім, якщо воно супроводжується надмірним зростанням затримки, фрагментації або навантаження на процесор. У межах цієї роботи сценарій вважається прийнятним лише тоді, коли він задовольняє сукупність критеріїв, а не окремий приватний показник.

У межах валідації додатково фіксуються локальні та похідні показники, що дозволяють деталізувати причини зміни наскрізних характеристик. До таких показників належать емпірична ймовірність успішного FEC-декодування $\mathrm{P_{dec}}$, її модельна оцінка P_{dec}^{mdl}, локальні коефіцієнти успішного проходження VPN- та proxy-рівнів Π_{vpn} і Π_{prx}, ефективний корисний розмір пакета $\mathrm{M_{eff}}$, а також показники ефективності та службових витрат η, $\mathrm{h_{FEC}}$, $\mathrm{h_{VPN}}$, $\mathrm{h_{prx}}$, $\mathrm{h_{net}}$ і $\mathrm{h_{tot}}$. Саме ці величини використовуються для локалізації причин деградації, порівняння профілів та інтерпретації результатів експериментального розділу.

Для формалізації критерію прийнятності доцільно ввести індикатор валідації сценарію

$$V(s) = \begin{cases} 1, \text{якщо } \Pi_{\mathrm{e2e}}(s) \geq P_{\mathrm{i,e2e}}^{min}, \tau_{95} \leq \tau_{95}^{max}, \sigma_{\mathrm{sec}}(s) = 1, \\ \quad \xi_{\mathrm{frag}}(s) = 0, \mathrm{u_{cpu}}(s) \leq \mathrm{u_{cpu}^{max}}, \Omega(\mathrm{s}) \leq \Omega_{\mathrm{max}}; \quad , \\ 0, \text{ у будь} - \text{якому іншому можливому випадку} \end{cases} \tag{3.4}$$

У такій постановці валідація спирається на чотири групи показників, для яких задаються відповідні обмеження прийнятності. Перша група характеризує надійність передавання. Основним показником тут є $\Pi_{e2e}(s)$, який відображає частку прикладних даних, коректно доставлених і відновлених на стороні приймача. Друга група характеризує часову ефективність і містить передусім τ_{95}, оскільки саме хвіст розподілу затримок є критичним для інтерактивних сервісів. Третя група охоплює безпекові показники, що характеризують коректність встановлення VPN-тунелю, відсутність порушень автентичності та контролю цілісності пакетів, а також коректну роботу механізмів rekey. Четверта група охоплює інфраструктурні обмеження: відсутність фрагментації, дотримання допустимого рівня CPU-навантаження та обмеження на сукупний оверхед профілю. Такий набір критеріїв добре узгоджується з реалізованою в системі подієвою телеметрією та механізмом погодження параметрів через PolicyEngine.

Додатково до інтегрального критерію доцільно використовувати локальні умови прийнятності для окремих класів сценаріївДля сценаріїв із пріоритетом надійності критерієм є максимізація показника Пе2е(s), а умовою прийнятності — виконання обмеження $\Pi_{e2e}(s) \geq P_{i,e2e}^{min}$.

Для сценаріїв із жорсткими часовими вимогами основною є умова $\tau_{95} \leq \tau_{95}^{max}$.

Для сценаріїв, у яких ключовим є збереження пропускної здатності, контролюється також показник ефективної швидкості G_{app}, а для ресурсно-обмежених середовищ – обмеження $u_{cpu}(s) \leq u_{cpu}^{max}$.

Окремо накладається умова безфрагментаційного передавання $L_{adu} + \Omega_{vpn} + \Omega_{fec} \leq MTU_{eff}$. Саме ця нерівність є практичною перевіркою того, що вибраний профіль не породжує систематичної фрагментації.

Для зручності показники валідації та відповідні обмеження прийнятності узагальнено в табл. 3.1.

Таблиця 3.1 – Показники та обмеження прийнятності сценаріїв

Критерій	Позначення	Умова прийнятності	Джерело вимірювання
Надійність доставки та відновлення	Π_{e2e}	$\Pi_{\mathrm{e2e}}(s) \geq P_{\mathrm{i,e2e}}^{min}$	fec-encode, fec-decode, журнали приймання
Затримка	τ_{95}	$\tau_{95} \leq \tau_{95}^{max}$	latency-sample
Криптографічна коректність	σ_{sec}	$\sigma_{\mathrm{sec}} = 1$	vpn-up, vpn-down, rekey, журнали AEAD/ESP/TLS
Відсутність фрагментації	ξ_{frag}	$\xi_{\mathrm{frag}}(s) = 0$ або нижче допустимого порога	frag, reasm, effectiveMtu()
Навантаження на процесор	$\mathrm{u}_{\mathrm{cpu}}$	$\mathrm{u}_{\mathrm{cpu}}(s) \leq \mathrm{u}_{\mathrm{cpu}}^{max}$	cpu-sample
Сукупний оверхед профілю	Ω	$\Omega \leq \Omega_{\max}$	розрахунок профілю та службових байтів
Успішність FEC-декодування	$\mathrm{P}_{\mathrm{dec}}, \mathrm{P}_{\mathrm{dec}}^{mdl}$	$\mathrm{P}_{\mathrm{dec}} \geq \mathrm{P}_{\mathrm{dec}}^{mdl}$, $\mathrm{P}_{\mathrm{dec}} \geq \mathrm{P}_{\mathrm{dec}}^{mdl} \leq \delta_{\mathrm{dec}}$	fec-decode, журнали втрат, модельний розрахунок
Локальна успішність криптографічного та proxy-рівня	$\Pi_{\mathrm{vpn}}, \Pi_{\mathrm{prx}}$	$\Pi_{\mathrm{vpn}} \to 1, \Pi_{\mathrm{prx}} \to 1$	vpn-up, vpn-down, журнали приймання, лічильники proxy
Ефективний корисний розмір без фрагментації	M_{eff}	$L_{\mathrm{app}} \leq M_{\mathrm{eff}}$	effectiveMtu(), frag, reasm
Ефективність та структура накладних витрат	η, $\mathrm{h}_{\mathrm{FEC}}$, $\mathrm{h}_{\mathrm{VPN}}$, $\mathrm{h}_{\mathrm{prx}}$, $\mathrm{h}_{\mathrm{net}}$,$\mathrm{h}_{\mathrm{tot}}$.	$\eta \geq \eta_{min}$, $\mathrm{h}_{\mathrm{tot}} \leq \mathrm{h}_{\mathrm{tot,max}}$	службові байти профілю, журнали пакетизації, розрахунок профілю

Як матрицю сценаріїв, у якій змінюються параметри каналу, тип VPN/оверлею та параметри FEC. Формально сценарій можна задати у вигляді

$$s = (\mathrm{snr}_{\mathrm{db}}, \varepsilon, burst\_len, vpn, \mathrm{n}_{\mathrm{out}}, \varphi, W, \mathrm{L}_{\mathrm{adu}}, rekey\_sec), \quad (3.5)$$

де $\mathrm{snr}_{\mathrm{db}}$ – відношення сигнал/шум у децибелах;

ε – частка стирань/втрат;

$burst\_len$ – середня довжина бурсту;

vpn – тип тунелю;

n_{out}– кількість outbound-профілів XRay;

φ– частка repair-пакетів;

W– розмір вікна або блока кодування;

$rekey\_sec$ – період перевстановлення ключів.

З огляду на вже використані в прототипі параметри, до базової матриці випробувань доцільно включити спокійний канал, канал із помірними втратами, канал із бурстовими втратами, а також сценарії з граничним MTU та обмеженим CPU. У межах кожної серії фіксуються події кодування/декодування, втрат, стану VPN, фрагментації, затримки та завантаження процесора. Саме така телеметрія вже закладена в поточну реалізацію експериментального стенду.

Таблиця 3.2 – Базова матриця експериментальних сценаріїв

Група сценаріїв	Параметри каналу	VPN / оверлей	Параметри FEC	Основна мета
Базовий спокійний режим	$snr_{db} \approx 9$ дБ, $\varepsilon \leq 0.02$	WireGuard, IPsec, OpenVPN-UDP	FEC вимкнено; LDPC R=3/4; Polar R≈1/	Перевірка базових виграшів без стресових умов
Помірні втрати	ε≈0.05, burst_len≈	ті самі	φ у робочому діапазоні, W базове	Перевірка здатності FEC компенсувати стирання
Сильні бурстові втрати	спалахи до 24 пакетів	WireGuard, OpenVPN-UDP	LDPC R=1/, повтор ×1, збільшене W	Перевірка стійкості віконного/надлишкового профілю

MTU-критичні режими	змінне L_{adu}, граничний MTU_{eff}	усі VPN	різні Ω_{fec}, clipping payload	Перевірка відсутності фрагментації
Ресурсно-обмежені режими	ті самі, але з обмеженням CPU	усі VPN	полегшені та важкі профілі FEC	Оцінка u_{cpu}, latency/throughput/CPU

Статистична обробка результатів має виконуватися не за одиничними прогонами, а за серіями повторів. Для кожної точки експериментального плану доцільно виконувати не менше 30 повторів, після чого обчислювати середні значення, дисперсії, медіани, 95-й процентиль затримки та 95 % довірчі інтервали для ефективної швидкості. Такий підхід уже узгоджується з логікою представлення результатів у четвертому розділі, де для швидкості наводяться довірчі інтервали, а для затримки – медіана та 95-й процентиль.

Основними обмеженнями експериментального плану є залежність висновків від конкретної апаратної конфігурації, відтворюваність параметрів канального емулятора та коректність оцінки ефективного MTU після інкапсуляції. Зокрема, висновки щодо співвідношення затримки, пропускної здатності та CPU-навантаження є коректними лише для тієї конфігурації, для якої було зафіксовано статус AES-NI або ARM CE та обмеження процесорних ресурсів. Крім того, параметри на кшталт snr_{db}, burst_len, rekey_sec і порогів безфрагментаційного MTU не можуть вважатися універсальними для всіх мережевих середовищ і мають інтерпретуватися як репрезентативні для тестового стенду.

До основних ризиків належать фрагментація, перевантаження процесора, надмірний оверхед профілю, нестабільність тунелю під час rekey та ускладнення профілів адаптації. Ризик фрагментації мінімізується попереднім кліпінгом корисного навантаження відповідно до умови $L_{adu} \leq MTU_{eff} - \Omega_{vpn} - \Omega_{fec}$, а також використанням effectiveMtu() і процедур DPLPMTUD/PLPMTUD. Ризик перевантаження CPU мінімізується шляхом виключення профілів, для яких $u_{cpu} >$

u_{cpu}^{max}, а також через окремий контроль подій cpu-sample. Ризик нестабільності тунелю та піків затримки мінімізується моніторингом vpn-up, vpn-down, rekey і повторними запусками з контрольованими таймерами. Ризик надмірної складності профілю мінімізується введенням обмеження $\Omega(p) \leq \Omega_{max}$, що не дозволяє вибирати профілі з непропорційно великими службовими витратами.

Підсумовуючи, валідація запропонованої системи повинна розглядатися як багатокритеріальна процедура, у якій прийнятність профілю визначається не окремим показником, а одночасним виконанням вимог до надійності, затримки, безпеки, відсутності фрагментації та обчислювального навантаження. Запропонована матриця сценаріїв дозволяє системно дослідити як базові, так і стресові режими роботи. Водночас введені обмеження та заходи мінімізації ризиків забезпечують відсікання нерелевантних або завідомо непридатних конфігурацій ще до етапу глибокого статистичного аналізу.

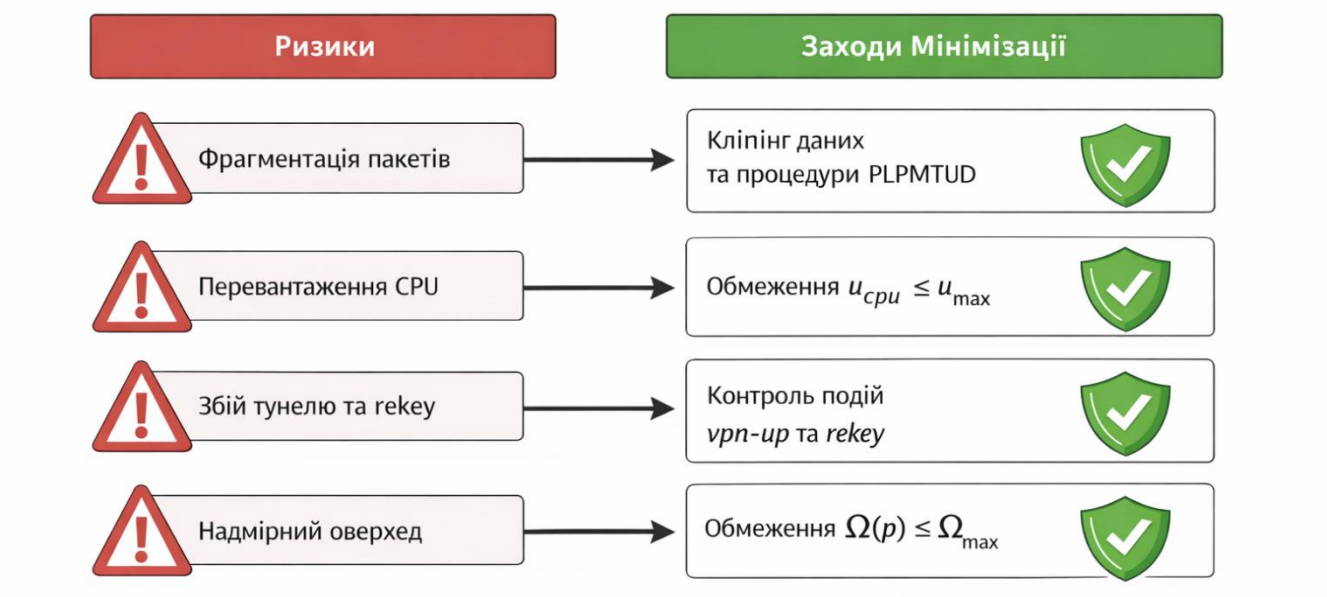


Рисунок 3.10 – Ризики та засоби мінімізації ризиків

3.8 Висновки за розділом

У третьому розділі розроблено моделі та методи побудови гібридних захищених каналів передавання даних, а також виконано їх програмну реалізацію в межах інтегрованої інформаційної технології.

1. Визначено загальну архітектуру реалізації гібридної технології, що поєднує механізми завадостійкого кодування, VPN-тунелювання та оверлейних сервісів для забезпечення надійності й захищеності передавання даних.

2. реалізовано метод синтезу профілю гібридного каналу, який забезпечує формування параметрів системи відповідно до характеристик мережі, рівня завад та вимог до якості обслуговування трафіку.

3. Виконано програмну реалізацію методу адаптивного керування параметрами FEC-кодування та оверлейних протоколів, що дозволяє динамічно змінювати конфігурацію системи залежно від стану каналу передавання даних.

4. Реалізовано модулі завадостійкого кодування та відновлення даних, призначені для зменшення впливу помилок і втрат пакетів у процесі передавання інформації.

5. Рреалізовано модулі VPN, V2Ray/XRay та криптографічного захисту, які забезпечують конфіденційність, цілісність і захищеність мережевої взаємодії.

6. Ввиконано інтеграцію окремих модулів у межах єдиної інформаційної технології, визначено особливості мережевої інфраструктури та обчислювальних ресурсів, необхідних для функціонування системи.

7. Сформовано критерії валідації та план експериментальних досліджень, що дозволяють оцінити ефективність запропонованих моделей і методів у різних умовах функціонування мережі.

Результати, пов’язані з дослідженням сумісності методів завадостійкого кодування та протоколів високого рівня, побудовою моделей стійких до завад систем передавання даних, а також реалізацією багаторівневого захисту на основі спільного використання VPN-протоколів і механізмів корекції помилок, були частково апробовані та висвітлені у працях автора [82–85].

За результатами розділу розроблено програмно-алгоритмічне забезпечення гібридної технології захищеного передавання даних та реалізовано інтегровану систему, що забезпечує спільне використання механізмів завадостійкого кодування, VPN-тунелювання та адаптивного керування параметрами мережевої взаємодії. Отримані результати створюють основу для проведення імітаційного моделювання та експериментальної перевірки ефективності запропонованих рішень.

РОЗДІЛ 4. ТЕСТУВАННЯ РЕАЛІЗАЦІЇ ГІБРИДНОЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

4.1 Експериментальна частина та система тестових сценаріїв

В даному розділі спрямоване на практичну перевірку результатів функціонування розробленої гібридної інформаційної технології. З погляду IDEF0 це відповідає валідації правих виходів функціонального блоку A0, а саме: переданих та відновлених прикладних даних, показників надійності передавання, результатів контролю цілісності та аналітичних даних для оцінювання якості. Таким чином, четвертий розділ логічно завершує побудовану раніше модель, оскільки переходить від опису вхідних даних, керувальних впливів і механізмів до перевірки фактичних вихідних результатів системи.

Окремим напрямом експериментальної перевірки є оцінювання впливу криптографічного оверлею на характеристики передавання даних. На відміну від дослідження криптостійкості алгоритмів, у роботі аналізуються експлуатаційні наслідки застосування криптографічного захисту, а саме: зміна ефективної пропускної здатності, накладних витрат, допустимого MTU, процесорного навантаження, затримки встановлення тунелю та поведінки системи під час процедур rekey. Це дозволяє оцінити місце криптографічного рівня в загальному контурі забезпечення надійності та захищеності передавання даних.

Експериментальна частина організована у вигляді матриці тестових сценаріїв, у межах якої варіюються три групи параметрів: умови каналу, параметри FEC та тип захищеного оверлею. Для каналу задаються значення SNR=3,6,9 дБ та пакетні втрати в діапазоні 0–10 %. Для завадостійкого кодування змінюються коефіцієнт надлишковості φ=0–0,5 і розмір вікна W=4 або W=16. Для захищеного транспортного середовища використовуються профілі IPsec, OpenVPN і WireGuard, а для XRay додатково перевіряються конфігурації з 1-3 outbound-профілями. У підсумку сформовано 36 базових комбінацій сценаріїв, кожна з яких виконується серією повторів для зменшення впливу випадкових коливань результатів.

Експериментальний стенд реалізовано на базі Java-прототипу з використанням Docker-контейнерів як віртуальних вузлів зв’язку. На передавальному вузлі розміщуються модулі формування трафіку, VPN-тунелювання та FEC-кодування, а на приймальному – модулі приймання, дешифрування, декодування та фіксації результатів. Між вузлами розташовується емулятор каналу, який дозволяє відтворювати задані значення затримки, втрат і деградації середовища. Така побудова дає змогу досліджувати систему не ізольовано на рівні окремого алгоритму, а як цілісний ланцюг передавання, захисту, відновлення та контролю якості.

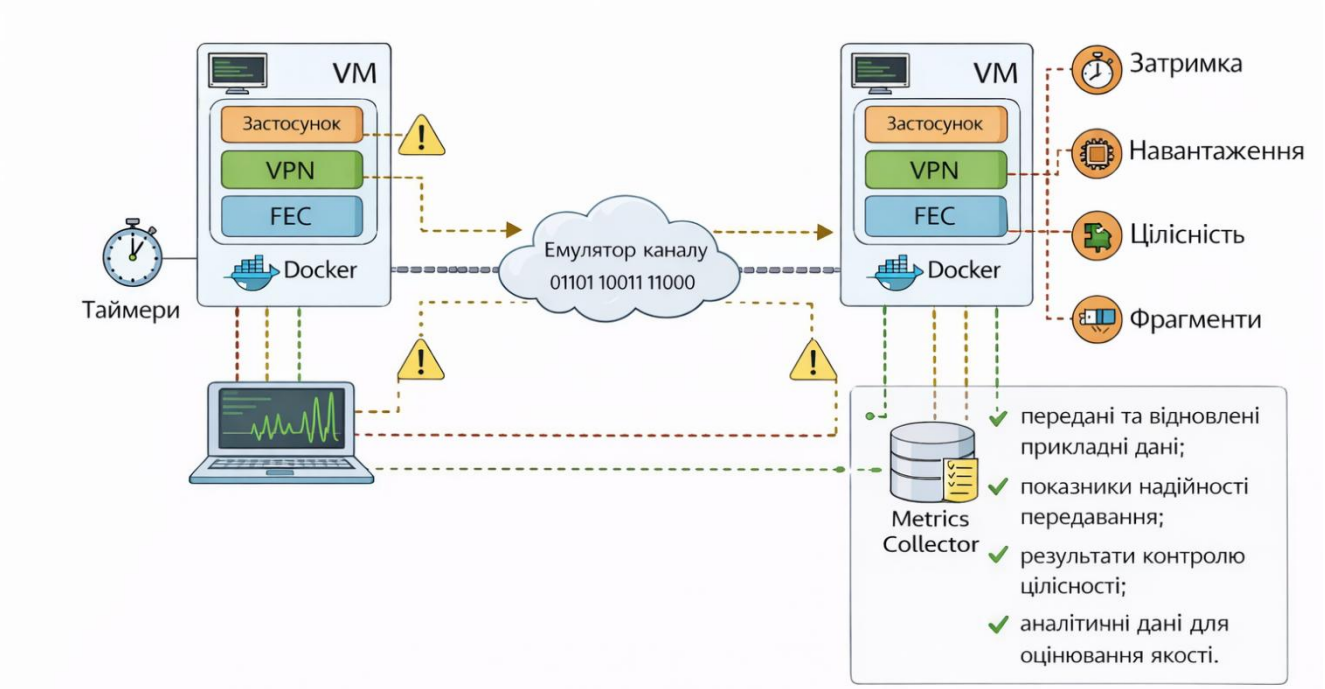


Рисунок 4.1 – Загальна схема експериментального стенду з віртуальними вузлами, емулятором каналу та точками вимірювання

Для кожного сценарію на вхід системи подається фіксований набір із 1000 ADU-пакетів. У процесі виконання тесту фіксуються показники, що безпосередньо відповідають виходам IDEF0-моделі. До них належать: факт коректного отримання і відновлення прикладних даних; коефіцієнт успішної доставки $П_{e2e}$; затримка доставки, зокрема 95-й процентиль τ_{95}; goodput на рівні застосунку; результати

контролю цілісності VPN-пакетів; частка фрагментованих пакетів; навантаження на процесор u_{cpu}. Отже, у межах експерименту перевіряється не лише працездатність окремих модулів, а й досягнення тих вихідних характеристик, які були визначені як цільові результати всієї інформаційної технології.

Точки вимірювання організовані за трьома рівнями. На рівні застосунку фіксуються час отримання повного ADU та частка успішно доставлених даних. На рівні програмних модулів вимірюється час обробки в FEC- і VPN-компонентах, а також події встановлення тунелю, rekey та помилки відновлення. На рівні мережевого середовища контролюються затримки, втрати та фрагментація. Збір і первинна агрегація цих даних виконується засобами MetricsCollector, а запуск, повторення сценаріїв і збереження журналів результатів забезпечує клас ExperimentRunner.

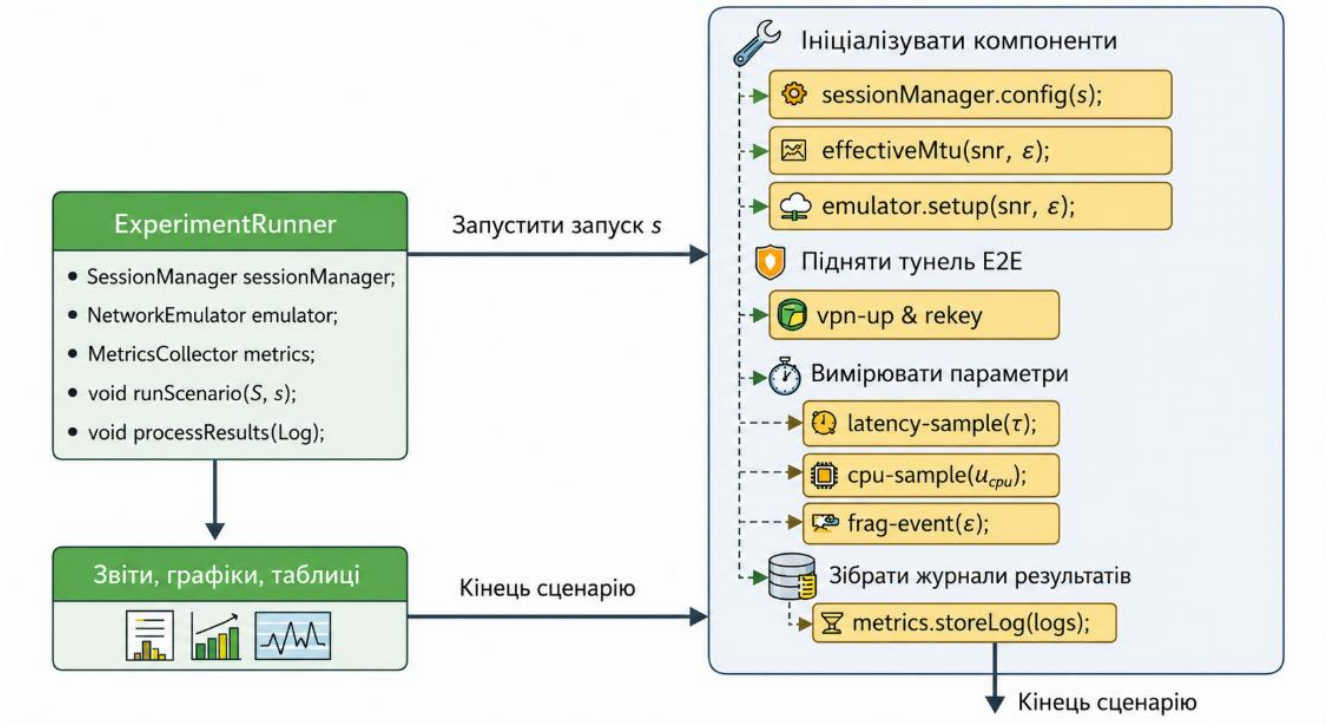


Рисунок 4.2 – Загальна схема експериментального стенду з віртуальними вузлами, емулятором каналу та точками вимірювання

Для зручності подання експериментального плану основні сценарії доцільно звести в таблицю.

Таблиця 4.1 – Базові групи тестових сценаріїв

Група сценаріїв	Варійовані параметри	Мета дослідження
Базові	SNR=9 дБ, втрати 0 – 1 %, φ=0	Контрольний режим без суттєвої деградації каналу
Канал із помірними втратами	SNR=6 дБ, втрати 3– 5 %, φ=0,1–0,3	Оцінка ефективності FEC у типових умовах
Канал із сильними втратами	SNR=3дБ, втрати 5 – 10 %, φ=0,2–0,5	Перевірка меж працездатності системи
VPN-порівняння	IPsec, OpenVPN, WireGuard	Оцінка впливу типу тунелю на затримку і goodput
XRay-конфігурації	1–3 outbounds	Перевірка впливу маршрутизаційної гнучкості

Для сценаріїв, у яких використовується захищений оверлей, додатково фіксуються показники T_{vpn}, T_{rekey}, u_{cpu}, Ω_{vpn}, G_{app} та $П_{vpn}$. Це дозволяє відокремити втрати, спричинені фізичним каналом і механізмами завадостійкого кодування, від втрат або деградації продуктивності, пов’язаних із роботою криптографічного рівня.

Окремо було сформовано динамічний сценарій, у межах якого значення SNR не залишалося сталим протягом усього сеансу, а змінювалося у часі відповідно до наперед заданого профілю деградації та відновлення каналу. Така постановка дозволила оцінити SNR не лише як параметр сценарію, а як змінну характеристику середовища передавання, що безпосередньо впливає на BER, FER та інші показники. У цьому сценарії фіксувалися часові траєкторії γ, а також відповідні реакції системи у вигляді зміни коефіцієнта надлишковості φ та підсумкових показників якості доставки. Це дало змогу експериментально підтвердити, що погіршення SNR проявляється не лише у зниженні якості фізичного каналу, а й у

зміні наскрізних характеристик функціонування гібридної інформаційної технології.

Дослідження роботи адаптивного механізму при динамічній зміні SNR. Метою експерименту було оцінювання реакції гібридної інформаційної технології на погіршення та подальше відновлення умов передавання даних. Для цього було сформовано динамічний сценарій, у якому відношення сигнал/шум γ змінювалося за заздалегідь визначеним часовим профілем. У процесі дослідження аналізувалися зміни коефіцієнта надлишковості FEC φ, 95-процентного часу доставки пакетів τ_{95} та досяжної корисної швидкості передавання Gapp. В експерименті досліджувався процес передавання даних у гібридному захищеному каналі за умов динамічної зміни якості середовища передавання. Тривалість одного циклу моделювання становила 60 с. Протягом сеансу значення відношення сигнал/шум γ змінювалося відповідно до заданого часового профілю, що включав етапи поступового погіршення та відновлення характеристик каналу. Контроль стану системи здійснювався з інтервалом 1 с. Передавання виконувалося для потоку даних інтенсивністю 10 Мбіт/с із використанням пакетів розміром 1400 байт. Для підвищення надійності застосовувався адаптивний механізм FEC, який автоматично коригував параметри кодування відповідно до поточного стану каналу. Кожна точка графічних залежностей сформована як середнє значення, отримане за результатами 120 незалежних запусків моделі. Результати наведені у додатку В, таблиця В1.

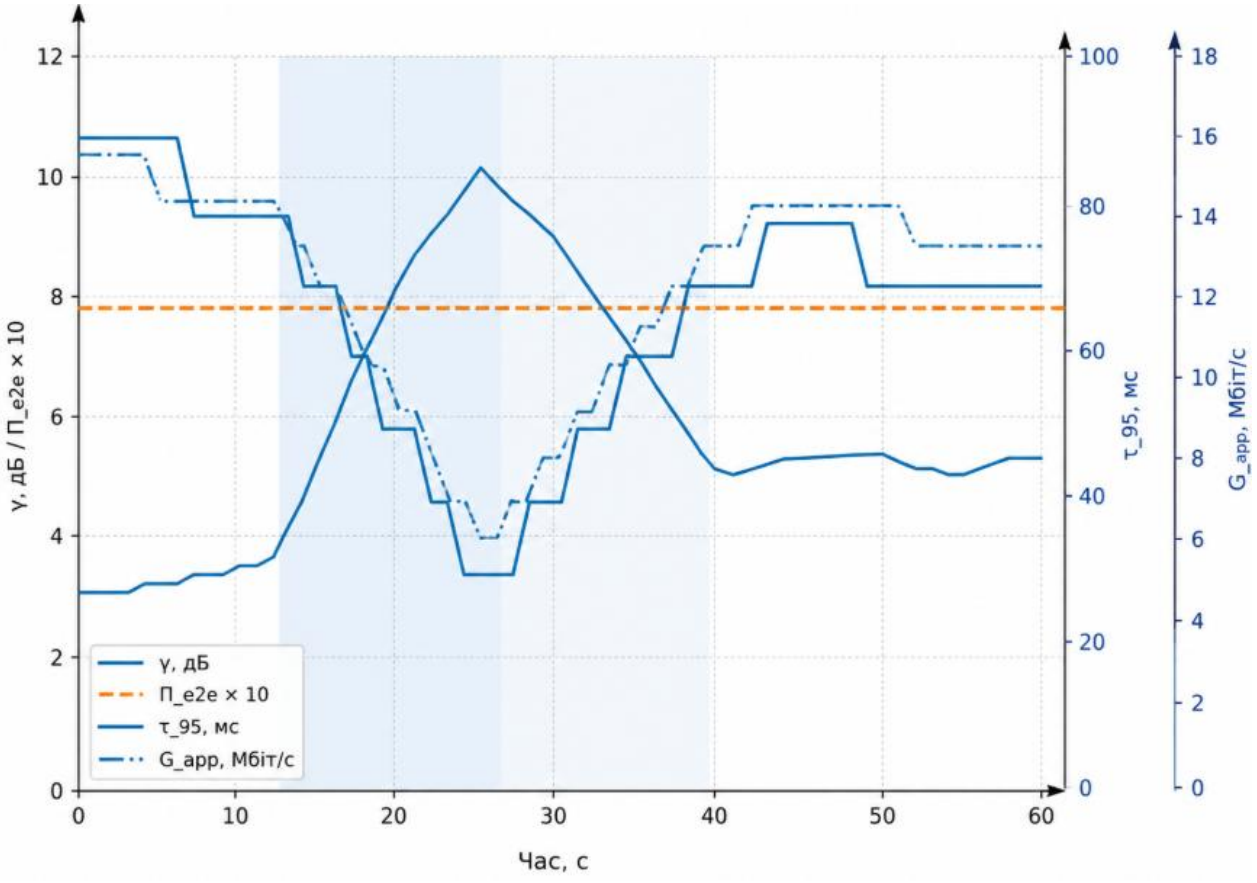


Рисунок 4.3 – Часові залежності у динамічному сценарії зміни SNR

Поряд із базовими сценаріями до матриці експериментів доцільно включити оцінювання часу підготовки захищеного каналу τ_{setup}. У межах цієї групи вимірюється інтервал від моменту ініціації процедури встановлення захищеного каналу або оверлейного профілю до моменту готовності системи до передавання корисних даних. Для IPsec це відповідає завершенню формування SA, для OpenVPN – завершенню TLS-handshake, для WireGuard – завершенню початкового handshake, а для XRay – завершенню ініціалізації конфігурації тунелювання та маршрутизації. Таке оцінювання дозволяє врахувати часову вартість входу системи у захищений режим як окремий показник ефективності.

Для кожної конфігурації результати усереднюються за серією прогонів, після чого формуються підсумкові звіти для подальшого аналізу в підрозділах 4.2–4.5. Такий підхід забезпечує зв’язок між експериментальним планом і структурою IDEF0-моделі: у межах дослідження контролюється, наскільки система за різних

умов здатна забезпечити саме ті виходи, які були визначені на етапі функціонального моделювання, тобто передані та відновлені прикладні дані, показники надійності передавання, результати контролю цілісності та аналітичні дані для оцінювання якості.

Окремо до матриці тестових сценаріїв доцільно включити вимірювання BER для кожної досліджуваної конфігурації. Для цього в умовах однакових значень SNR, рівня втрат, коефіцієнта надлишковості φ та типу захищеного оверлею фіксується частка бітів, відновлених із помилкою після проходження каналу. Таке оцінювання дозволяє кількісно встановити, як зміна параметрів FEC та вибір профілю тунелювання впливають на фізичний рівень достовірності передавання, а також забезпечує основу для подальшого порівняння режимів IPsec, OpenVPN, WireGuard і XRay-конфігурацій.

Крім безпосереднього вимірювання BER та FERR, для кожної серії сценаріїв доцільно визначати виграш кодування G_{code}. Для цього за експериментально отриманими залежностями BER(SNR) або FER(SNR) встановлюється різниця між значеннями SNR, необхідними для досягнення однакового цільового рівня помилок у режимі без FEC та в режимі з FEC. Такий підхід дозволяє перейти від набору окремих кривих до узагальненого показника ефективності завадостійкого кодування в умовах використання різних типів захищеного оверлею, включаючи IPsec, OpenVPN, WireGuard та XRay-конфігурації.

Окремо до матриці тестових сценаріїв доцільно включити групу перевірок, спрямованих на чисельне оцінювання інтегрального індексу захищеності I_{sec}. У межах цієї групи виконуються сценарії несанкціонованої автентифікації, введення модифікованих пакетів, імітації replay-передавань та перевірки коректності повторного узгодження ключового матеріалу. За результатами таких сценаріїв обчислюються часткові показники A_*, після чого визначається підсумкове значення I_{sec} для профілів IPsec, OpenVPN та WireGuard.

4.2 Результати тестування передавання та відновлення даних

У ході проведених експериментів встановлено, що реалізована гібридна інформаційна технологія забезпечує коректне передавання та відновлення даних у більшості досліджених сценаріїв. Отримані результати підтверджують, що ефективність системи істотно залежить від поєднання трьох груп факторів: якості каналу, обраного VPN-оверлею та рівня надлишковості FEC. У стабільних умовах каналу система працює передбачувано навіть за помірних значень надлишковості, тоді як у режимах із низьким SNR або підвищеною часткою втрат саме FEC-компонент стає визначальним для збереження прийнятного рівня доставки прикладних даних. Таке спостереження узгоджується як із закладеною в розділі 4.1 методикою випробувань, так і з проміжними висновками щодо робочих зон кодів та бюджету накладних витрат.

Окремо слід підкреслити, що коефіцієнт надлишковості φ у проведених експериментах виступає не лише параметром налаштування FEC, а й одним із ключових факторів кінцевого результату. Саме зміна φ визначає компроміс між підвищенням імовірності коректного відновлення даних та зростанням накладних витрат на передавання.

Для деталізації внеску FEC-компонента додатково оцінювалися емпірична ймовірність успішного декодування P_{dec} та її модельна оцінка P_{dec}^{mdl}. Отримані результати показали, що зі зростанням частки repair-пакетів φ величина P_{dec} зростає монотонно, а різниця між P_{dec} та P_{dec}^{mdl} залишається обмеженою в межах робочих сценаріїв. Це підтверджує, що аналітична модель FEC придатна для попереднього вибору параметрів профілю та узгоджується з експериментальними результатами прототипу.

Проведене ослідження впливу коефіцієнта надлишковості FEC на ймовірність успішного декодування, з метою оцінювання впливу коефіцієнта надлишковості FEC φ на ймовірність успішного відновлення даних у каналі з різним рівнем втрат пакетів. Під час дослідження порівнювалися результати імітаційного моделювання P_{dec} та значення, отримані за аналітичною моделлю

P_{dec}^{mdl}. Це дозволило оцінити точність розробленої моделі та визначити діапазон значень φ, за яких забезпечується стабільне відновлення даних. Моделювання виконувалося для трьох рівнів втрат пакетів: ε = 0,02, ε = 0,05 та ε = 0,10. Значення коефіцієнта надлишковості φ змінювалося від 0,04 до 0,60. Для кожної точки виконувалося 120 незалежних запусків моделі передачі даних із випадковою генерацією втрат пакетів відповідно до заданого значення ε. Результати є усередненими значеннями за всіма експериментальними серіями. Результати наведені у додатку В, таблиці В2-В4.

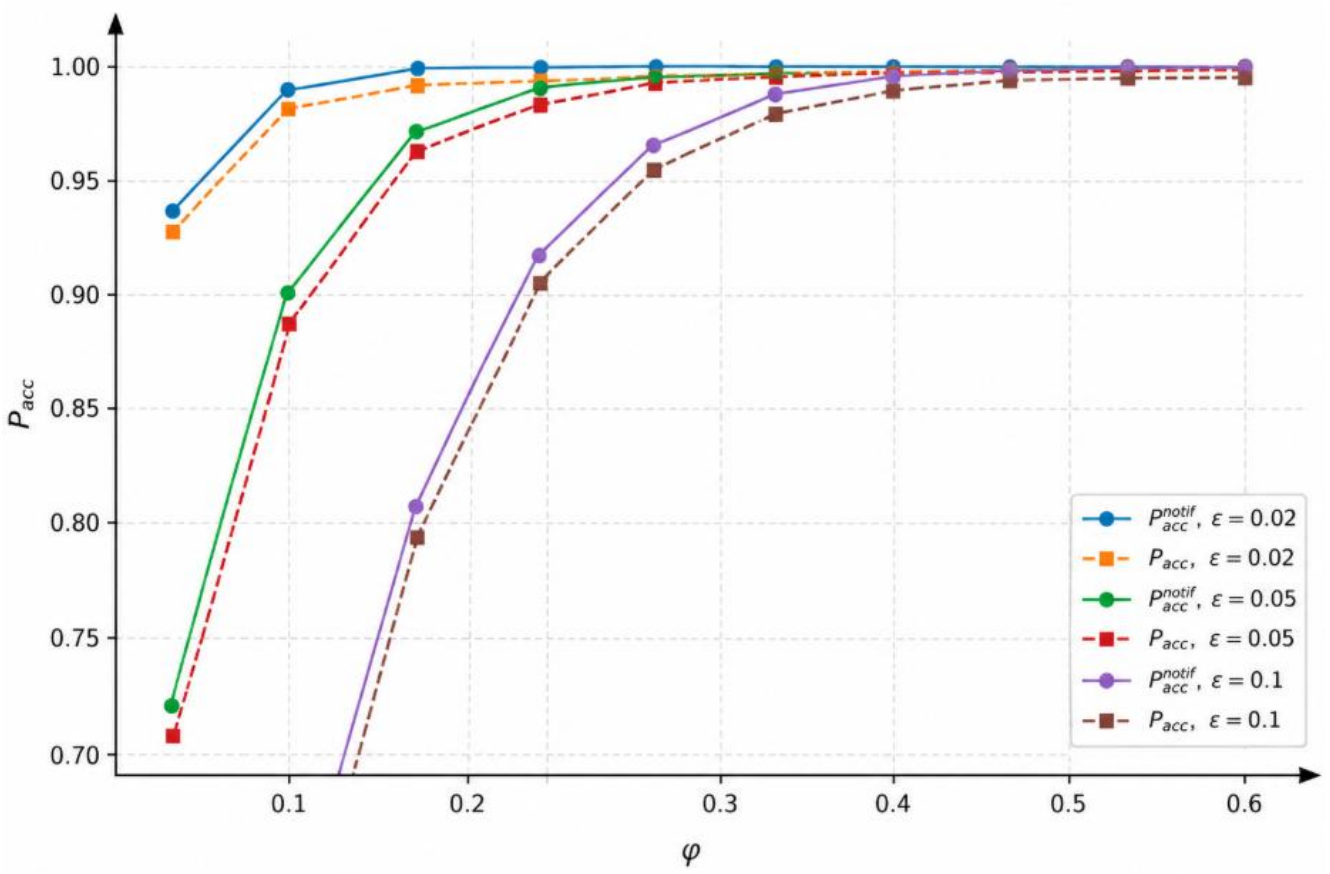


Рисунок 4.3 – Залежність P_{dec} та P_{dec}^{mdl} від φ для різних значень ε

Отримані результати показали, що в області малих значень φ рівень корекційної надлишковості є недостатнім для стабільної роботи в деградованому

каналі, тоді як надмірне збільшення φ не забезпечує пропорційного покращення доставки, але погіршує показники goodput і часові характеристики. Таким чином, саме φ є тим параметром, який визначає робочу область ефективності FEC у запропонованій інформаційній технології.

Найбільш показові відмінності спостерігалися у сценаріях із низьким рівнем SNR, насамперед при SNR=3 дБ. За відсутності додаткового FEC у таких умовах значна частка пакетів втрачалася ще до того, як могла бути відновлена на прикладному рівні, унаслідок чого коефіцієнт успішної доставки різко знижувався. Натомість при переході до профілів із φ≥0,2 система демонструвала суттєве покращення результатів: більшість ADU успішно досягала приймача, а процес декодування забезпечував відновлення майже всіх корисних даних. У наведених експериментальних сценаріях для таких режимів спостерігалося значення $П_{e2e} \approx 0{,}98$, що свідчить про досягнення практично повної працездатності навіть у деградованому каналі. Зокрема, у сценарії «WireGuard, SNR=3 дБ, φ=0,3» було відновлено 99,2 % пакетів, а кількість відмов на прикладному рівні залишалася поодинокою.

Отримані результати важливі не лише з погляду абсолютних чисел, а й з погляду загальної форми залежності. У всіх серіях вимірювань спостерігалася характерна закономірність: зі збільшенням φ ймовірність успішної доставки зростала до певного насичення, після чого приріст ставав менш помітним. Це означає, що надлишковість дійсно компенсує втрати й стирання в каналі, однак після досягнення робочої зони подальше збільшення repair-частини вже дає менший ефект у відносних одиницях.

Саме тому для практичних профілів доцільно орієнтуватися не на максимальне можливе φ, а на таке значення, за якого досягається необхідний рівень $П_{e2e}$ без непропорційного збільшення затримки та накладних витрат. Така інтерпретація добре узгоджується і з паспортом канального шару, де для нижчих кодових коефіцієнтів або більш захищених профілів уже спостерігається краща стійкість у “брудних” каналах.

Для оцінювання впливу коефіцієнта надлишковості FEC φ на коефіцієнт успішної доставки $П_{e2e}$ було проведено серію експериментів для VPN-профілів WireGuard, IPsec та OpenVPN за значень SNR 3 дБ і 6 дБ. У процесі моделювання значення φ змінювалося в діапазоні від 0 до 0,5, а для кожної конфігурації виконувалося понад 100 незалежних запусків моделі передачі даних. Наведені на рисунку результати являють собою усереднені значення коефіцієнта успішної доставки, отримані за підсумками всіх експериментальних серій.

Для оцінювання впливу коефіцієнта надлишковості FEC φ на коефіцієнт успішної доставки $P_{s,tot}$ було проведено серію експериментів для VPN-профілів WireGuard, IPsec та OpenVPN за значень SNR 3 дБ і 6 дБ. У процесі дослідження значення коефіцієнта надлишковості змінювалося в діапазоні від 0 до 0,53, що дозволило проаналізувати вплив додаткових repair-пакетів на результативність передачі даних. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями коефіцієнта успішної доставки $P_{s,tot}$. Результати наведені у додатку В, таблиця В5.

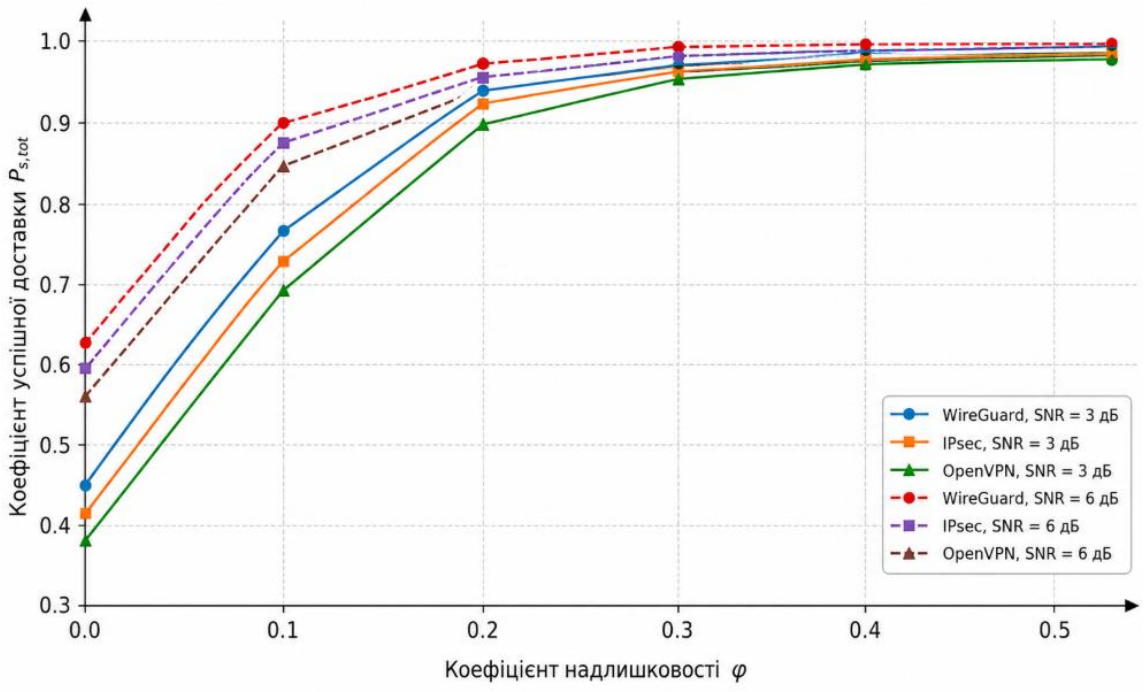


Рисунок 4.4 – Порівняння коефіцієнта успішної доставки $П_{e2e}$ для різних значень φ та VPN-профілів при SNR=3 і 6 дБ

Окремо було проаналізовано часові характеристики доставки. Як показали вимірювання, додавання FEC-компонента закономірно збільшує сумарну затримку, оскільки до процесу передавання додаються операції кодування, формування repair-пакетів, буферизації та декодування на приймальному боці. Проте це збільшення в більшості сценаріїв залишалося контрольованим і не виводило систему за межі допустимих цільових параметрів. Для сценаріїв із SNR=6 дБ встановлено, що при φ=0,05 95-й процентиль затримки становив приблизно $\tau_{95} \approx 120$ мс, тоді як при φ=0,3 він зростав до $\tau_{95} \approx 140$мс. Отже, збільшення надлишковості супроводжувалося підвищенням затримки, але цей приріст був значно меншим за виграш у надійності доставки. Без FEC за тих самих умов втрати могли перевищувати 40 %, що фактично робило канал непридатним для стабільної доставки ADU.

Таким чином, експерименти показали, що для системи характерний типовий компроміс між надійністю та затримкою: профілі з нижчою надлишковістю мають кращі часові характеристики, але гірше працюють у режимах із деградацією каналу, тоді як профілі з вищим φ збільшують τ_{95}, проте істотно зменшують частку невідновлених даних. Для практичного використання це означає, що вибір профілю має здійснюватися не ізольовано за критерієм мінімальної затримки або максимальної надійності, а з урахуванням цільового режиму функціонування. Саме з цієї причини в подальших підрозділах доцільно аналізувати не окремі величини, а їх спільну поведінку в межах конкретного профілю системи.

Ще одним важливим результатом тестування стала оцінка впливу VPN-інкапсуляції на фрагментацію пакетів. У межах серії експериментів встановлено, що ризик фрагментації залежить не лише від вихідного розміру ADU, а й від сукупного бюджету накладних витрат, який формується за рахунок FEC-службової частини та заголовків VPN-протоколу. Саме тому інтерпретація результатів передавання й відновлення повинна виконуватися з урахуванням сумарного overhead, а не лише параметрів корекційного коду. Це безпосередньо узгоджується з уже зафіксованим у матеріалах висновком, що бюджет накладних FEC необхідно

складати з витратами інкапсуляції VPN, щоб не перевищити MTU та не втратити ефективність передавання.

У більшості сценаріїв фрагментація проявлялася рідко й не перевищувала 5 % пакетів, що свідчить про коректну роботу механізму підбору MTU та адаптивної пакетизації. Це означає, що система в більшості режимів уникала систематичного перевищення допустимого розміру мережевої дейтаграми, а отже, не створювала зайвих втрат і коливань затримки через повторне складання фрагментів. Разом із тим у профілях із OpenVPN ризик фрагментації виявився вищим, ніж у WireGuard або IPsec, що пояснюється більшим службовим навантаженням і додатковими заголовками транспортного рівня. Однак навіть у цих випадках адаптивне коригування розміру корисного навантаження дозволяло повністю прибрати фрагментацію, і в серіях вимірювань фіксувалося значення $\xi=0$. Такий результат є важливим, оскільки показує, що проблема фрагментації в системі не ігнорується, а компенсується на рівні узгодження параметрів пакетизації та тунелювання.

Для оцінювання впливу коефіцієнта надлишковості FEC φ на затримку доставки та рівень фрагментації пакетів було проведено серію експериментів для VPN-профілів IPsec, OpenVPN та WireGuard. У процесі дослідження значення φ змінювалося в діапазоні від 0 до 0,30. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, за результатами яких визначалися 95-й процентиль затримки доставки τ_{95} та частка фрагментованих пакетів ξ_{frag}. Наведені результати є усередненими значеннями, отриманими за всіма експериментальними серіями. Результати наведені у додатку В, таблиця В6.

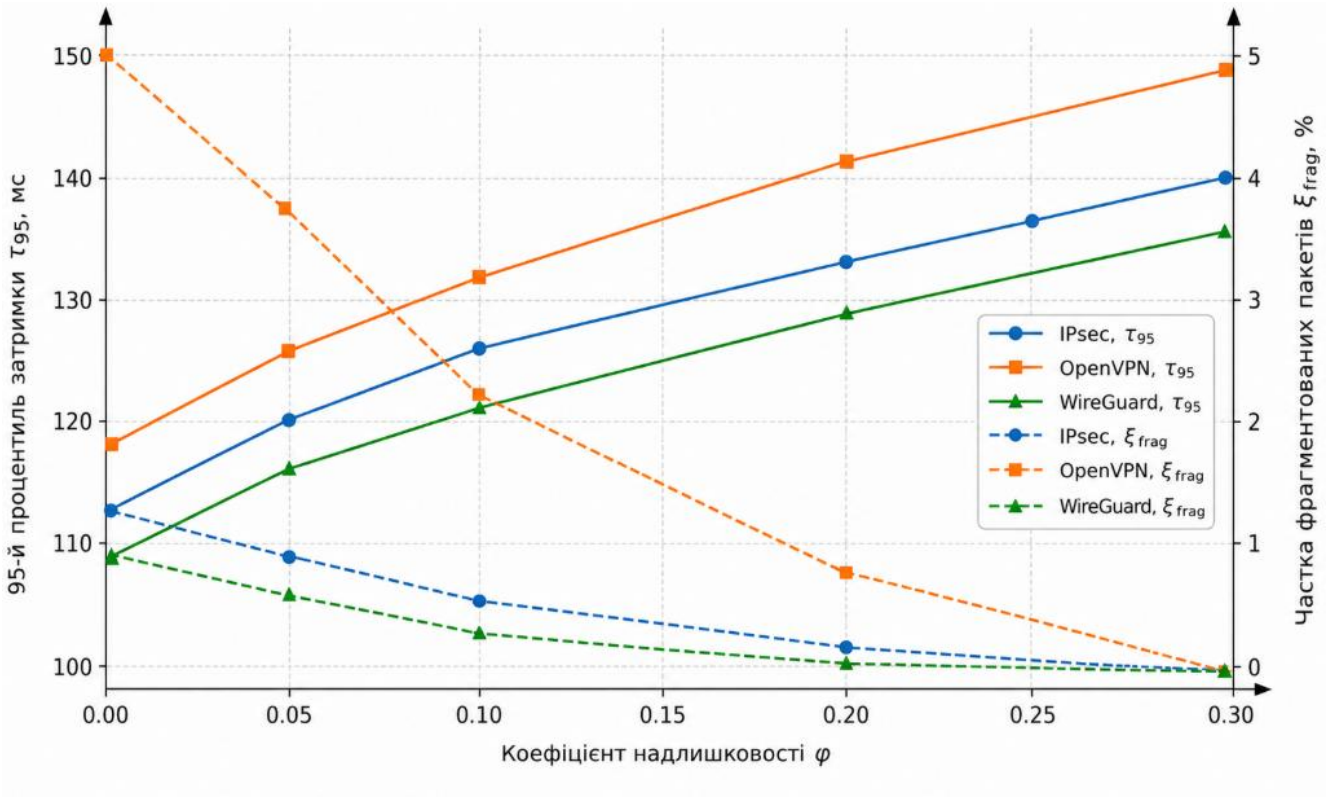


Рисунок 4.5 – Залежність τ_{95} та частки фрагментованих пакетів від φдля профілів IPsec, OpenVPN і WireGuard

Узагальнюючи результати тестування передавання та відновлення даних, можна зробити висновок, що реалізована система досягає поставленої мети саме як гібридна інформаційна технологія, а не як проста сума окремих компонентів. При зниженні якості каналу один лише VPN не забезпечує належної доставки прикладних даних, тоді як додавання FEC дозволяє втримати $П_{e2e}$на високому рівні. Водночас накладні витрати такого підходу залишаються контрольованими: затримка зростає помірно, а фрагментація за коректного підбору MTU практично усувається. Отже, експериментально підтверджено, що поєднання захищеного оверлею, адаптивної пакетизації та завадостійкого кодування забезпечує передані та відновлені прикладні дані, показники надійності передавання та результати контролю цілісності, тобто саме ті праві виходи, які були визначені у функціональній IDEF0-моделі системи.

4.3 Оцінювання показників надійності та якості функціонування

Оцінювання результатів експериментального дослідження виконувалося за сукупністю наскрізних метрик, які безпосередньо характеризують праві виходи функціональної IDEF0-моделі системи. У цьому підрозділі аналізуються передані та відновлені прикладні дані, показники надійності передавання, результати контролю цілісності та аналітичні дані для оцінювання якості функціонування.

Для локалізації причин деградації наскрізних характеристик було додатково проаналізовано локальні коефіцієнти успішного проходження пакетів через криптографічний і proxy-рівні, а саме Π_{vpn} та Π_{prx}. Показано, що за однакових умов каналу зниження наскрізної успішності може бути пов’язане не лише з недостатньою відновлюваністю FEC-блоків, а й з відкиданням пакетів на етапі криптографічної перевірки або proxy-обробки. Тому спільний розгляд Π_{vpn}, Π_{prx} та P_{dec} дозволяє відокремити втрати, зумовлені каналом, від втрат, що виникають на верхніх шарах захищеного тракту.

Для дослідження впливу якості каналу на функціонування окремих компонентів гібридної інформаційної технології було проведено серію експериментів для VPN-профілів IPsec, OpenVPN та WireGuard. У процесі моделювання оцінювалися коефіцієнти успішного проходження пакетів через криптографічний рівень Π_{vpn} та proxy-рівень Π_{prx} за різних значень відношення сигнал/шум SNR. Значення SNR приймали 3, 6 та 9 дБ. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі передачі даних, а підсумкові значення показників визначалися шляхом усереднення отриманих результатів. Це дозволило оцінити внесок окремих рівнів обробки пакетів у формування загальної успішності доставки даних. Результати наведені у додатку В, таблиця В7.

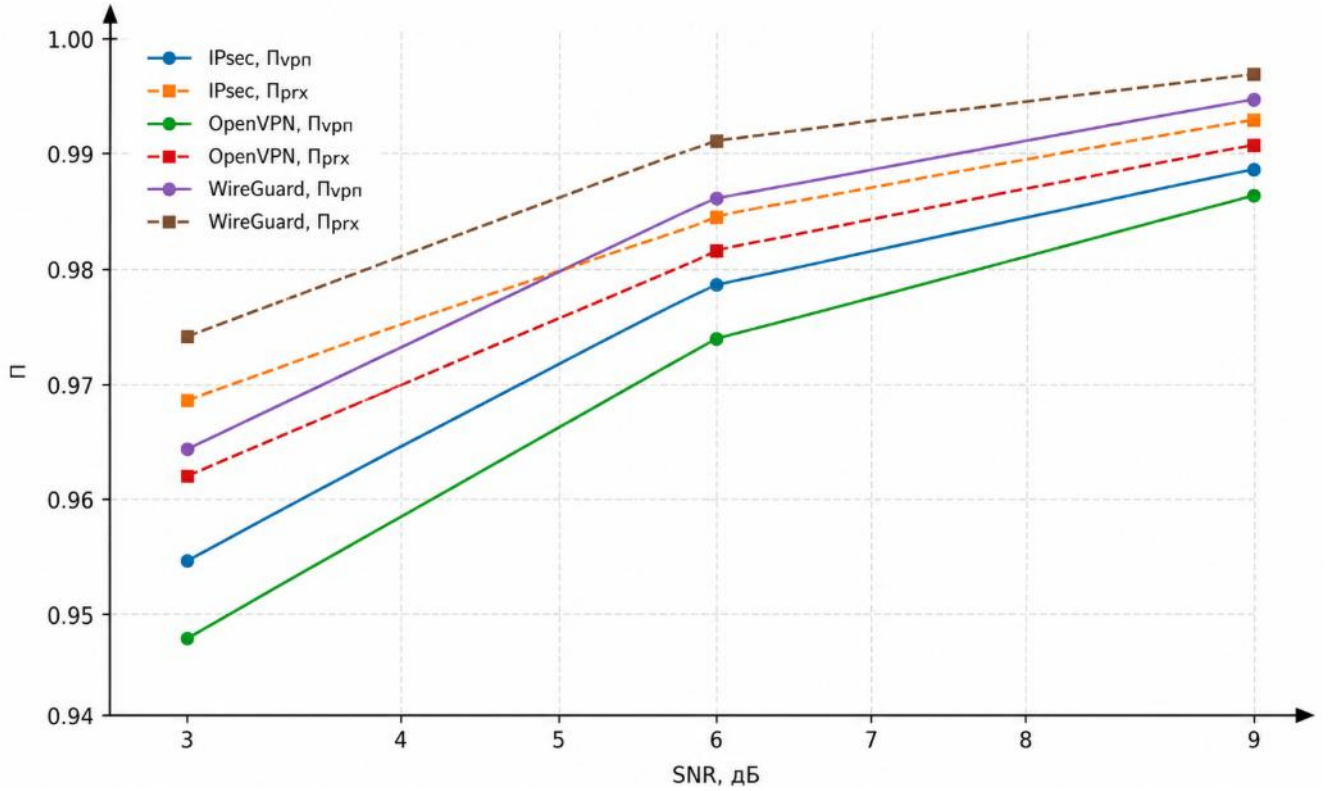


Рисунок 4.6 – Порівняння $П_{vpn}$ та $П_{prx}$ для профілів IPsec, OpenVPN і WireGuard за різних умов каналу

Насамперед було оцінено надійність доставки даних. Отримані результати показали, що для всіх профілів із φ≥0,2 значення $П_{e2e}$ перевищувало 0,95, тобто відповідало встановленим вимогам до успішної доставки та відновлення прикладних даних. Натомість сценарії без використання FEC демонстрували значно гірший результат: у таких режимах $П_{e2e}$<0,6, тому їх слід вважати непридатними для забезпечення стабільного функціонування системи в умовах деградації каналу. У цілому зі збільшенням φ надійність доставки зростала майже лінійно до граничного рівня, після чого спостерігалося насичення, коли подальше збільшення надлишковості вже не давало пропорційного виграшу. Це свідчить про наявність практично доцільної робочої області параметрів FEC, у якій досягається потрібний рівень $П_{e2e}$ без надмірного збільшення накладних витрат.

Другим ключовим показником виступала затримка доставки. Встановлено, що порівняно з профілями без FEC модулі кодування і декодування додавали

приблизно 10–20 % до сумарної затримки, що в абсолютному вираженні становило близько 20–30 мс. Проте навіть за такого зростання часові характеристики залишалися в межах заданих цілей. Важливо, що основний внесок у зростання затримки формувався не лише операціями FEC, а й буферизацією, шифруванням та службовими подіями тунелювання. Зокрема, у процесі роботи інтерфейсів спостерігалися короткочасні імпульси затримки під час handshake-процедур та оновлення ключів, однак вони згладжувалися завдяки використанню асинхронної черги пакетів і не призводили до втрати працездатності системи. Таким чином, зростання τ_{95} мало керований характер і не руйнувало загальну якість сервісу.

Третій блок оцінювання стосувався ефективності використання мережевого ресурсу, яку в роботі доцільно інтерпретувати через goodput на рівні застосунку. Експериментальні результати показали, що зі збільшенням φ корисна швидкість доставки закономірно зменшувалася, оскільки частина смуги пропускання витрачалася на передавання repair-пакетів і службових заголовків. Зокрема, для профілю φ=0,3 goodput був приблизно на 15 % нижчим, ніж для профілю φ=0,05. Водночас навіть у такому режимі загальна пропускна здатність у VPN-сценаріях залишалася прийнятною і перевищувала 8 Мбіт/с. Це означає, що підвищення надійності досягалося не за рахунок повної втрати ефективності каналу, а в межах керованого компромісу між доставкою, затримкою та накладними витратами профілю. Саме така постановка узгоджується з критеріями, сформульованими раніше для goodput і вартості профілю.

Окремо було проаналізовано витрати обчислювальних ресурсів. Найбільше навантаження на процесор зафіксовано для конфігурації IPsec+WireGuard при φ=0.3 , де використання CPU сягало приблизно 70 % ресурсу однієї віртуальної машини. Для профілів із φ≤0,1 завантаження процесора залишалося нижчим за 40 %, що свідчить про значно м’якший режим обчислювальної експлуатації. Отже, підвищення надлишковості та криптографічної складності профілю неминуче впливає на u_{cpu} , однак у межах досліджених сценаріїв ці витрати не виходили за межі, які можна вважати прийнятними для сучасного обладнання. Це дозволяє

зробити висновок, що реалізовані моделі не лише забезпечують потрібний рівень надійності, а й залишаються практично здійсненними з погляду ресурсного навантаження.

Для оцінювання впливу коефіцієнта надлишковості FEC φ на пропускну здатність системи та витрати обчислювальних ресурсів було проведено серію експериментів для профілів IPsec, OpenVPN і WireGuard. У ході дослідження аналізувалися значення корисної пропускної здатності goodput та рівень завантаження процесора u_{cpu} при зміні коефіцієнта надлишковості в діапазоні від 0 до 0,3. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями відповідних показників. Це дозволило оцінити компроміс між підвищенням надійності передачі даних за рахунок FEC та пов'язаними з цим втратами пропускної здатності й додатковими обчислювальними витратами. Результати наведені у додатку В, таблиця В8.

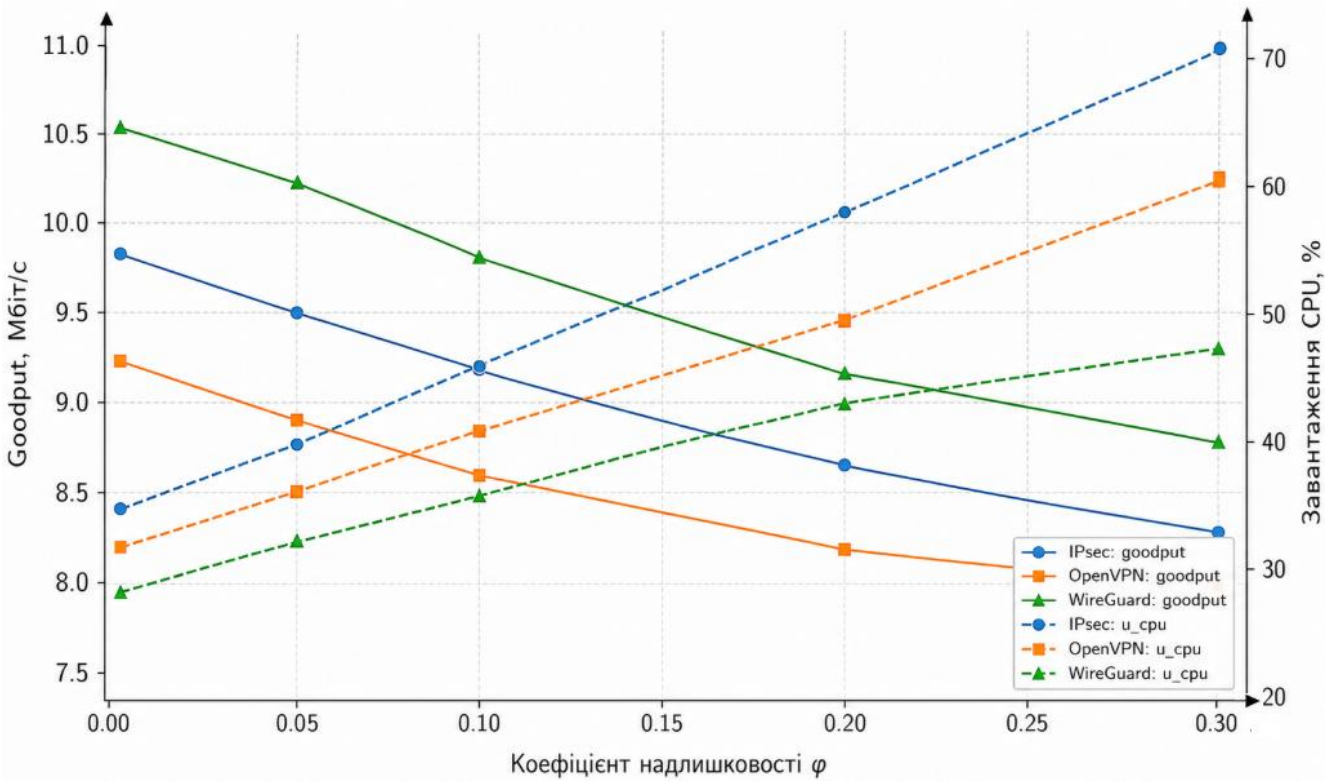


Рисунок 4.7 – Залежність goodput та завантаження CPU від коефіцієнта надлишковості φ для профілів IPsec, OpenVPN і WireGuard

Додатково встановлено, що відмінності між VPN-профілями проявляються не лише у значеннях τ_{95} та G_{app} в усталеному режимі, а і в часі входу системи у захищений стан, який характеризується метрикою τ_{SA}. Для сценаріїв із короткими сеансами або частими перевстановленнями тунелю саме τ_{SA} стає суттєвим чинником загальної ефективності, оскільки визначає часові витрати до початку корисного передавання. Тому оцінювання профілів IPsec, OpenVPN та WireGuard доцільно здійснювати за сукупністю показників τ_{SA}, τ_{95}, G_{app}, $П_{e2e}$ та Ω_{tot}, а не лише за характеристиками усталеного обміну.

Узагальнюючи результати оцінювання, можна стверджувати, що запропонована гібридна інформаційна технологія демонструє збалансовані показники функціонування. З одного боку, введення FEC помітно підвищує $П_{e2e}$ і забезпечує стійке відновлення прикладних даних навіть у несприятливих умовах каналу. З іншого боку, таке підвищення супроводжується помірним зростанням τ_{95}, зменшенням goodput та збільшенням u_{cpu}, однак ці зміни залишаються в допустимих межах. Отже, для практичних цілей найбільш доцільними слід вважати профілі з помірною надлишковістю, насамперед у діапазоні $\varphi \approx 0{,}2–0{,}3$, оскільки саме в цій області досягається найкраще співвідношення між надійністю доставки, затримкою, ефективністю використання каналу та ресурсними витратами.

4.4 Аналіз ефективності реалізованих моделей і методів

Експериментальні результати підтвердили ефективність запропонованих моделей і методів побудови гібридної інформаційної технології. Аналіз показав, що поєднання механізмів завадостійкого кодування, захищеного тунелювання та адаптивного керування параметрами передавання забезпечує суттєве підвищення надійності доставки без критичного погіршення часових характеристик або неприйнятного зростання ресурсних витрат. Це означає, що запропоновані рішення є ефективними не лише на рівні окремих алгоритмів, а й у межах цілісної багаторівневої системи, де результат визначається узгодженою роботою FEC, VPN

та оверлейного маршрутизатора. Такий висновок узгоджується із загальною логікою розділу 4, у якому практично перевіряються ті виходи, що були закладені у функціональній IDEF0-моделі системи, а саме передані та відновлені дані, показники надійності, результати контролю цілісності та аналітичні дані для оцінювання якості.

Додатково було оцінено показник τ_{setup}, який характеризує часові витрати на підготовку захищеного каналу до передавання корисних даних. Отримані результати показали, що значення τ_{setup} залежить від типу захищеного оверлею та складності процедури його ініціалізації. Для профілів із простішою схемою встановлення каналу час входу у захищений режим є меншим, тоді як профілі з багатокроковим узгодженням параметрів характеризуються більшими початковими часовими витратами. Це дозволяє враховувати τ_{setup} разом із τ_{95}, G_{app} та $П_{\text{e2e}}$ при порівнянні ефективності реалізованих профілів.

Для оцінювання часових витрат на ініціалізацію захищеного каналу було проведено серію експериментів для профілів IPsec, OpenVPN, WireGuard та XRay. У процесі дослідження визначався показник τ_{setup}, який характеризує інтервал часу від моменту запуску процедури встановлення захищеного з'єднання до готовності системи до передавання корисних даних. Для кожного профілю виконувалося понад 100 незалежних запусків із подальшим усередненням отриманих результатів. Це дозволило оцінити вплив особливостей процедур узгодження параметрів, обміну службовими повідомленнями та ініціалізації криптографічних механізмів на швидкість підготовки захищеного каналу. Результати наведено у додатку В, таблиця В9.

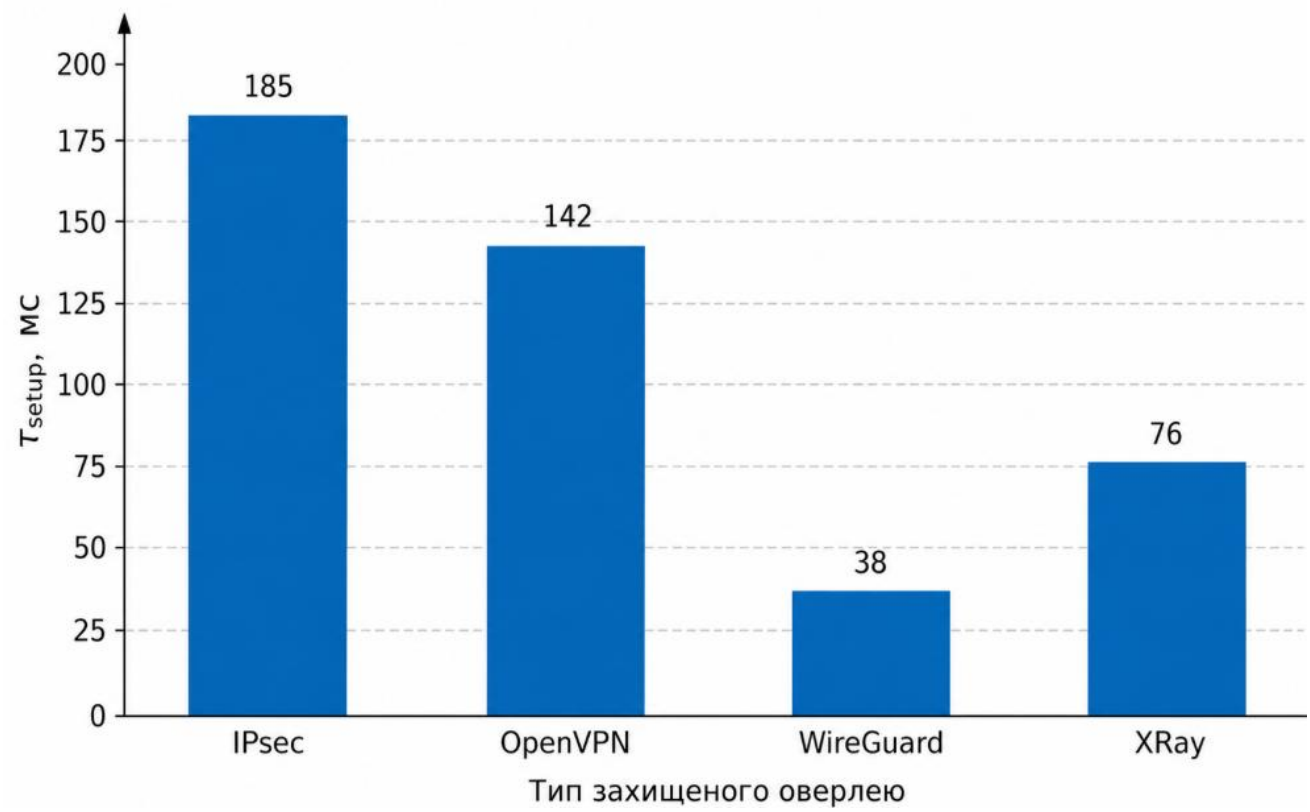


Рисунок 4.8 – Порівняння часу підготовки захищеного каналу τ_{setup} для профілів IPsec, OpenVPN, WireGuard та XRay

Найбільш наочно ефективність запропонованого підходу проявляється у порівняльних сценаріях, де одна й та сама конфігурація мережевого середовища досліджується за наявності й за відсутності FEC. Так, у наведеному експерименті поєднання профілю IPsec з φ=0,2 дало $П_{e2e}$=0,97 при τ_{95}=130мс, тоді як аналогічний профіль без кодування мав лише $П_{e2e}$=0,45 при τ_{95}=110 мс. Це означає, що введення FEC забезпечило приріст надійності на 0,52, тобто на 52 процентних пункти, при зростанні 95-го процентиля затримки лише приблизно на 18 %. У відносному вираженні показник наскрізної доставки збільшився більш ніж у два рази. Такий результат є принципово важливим, оскільки демонструє: навіть помірна надлишковість дозволяє перевести систему з режиму нестійкого функціонування у режим практично повноцінної доставки даних, а ціна такого переходу в часовому сенсі є порівняно невеликою.

Для оцінювання впливу коефіцієнта надлишковості FEC φ на коефіцієнт успішної доставки $П_{e2e}$ було проведено серію експериментів для профілів WireGuard, IPsec та OpenVPN за значень SNR 3 дБ і 6 дБ. У процесі дослідження коефіцієнт надлишковості змінювався в діапазоні від 0 до 0,5, що дозволило оцінити ефективність використання додаткових repair-пакетів в умовах різної якості каналу. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі передачі даних, а наведені результати є усередненими значеннями коефіцієнта успішної доставки $П_{e2e}$. Результати наведені у додатку В, таблиця В10.

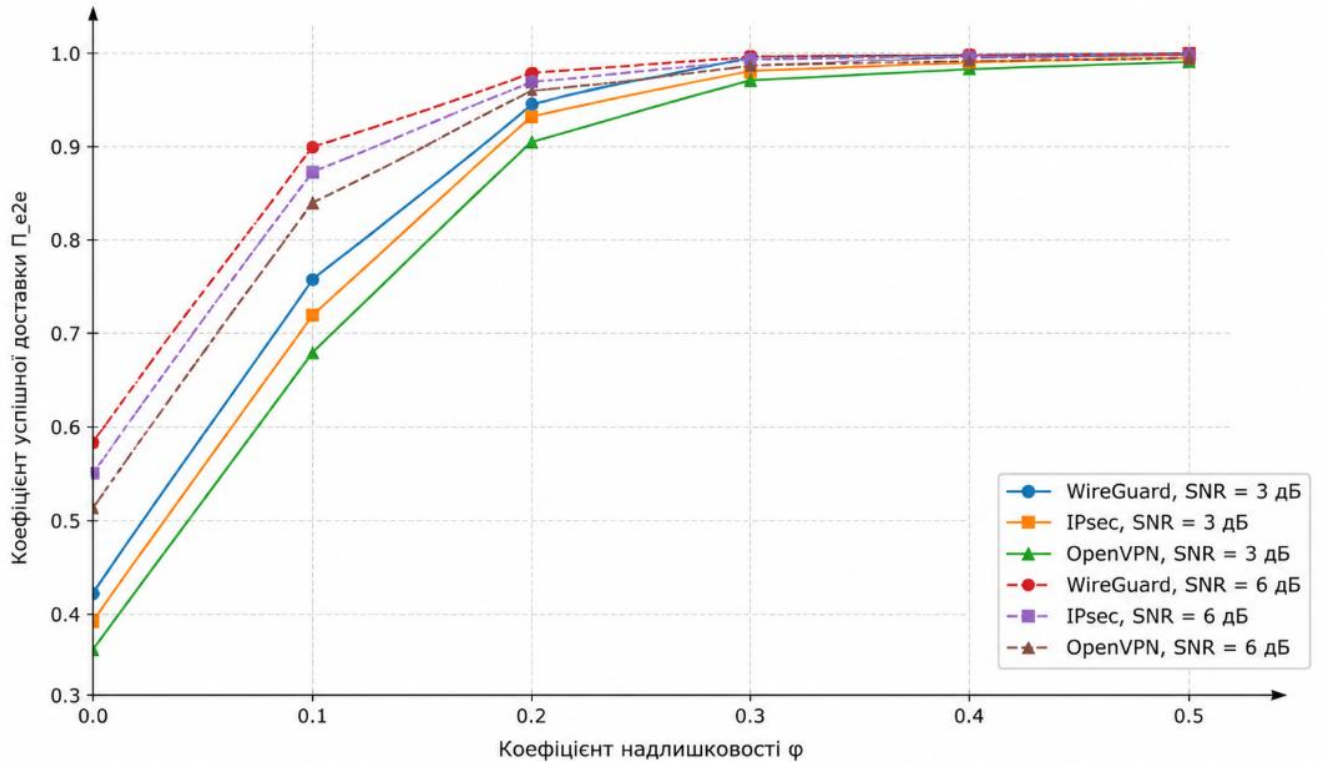


Рисунок 4.9 – Залежність коефіцієнта успішної доставки $П_{e2e}$ від коефіцієнта надлишковості φ для профілів IPsec, OpenVPN і WireGuard при SNR=3та 6 дБ.

Окремий блок експериментального дослідження було присвячено оцінюванню бітової ймовірності помилки BER у досліджуваних профілях передавання. Для кожної конфігурації, що задавалася поєднанням значень SNR, коефіцієнта надлишковості φ, типу захищеного оверлею та параметрів каналу,

визначалося значення BER як частка бітів, прийнятих із помилкою. Це дозволило доповнити оцінювання наскрізних метрик $П_{e2e}$, τ_{95} і G_{app} характеристикою фізичного рівня, яка безпосередньо відображає якість передавання в умовах завад.

Результати показали, що зі зменшенням SNR значення BER закономірно зростає, однак застосування FEC із помірними значеннями φ дозволяє істотно зменшити частку бітових помилок порівняно з режимом без додаткової надлишковості. Для профілів із VPN-оверлеєм це особливо важливо, оскільки навіть незначні пошкодження бітового потоку можуть призводити до непридатності цілих зашифрованих пакетів для подальшого коректного відновлення. У цьому сенсі показник BER виступає базовою фізичною характеристикою, яка пояснює подальшу поведінку метрик вищого рівня, насамперед $П_{e2e}$.

Для дослідження впливу якості каналу на ймовірність виникнення бітових помилок було проведено серію експериментів для профілів IPsec, OpenVPN, WireGuard та XRay. У ході дослідження аналізувалася залежність BER від відношення сигнал/шум SNR для режиму без використання FEC, а також для режимів із коефіцієнтами надлишковості φ=0,10 та φ=0,20. Значення SNR змінювалося в діапазоні від 0 до 10 дБ. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями BER, отриманими за всіма серіями вимірювань. Результати наведені в додатку В, таблиці В11-В14.

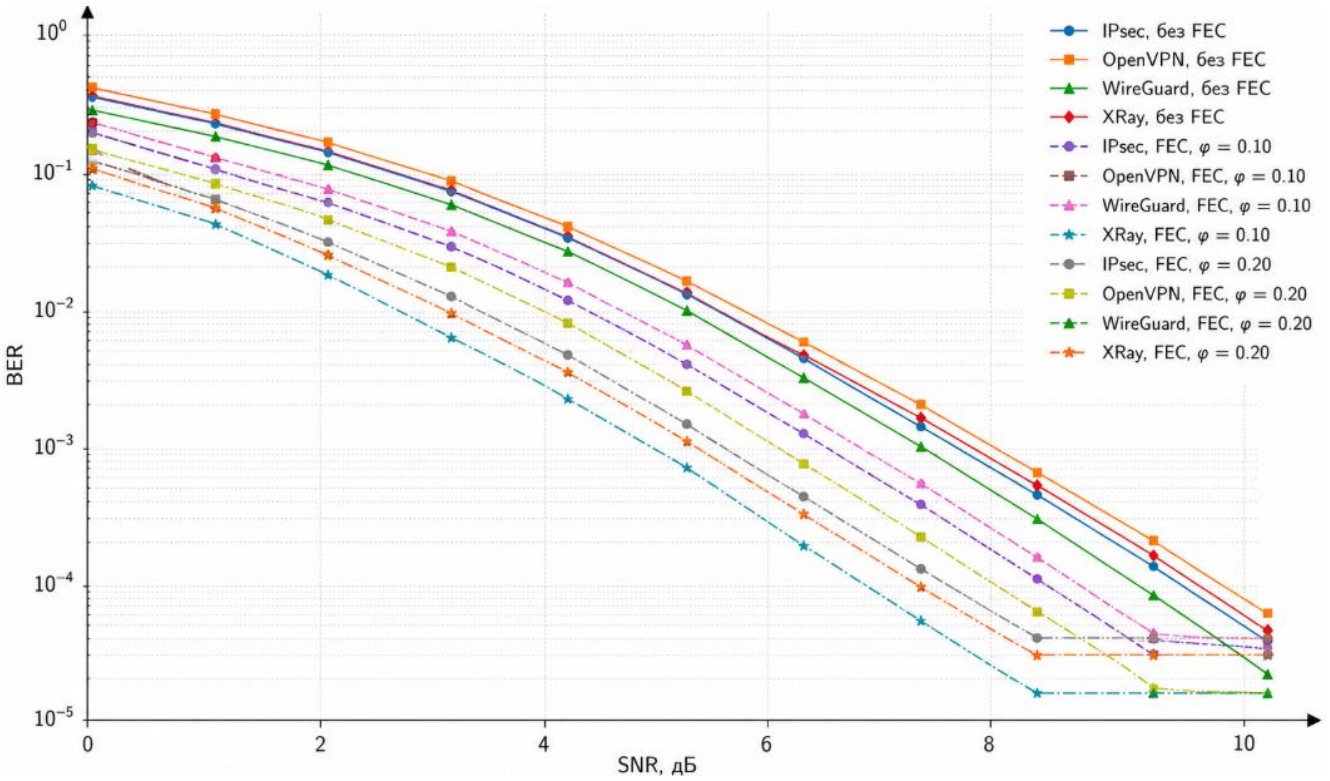


Рисунок 4.10. – Залежності BER(SNR) для профілів без FEC і з FEC за різних значень φ та для різних типів захищеного оверлею

Виграш кодування G_{code} визначався як різниця між значеннями SNR, за яких профілі без FEC і з FEC забезпечували однаковий рівень помилок. Для всіх досліджуваних профілів отримано додатні значення G_{code}, величина яких залежить від φ та типу захищеного оверлею.

Для оцінювання ефективності використання FEC було проведено серію експериментів з визначення кодового виграшу G_{code} для профілів IPsec, OpenVPN, WireGuard та XRay. Кодовий виграш визначався як різниця між значеннями SNR, за яких системи без FEC та з FEC забезпечували однаковий рівень BER. У дослідженні розглядалися значення коефіцієнта надлишковості φ від 0 до 0,3. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями кодового виграшу. Результати наведені у додатку В, таблиця В15.

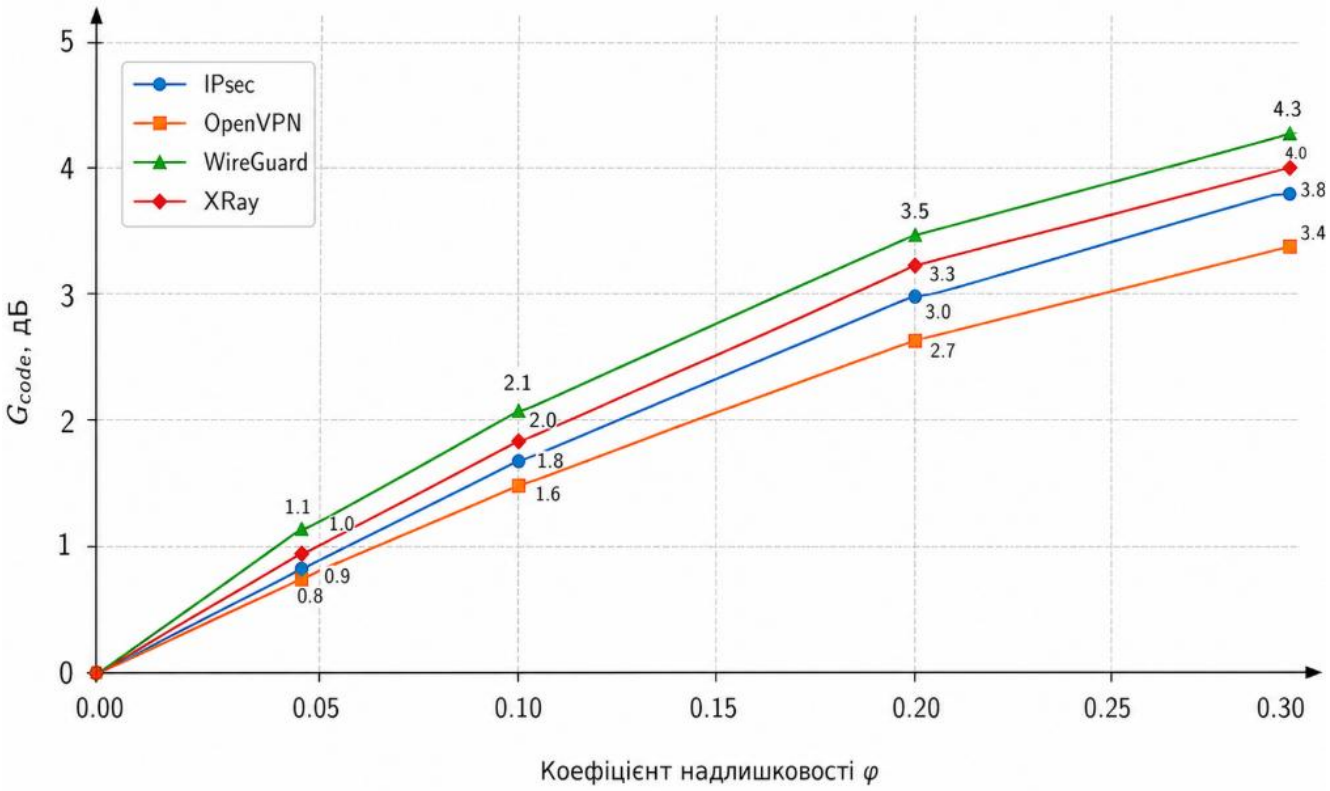


Рисунок 4.11 – Виграш кодування G_{code} для профілів IPsec, OpenVPN, WireGuard та XRay за різних значень φ

Узагальнення результатів для різних сценаріїв показує, що найбільший ефект від упровадження FEC досягається в тих режимах, де сам по собі VPN-тунель не здатний компенсувати втрати каналу. У стабільних умовах виграш від кодування є помірним, оскільки базовий рівень доставки й без того достатньо високий. Проте зі зниженням якості каналу або зі зростанням частки втрат роль FEC різко зростає: він починає виконувати функцію не допоміжного, а визначального механізму забезпечення працездатності системи. Водночас отримані результати свідчать, що найбільш доцільними є не максимальні, а збалансовані значення φ, оскільки після досягнення робочої області подальше збільшення надлишковості вже не дає пропорційного виграшу у $П_{e2e}$, зате погіршує goodput, збільшує τ_{95} та підвищує навантаження на процесор. Отже, ефективність запропонованих методів полягає не у простому нарощуванні захисних механізмів, а у досягненні збалансованого режиму роботи системи.

Окремого аналізу потребує адаптивний метод керування, оскільки саме він забезпечує збереження цільових показників у змінних мережевих умовах. У тесті з динамічною зміною параметрів каналу встановлено, що контролер здатний автоматично змінювати коефіцієнт надлишковості φ і вибір outbound-профілю так, щоб утримувати $П_{e2e}$>0,95 навіть при погіршенні умов передавання. Зокрема, під час зниження SNR з 6 до 3 дБ система підвищувала рівень корекційної надлишковості та переходила на альтернативний маршрут у V2Ray/XRay. У результаті 95-й процентиль затримки залишався нижчим за встановлений поріг, тоді як без адаптації ті самі умови призводили б до помітного падіння надійності доставки й погіршення часових характеристик. Це підтверджує, що адаптивний метод виконує не декоративну, а функціонально необхідну роль: він дозволяє не просто один раз підібрати прийнятний профіль, а підтримувати якість функціонування системи в режимі поточних змін середовища.

Для оцінювання ефективності адаптивного методу керування було проведено серію експериментів у динамічному сценарії зі зміною параметрів каналу передавання. У процесі дослідження значення SNR змінювалося від 6 до 3 дБ із подальшим відновленням початкових умов. Адаптивний контролер автоматично змінював коефіцієнт надлишковості FEC φ та виконував вибір профілю передавання відповідно до поточного стану каналу. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями параметрів функціонування системи. Результати наведені у додатку В, таблиця В16.

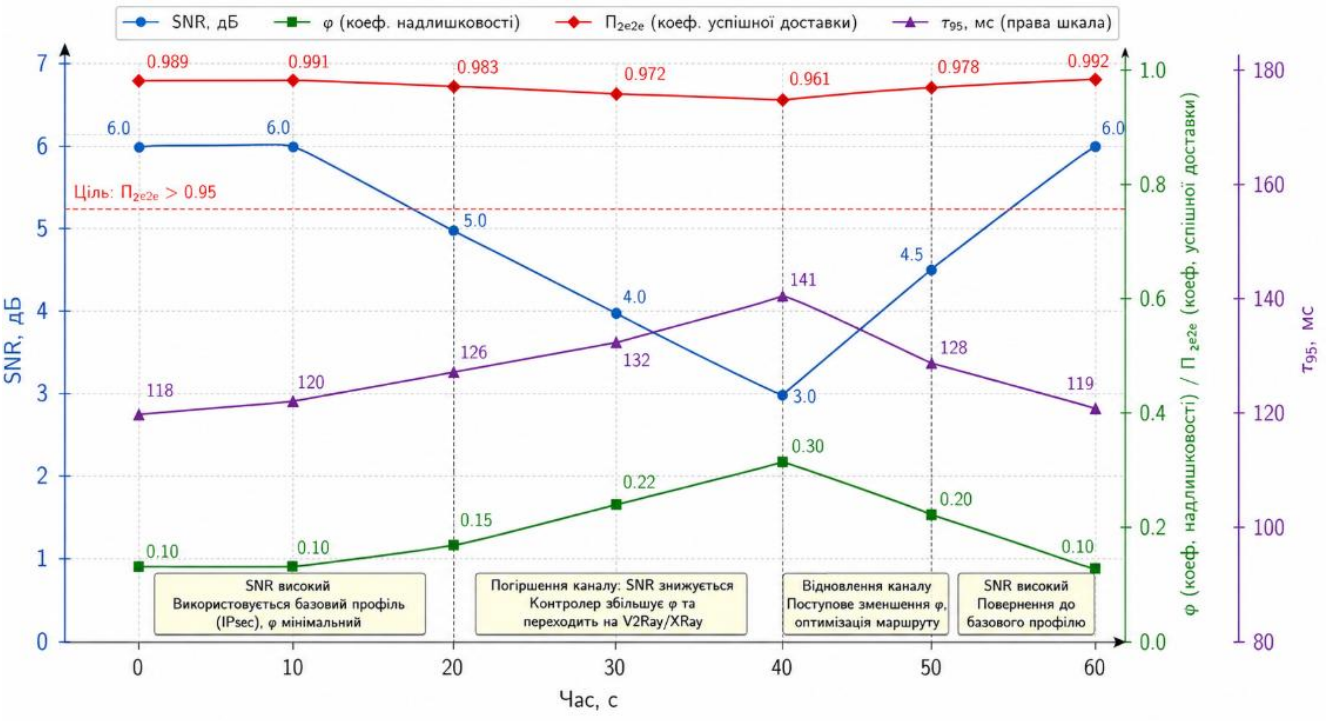


Рисунок 4.12 – Часові залежності SNR, коефіцієнта надлишковості φ та коефіцієнта успішної доставки $П_{e2e}$ при роботі адаптивного методу керування.

Важливо також підкреслити, що ефективність реалізованих методів не зводиться лише до збільшення надійності доставки. Аналіз попередніх підрозділів показав, що результати повинні інтерпретуватися комплексно – з урахуванням затримки, goodput, фрагментації та ресурсної вартості профілю. Саме в такій багатокритеріальній постановці запропоновані моделі демонструють свою практичну доцільність. FEC підвищує $П_{e2e}$, але не руйнує SLA за затримкою; адаптивна пакетизація дозволяє утримувати фрагментацію на мінімальному рівні; а керування маршрутом через XRay/V2Ray забезпечує додатковий ступінь гнучкості у виборі транспортного середовища. У сукупності це дає підстави стверджувати, що запропонована інформаційна технологія не просто працює, а працює ефективно саме як інтегрована система, у якій кожний модуль компенсує обмеження інших. Звідси випливає і головний практичний висновок: найбільшу ефективність демонструють профілі з помірною надлишковістю та активним

адаптивним керуванням, тоді як крайні режими – без FEC або з надмірною надлишковістю – є менш вигідними з точки зору сукупного балансу метрик.

Окремо було оцінено ефективний корисний розмір пакета M_{eff}, який характеризує верхню межу прикладного навантаження без систематичної фрагментації в межах вибраного профілю. Експериментальні результати показали, що значення M_{eff} змінюється залежно від типу VPN-оверлею та частки службових заголовків, а його врахування під час вибору L_{app} дозволяє уникати різкого зростання ξ_{frag}. Таким чином, показник M_{eff} підтверджує практичну придатність методу керування пакетизацією та узгоджується з вимогою безфрагментаційного передавання.

Для оцінювання ефективного корисного розміру пакета M_{eff} було проведено серію експериментів для профілів IPsec, OpenVPN та WireGuard. У ході дослідження визначався максимальний обсяг прикладних даних, який може бути переданий без виникнення систематичної фрагментації з урахуванням службових заголовків VPN-оверлею та транспортних протоколів. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями ефективного корисного розміру пакета. Це дозволило оцінити вплив накладних витрат різних профілів на доступний обсяг корисного навантаження та перевірити ефективність методу адаптивної пакетизації. Результати наведені у додатку В, таблиця В17.

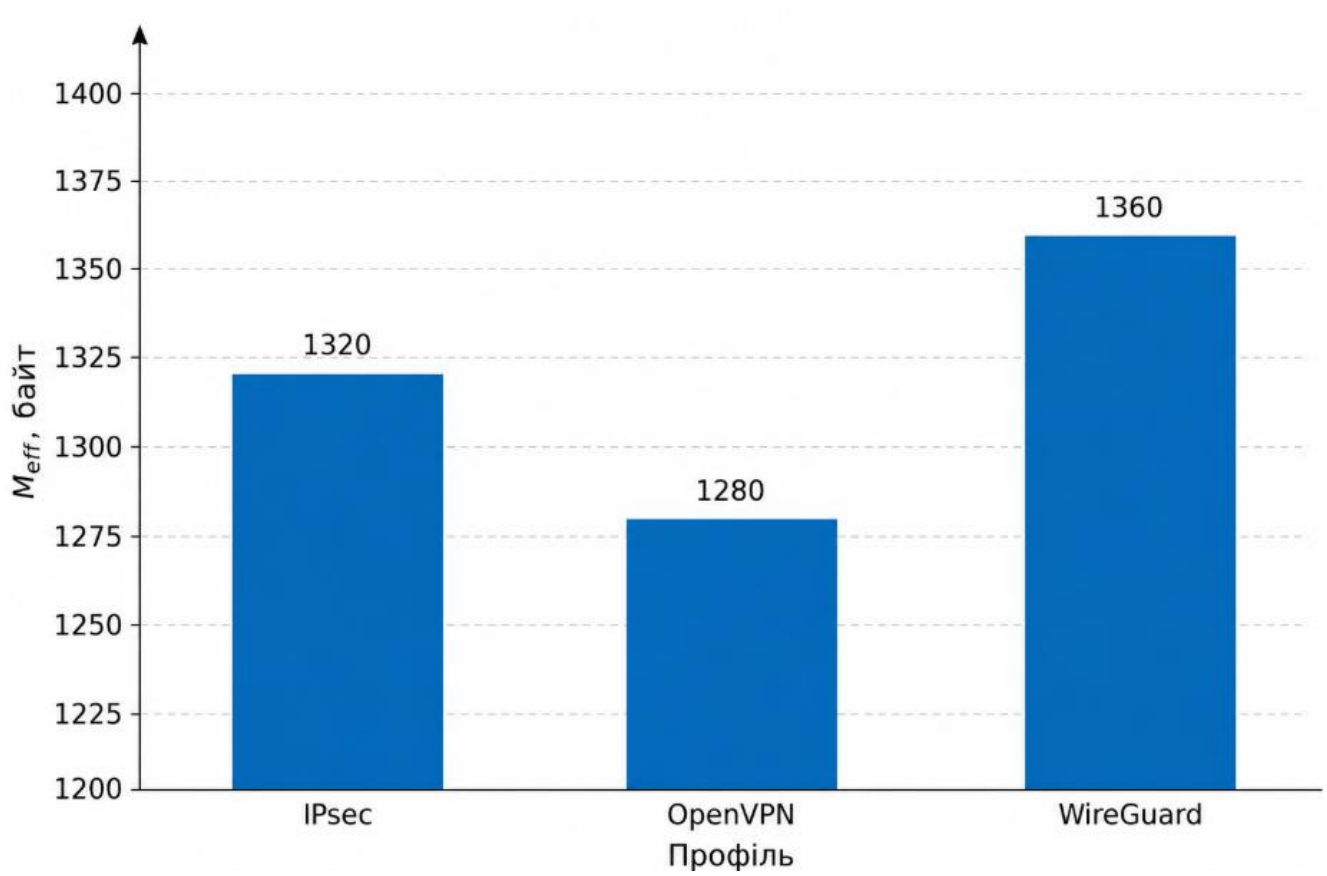


Рисунок 4.13 – Порівняння значень M_{eff} для профілів IPsec, OpenVPN та WireGuard.

З позицій ефективності важливою є не лише оцінка абсолютних значень goodput або затримки, а й аналіз структури накладних витрат профілю. Для цього було розглянуто інтегральний показник ефективності η, а також розкладено сумарний оверхед h_{tot} на складові h_{FEC}, h_{VPN}, h_{prx}і h_{net}. Отримані результати показали, що зі збільшенням φ виграш у надійності досягається ціною зростання h_{FEC}, тоді як вибір типу тунелю найбільше впливає на h_{VPN}. У свою чергу, proxy-рівень формує додаткову частку h_{prx}, яка є прийнятною лише за умови збереження достатнього значення η. Отже, показник η доцільно розглядати як інтегральну характеристику експлуатаційної доцільності профілю після перевірки його допустимості за критеріями надійності, затримки та фрагментації.

Для оцінювання інтегральної ефективності захищених профілів було проведено серію експериментів для IPsec, OpenVPN та WireGuard. У процесі

дослідження аналізувалися складові сумарного оверхеду h_{tot}, які включали мережеві накладні витрати h_{net}., надлишковість FEC h_{FEC}, накладні витрати VPN-рівня h_{VPN} та витрати proxy-рівня h_{prx}. Додатково визначався інтегральний показник ефективності η, який характеризує співвідношення між досягнутим рівнем якості передачі та сумарними накладними витратами профілю. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями відповідних показників. Результати наведені у додатку В, таблиця В18.

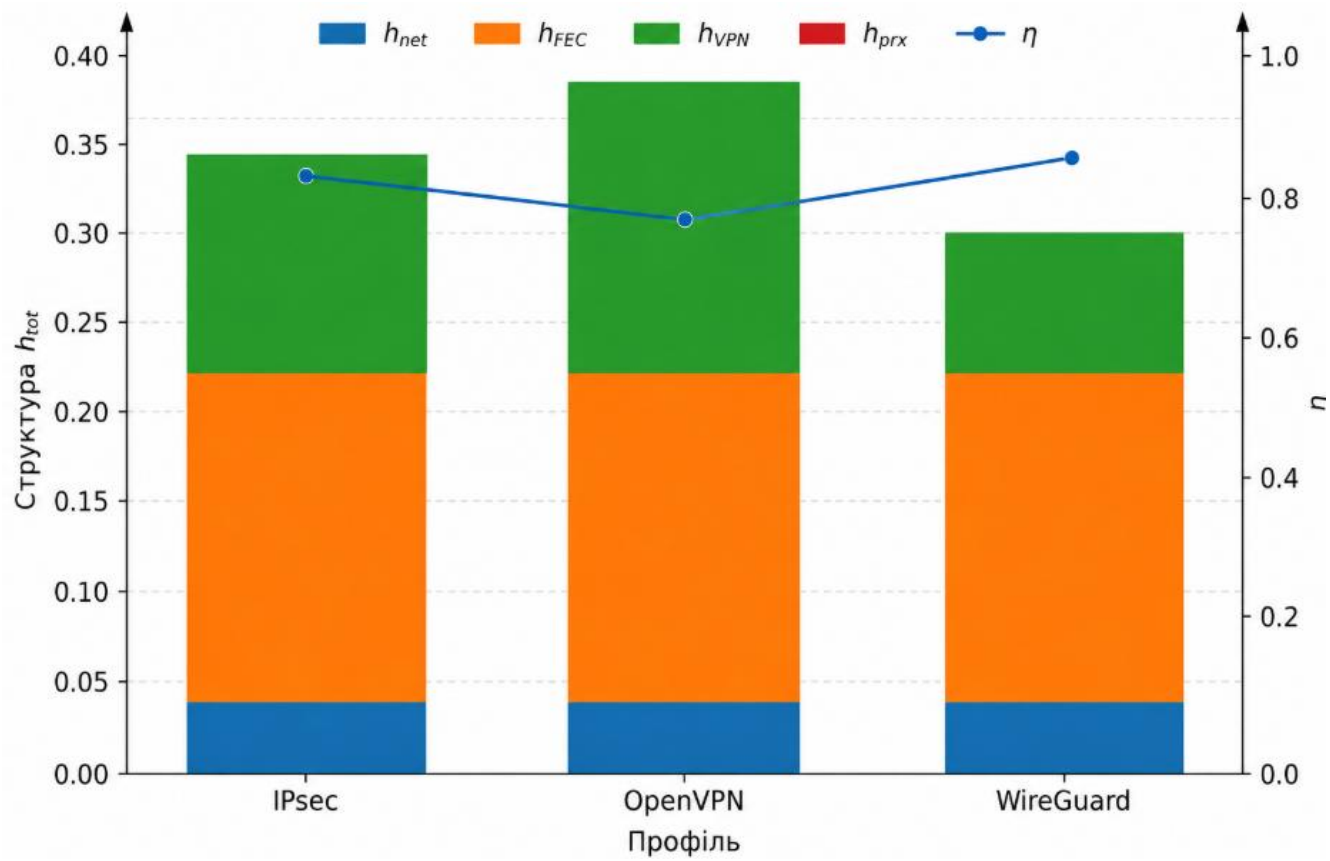


Рисунок 4.14 – Порівняння η та структури h_{tot} для профілів IPsec, OpenVPN та WireGuard

Отже, аналіз експериментальних даних підтверджує основну гіпотезу роботи: поєднання завадостійкого кодування з VPN-тунелюванням і адаптивним

вибором параметрів дозволяє суттєво підвищити надійність і стійкість передавання даних у мережах без непропорційного погіршення якості сервісу. Саме це і свідчить про ефективність реалізованих моделей і методів у межах запропонованої гібридної інформаційної технології.

4.5 Порівняльний аналіз результатів та узагальнення

Порівняльний аналіз експериментальних результатів показав, що найбільш ефективними є конфігурації, у яких механізми завадостійкого кодування поєднуються із захищеним VPN-оверлеєм. Використання лише VPN забезпечує криптографічний захист передавання, однак у несприятливих умовах каналу не гарантує потрібного рівня успішної доставки прикладних даних. Натомість додавання FEC дозволяє суттєво підвищити коефіцієнт успішної доставки Π_{e2e}, особливо в сценаріях зі зниженим SNR та підвищеними втратами пакетів. Це підтверджує доцільність об'єднання криптографічного захисту та корекційної надлишковості в межах єдиної гібридної інформаційної технології.

Більш детальний аналіз показав, що перевага комбінованих FEC–VPN-профілів полягає у підвищенні ймовірності успішної доставки пакетів, зменшенні частки помилково декодованих блоків та забезпеченні стабільності передачі даних в умовах втрат і мережевих завад. Зокрема, для ефективних конфігурацій характерними є високі значення P_{dec} за малого розходження з P_{dec}^{mdl} близькі до одиниці значення Π_{vpn} та Π_{prx}, дотримання умови L_{app} без систематичної фрагментації, а також прийнятний баланс між h_{tot} і η. Саме сукупний розгляд цих показників дозволяє вважати вибрані профілі не лише працездатними, а й практично доцільними для використання в реальних мережевих умовах.

Для оцінювання впливу коефіцієнта надлишковості FEC на коефіцієнт успішної доставки Π_{e2e} було проведено серію експериментів для профілів IPsec, OpenVPN та WireGuard за фіксованого значення SNR = 3 дБ. У ході дослідження розглядалися три режими роботи: без використання FEC (φ=0), а також із коефіцієнтами надлишковості φ=0,2 та φ=0,3. Для кожної конфігурації

виконувалося понад 100 незалежних запусків моделі передачі даних, а наведені результати є усередненими значеннями коефіцієнта успішної доставки $П_{e2e}$. Такий підхід дозволив оцінити внесок механізму FEC у забезпечення надійності доставки даних в умовах деградованого каналу. Результати наведені у додатку В, таблиця В19.

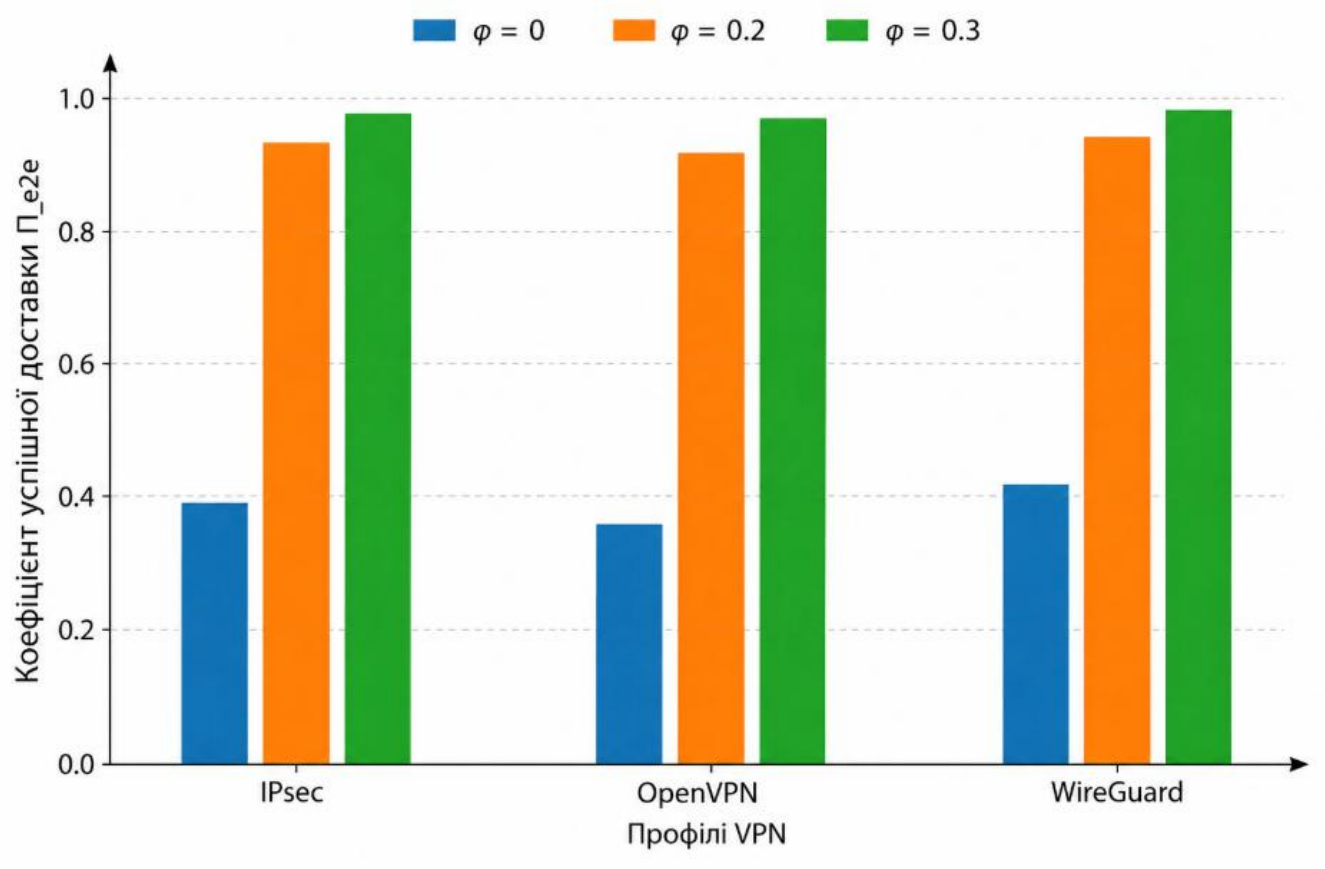


Рисунок 4.15 – Порівняння коефіцієнта успішної доставки $П_{e2e}$в для профілів IPsec, OpenVPN і WireGuard при SNR=3 дБ та різних значеннях коефіцієнта надлишковості

Додатково для фізичного рівня виконано оцінювання BER, FER та виграшу кодування для досліджуваних профілів. Для цього в тих самих тестових сценаріях, у яких аналізувалися $П_{e2e}$, $τ_{95}$, G_{app}, $Ω_{tot}$ та $ξ_{frag}$, фіксувалися залежності BER(SNR) та FER(SNR) для профілів без FEC і з FEC за однакових значень φ та незмінного типу захищеного оверлею. Одержані результати показали, що

застосування FEC зменшує BER та FER в усьому дослідженому діапазоні SNR, причому найбільш виражений ефект спостерігається в області зниженого SNR, де профілі без кодування переходять у режим нестійкого приймання. Виграш кодування оцінювався як різниця між значеннями SNR, потрібними для досягнення однакового цільового рівня BER або FER у профілях без FEC та з FEC. Це підтверджує, що поліпшення наскрізної доставки Π_{e2e} має безпосереднє підґрунтя на фізичному рівні: зі зменшенням BER і FER після застосування FEC знижується λ_{e2e} та підвищується ймовірність коректного відновлення прикладних даних.

Для оцінювання впливу FEC на характеристики фізичного рівня було проведено серію експериментів із визначення залежностей BER(SNR) та FER(SNR) для різних значень коефіцієнта надлишковості φ. У процесі дослідження значення SNR змінювалося в діапазоні від 0 до 10 дБ, а для кожної точки виконувалося понад 100 незалежних запусків моделі. Аналіз проводився для режиму без використання FEC та для профілів із коефіцієнтами надлишковості φ=0.10, φ=0.20 і φ=0.30. Наведені результати є усередненими значеннями бітової ймовірності помилки BER та ймовірності помилки кадру FER, отриманими за всіма серіями вимірювань. Результати наведені у додатку В, таблиця В20

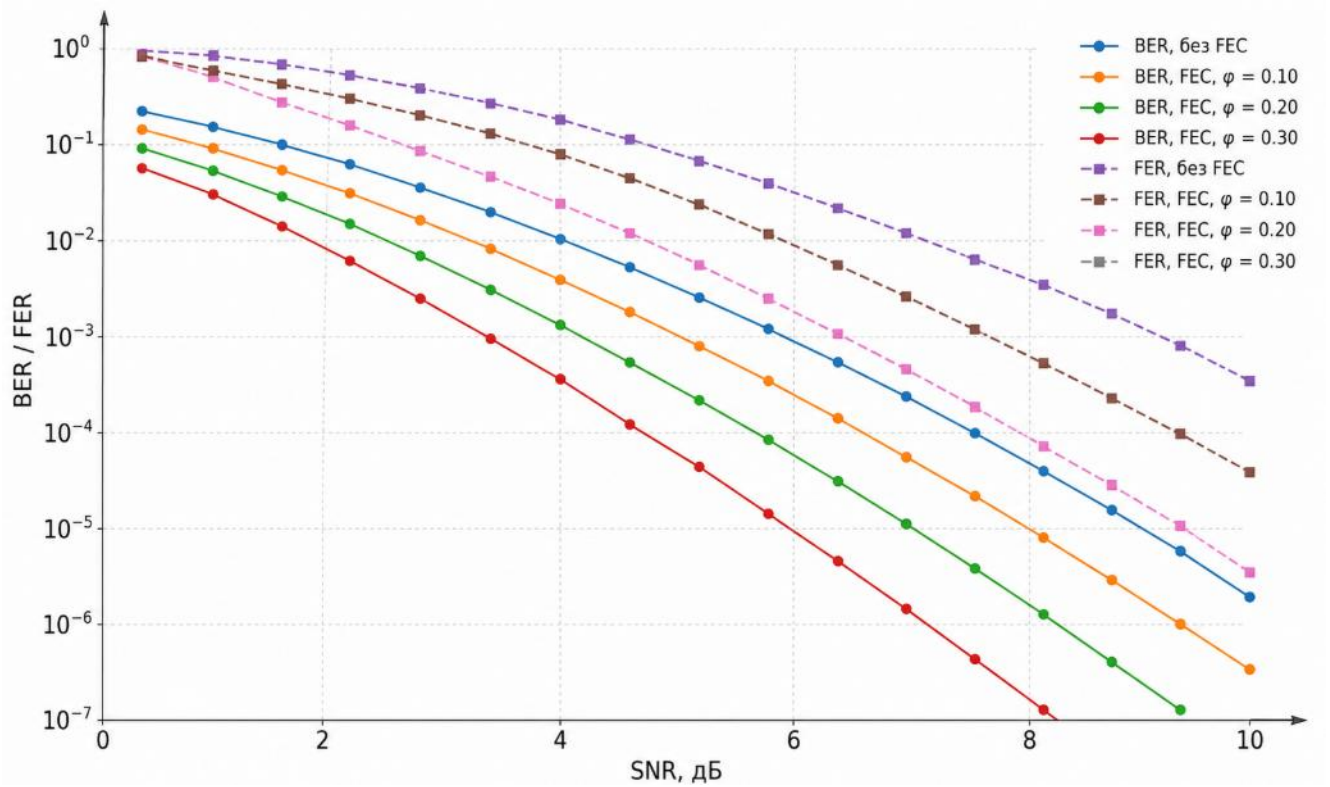


Рисунок 4.16 – Залежності BER(SNR) та FER(SNR) для профілів без FEC і з FEC при різних значеннях φ

Порівняння окремих VPN-профілів засвідчило, що WireGuard у середньому демонструє менші затримки, ніж OpenVPN, що пояснюється меншою складністю криптографічної та транспортної обробки. Водночас OpenVPN характеризується більшими накладними витратами й вищою чутливістю до фрагментації. IPsec, своєю чергою, займає проміжне положення, забезпечуючи більш збалансоване співвідношення між часовими характеристиками та стійкістю передавання. Разом із тим у всіх випадках збільшення φ приводить до зростання τ_{95}, але це зростання є помірним і компенсується покращенням надійності доставки.

Для оцінювання взаємозв'язку між затримкою доставки та рівнем фрагментації пакетів було проведено серію експериментів для профілів IPsec, OpenVPN та WireGuard. У ході дослідження коефіцієнт надлишковості FEC φ змінювався від 0 до 0,3, а для кожної конфігурації визначалися 95-й процентиль затримки τ_{95} та частка фрагментованих пакетів ξ_{frag}. Для кожної точки

виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями відповідних показників. Такий підхід дозволив оцінити компроміс між часовими характеристиками системи та ризиком виникнення фрагментації для різних VPN-профілів. Результати наведені у додатку В, таблиця В21.

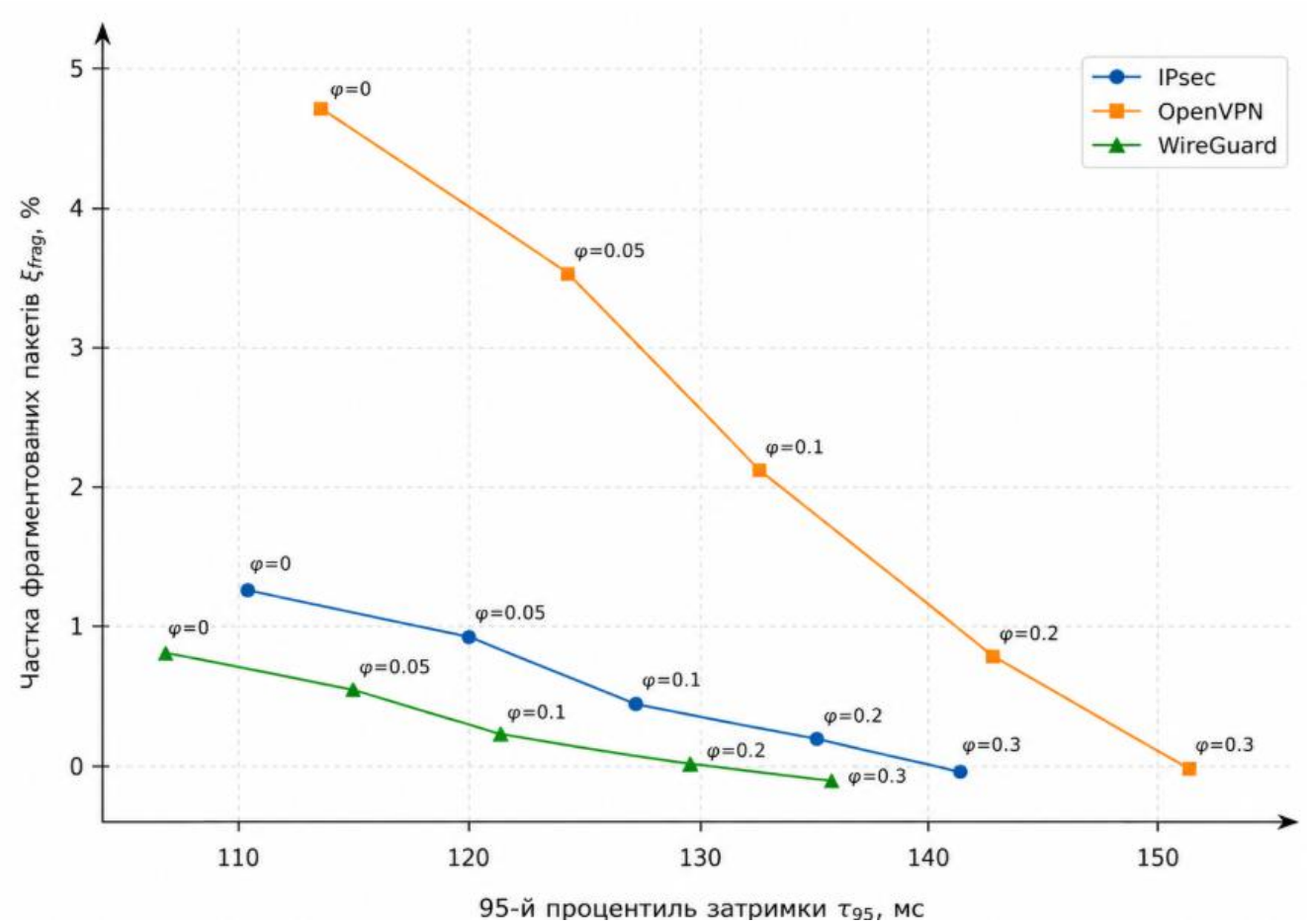


Рисунок 4.17 – Порівняння профілів IPsec, OpenVPN і WireGuard за показниками $\tau_{95} - \xi_{frag}$

Отримані результати також показали, що зростання надлишковості має межу практичної доцільності. При малих значеннях φ система не завжди забезпечує потрібний рівень $П_{e2e}$, тоді як надмірне збільшення φ знижує goodput і підвищує навантаження на процесор. Таким чином, найкращі результати досягаються не за максимального рівня FEC, а за помірної надлишковості, коли забезпечується

компроміс між надійністю, затримкою, пропускною здатністю та ресурсними витратами. У проведених експериментах саме профілі з φ≈0,2–0,3 виявилися найбільш збалансованими.

Для оцінювання компромісу між пропускною здатністю системи та обчислювальними витратами було проведено серію експериментів для профілів IPsec, OpenVPN та WireGuard. У ході дослідження коефіцієнт надлишковості FEC φ змінювався від 0 до 0,3, а для кожної конфігурації визначалися значення корисної пропускної здатності goodputgoodputgoodput та завантаження процесора u_{CPU},. Для кожної точки виконувалося понад 100 незалежних запусків моделі, а наведені результати є усередненими значеннями відповідних показників. Такий підхід дозволив оцінити вплив збільшення надлишковості на ефективність використання обчислювальних ресурсів і пропускну здатність системи. Результати наведені у додатку В, таблиця В22.

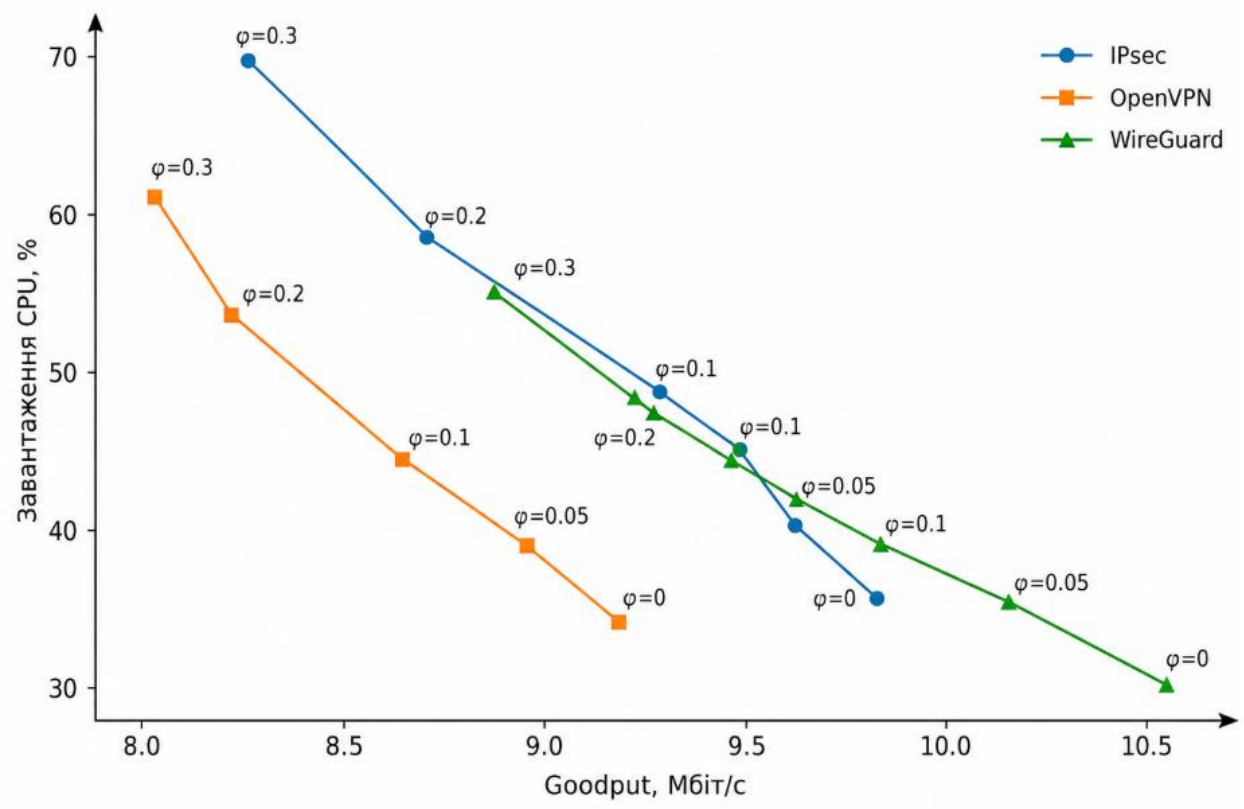


Рисунок 4.18 – Порівняння профілів IPsec, OpenVPN і WireGuard за показниками goodput та завантаження CPU

Важливим результатом є також підтвердження ефективності адаптивного керування. У сценаріях зі змінними умовами каналу система змінювала параметри φ та маршрут передавання так, щоб утримувати $П_{e2e}$ на цільовому рівні та не виходити за межі допустимих значень τ_{95}. Це свідчить про те, що запропоновані моделі і методи є ефективними не лише у статичних конфігураціях, а й у динамічних умовах функціонування.

Для формування базового сценарію було проведено серію експериментів без використання механізмів FEC та VPN-оверлеїв. Дослідження виконувалося в умовах поступового погіршення характеристик каналу шляхом збільшення ймовірності втрати пакетів та зниження якості фізичного середовища передавання. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі з подальшим усередненням результатів. У межах експерименту оцінювалися показники пропускної здатності (Throughput), затримки RTT, якості обслуговування QoS (MOS), бітової ймовірності помилки BER, кадрової ймовірності помилки FER та інтегральний індекс стабільності каналу.

У дослідженні використовувалися значення SNR від 10 до 20 дБ, імовірність втрати пакетів p_{loss} від 0 до 10 %, середній рівень мережевих завад, відсутність механізмів FEC та відсутність VPN-оверлею. Передавання здійснювалося без додаткової надлишковості та без криптографічного тунелювання. Результати наведені у додатку В, таблиці В23-В24.

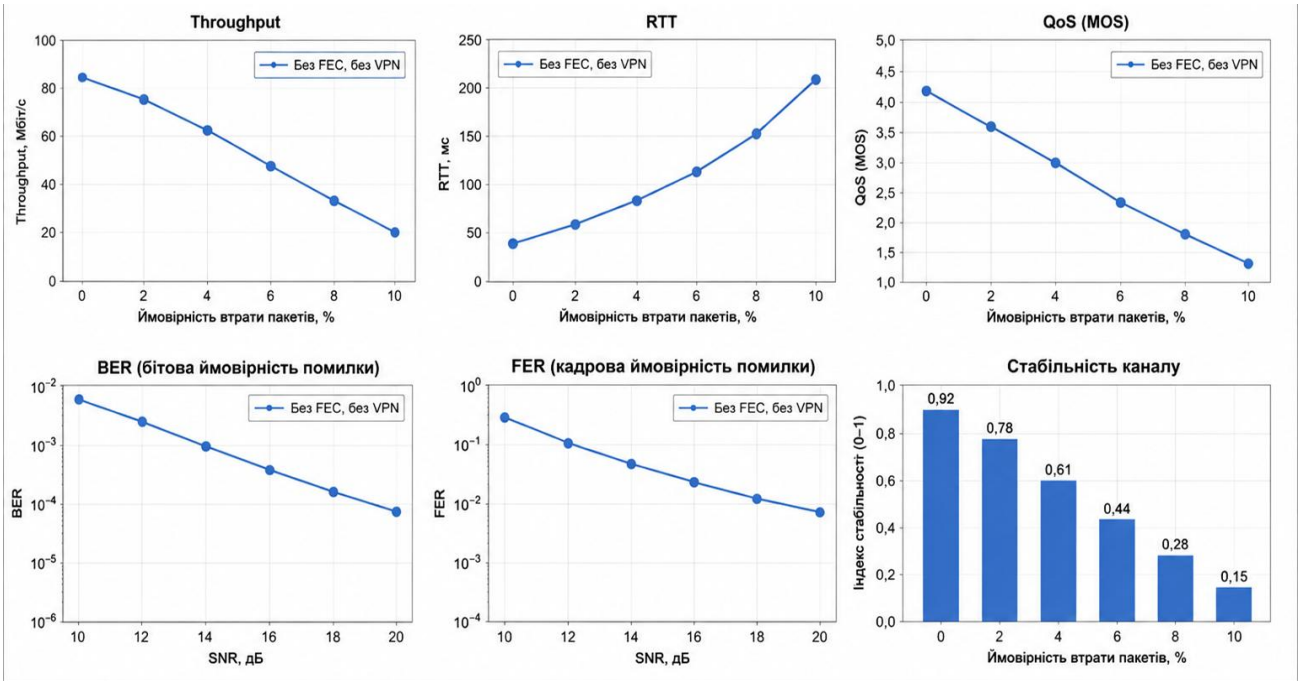


Рисунок 4.19 – Результати дослідження характеристик каналу без використання FEC та VPN

Отримані результати демонструють суттєву деградацію характеристик каналу за відсутності механізмів корекції помилок та захищеного тунелювання. Зі збільшенням імовірності втрати пакетів спостерігається зниження пропускної здатності, зростання затримки RTT, погіршення показника QoS, а також зменшення інтегрального індексу стабільності. Саме цей сценарій використовується як базовий для подальшого порівняння з конфігураціями, що застосовують FEC, VPN та їх комбіноване використання.

Для оцінювання впливу механізму FEC на характеристики каналу було проведено серію експериментів без використання VPN-оверлеїв. Передавання здійснювалося із застосуванням завадостійкого кодування та додаткової надлишковості, що дозволяло компенсувати втрати пакетів і підвищувати ймовірність коректного відновлення даних. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі з подальшим усередненням результатів. У межах експерименту оцінювалися показники пропускної здатності, затримки RTT,

якості обслуговування QoS, бітової та кадрової ймовірності помилки, а також інтегральний індекс стабільності каналу.

У дослідженні використовувалися значення SNR від 10 до 20 дБ, імовірність втрати пакетів p_{loss} від 0 до 10 %, середній рівень завад, застосування FEC-кодування та відсутність VPN-тунелювання. Результати наведені у додатку В, таблиці В25-В26.

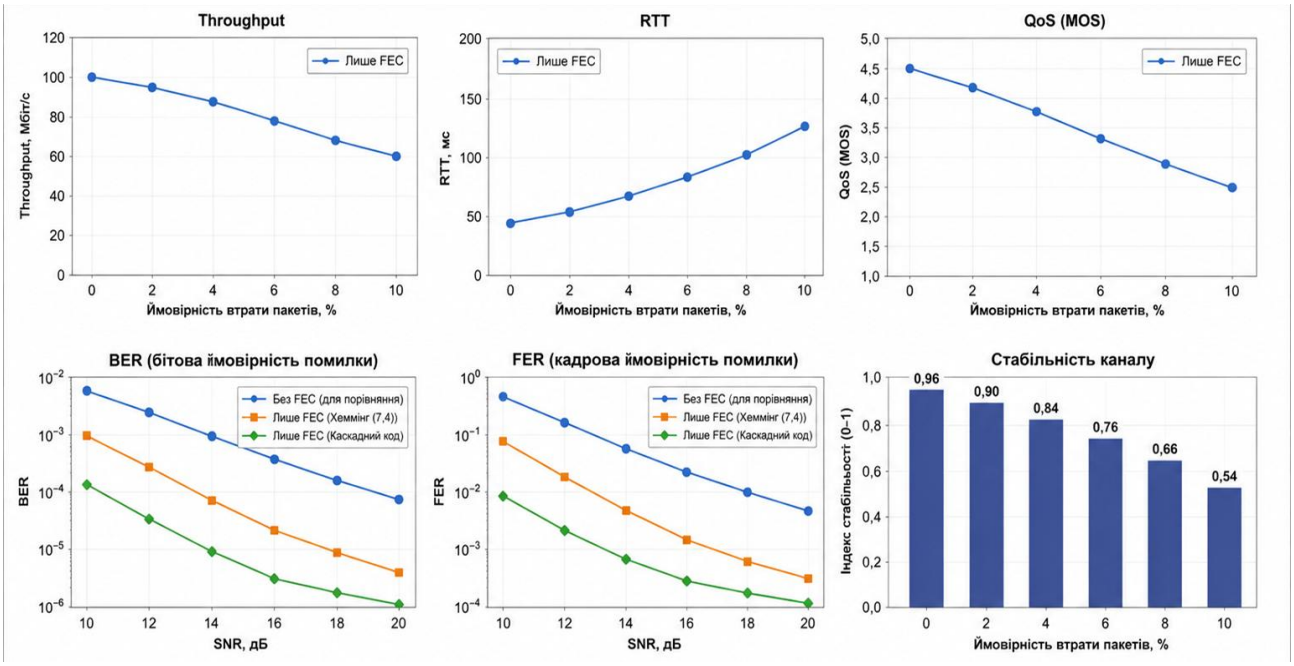


Рисунок 4.20 – Результати дослідження характеристик каналу з використанням FEC

Порівняно з базовим сценарієм застосування лише FEC забезпечує суттєве зниження BER і FER, а також помітне підвищення стабільності каналу. Водночас додаткова надлишковість призводить до певного зменшення пропускної здатності та зростання затримки RTT. Незважаючи на це, загальний ефект від використання FEC є позитивним, оскільки підвищення надійності передачі даних компенсує пов'язані з кодуванням накладні витрати.

Для оцінювання впливу VPN-тунелювання на характеристики каналу було проведено серію експериментів без використання механізмів FEC. У дослідженні

порівнювалися профілі IPsec, OpenVPN (UDP) та WireGuard за однакових умов передавання даних. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі з подальшим усередненням результатів. У ході експерименту оцінювалися показники пропускної здатності (Throughput), затримки RTT, якості обслуговування QoS (MOS), бітової та кадрової ймовірності помилки (BER і FER), а також інтегральний індекс стабільності каналу.

У дослідженні використовувалися значення SNR від 10 до 20 дБ, імовірність втрати пакетів p_{loss} від 0 до 10 %, середній рівень мережевих завад, використання VPN-профілів IPsec, OpenVPN (UDP) та WireGuard без застосування FEC-кодування. Результати наведені у додатку В, таблиці В27-В28.

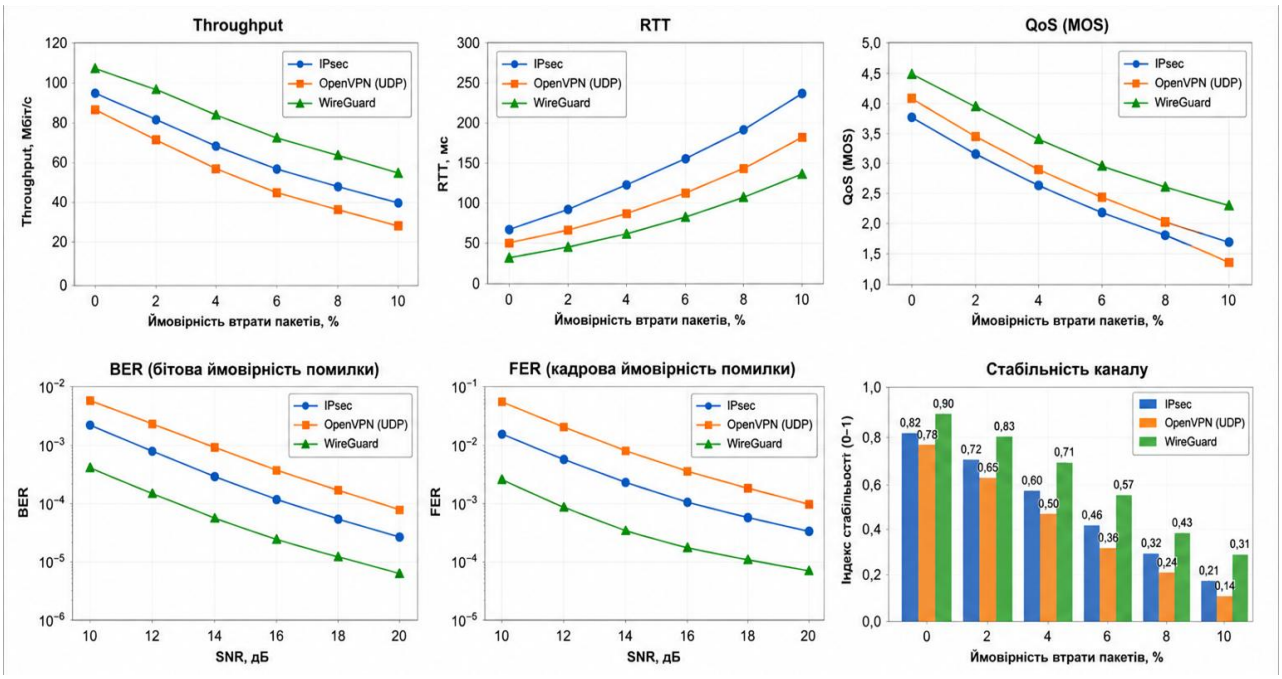


Рисунок 4.21 – Результати дослідження характеристик каналу з використанням VPN

Отримані результати показали, що використання лише VPN-тунелювання забезпечує захист трафіку, проте саме по собі не усуває вплив втрат пакетів і завад каналу. Найкращі результати серед досліджуваних профілів продемонстрував WireGuard, який характеризувався найбільшою пропускною здатністю,

найменшими затримками та найвищим індексом стабільності. OpenVPN забезпечував найнижчі показники пропускної здатності та найвищі значення BER і FER, тоді як IPsec займав проміжне положення. Це свідчить про те, що VPN-тунелювання підвищує захищеність передавання даних, але для суттєвого покращення надійності доставки потребує додаткового застосування механізмів корекції помилок.

Для оцінювання ефективності інтегрованого підходу було проведено серію експериментів із одночасним використанням механізмів FEC-кодування та VPN-тунелювання. У дослідженні розглядалися профілі FEC+IPsec, FEC+OpenVPN (UDP) та FEC+WireGuard. Для кожної конфігурації виконувалося понад 100 незалежних запусків моделі з подальшим усередненням результатів. У ході експерименту оцінювалися показники пропускної здатності (Throughput), затримки RTT, якості обслуговування QoS (MOS), бітової та кадрової ймовірності помилки (BER і FER), а також інтегральний індекс стабільності каналу. Метою дослідження було визначення впливу одночасного використання FEC і VPN на надійність та якість передачі даних в умовах втрат пакетів і завад каналу.

У дослідженні використовувалися значення SNR від 10 до 20 дБ, імовірність втрати пакетів p_{loss} від 0 до 10 %, середній рівень мережевих завад, застосування FEC-кодування та VPN-профілів IPsec, OpenVPN (UDP) і WireGuard. Результати наведені у додатку В, таблиці В29-В30.

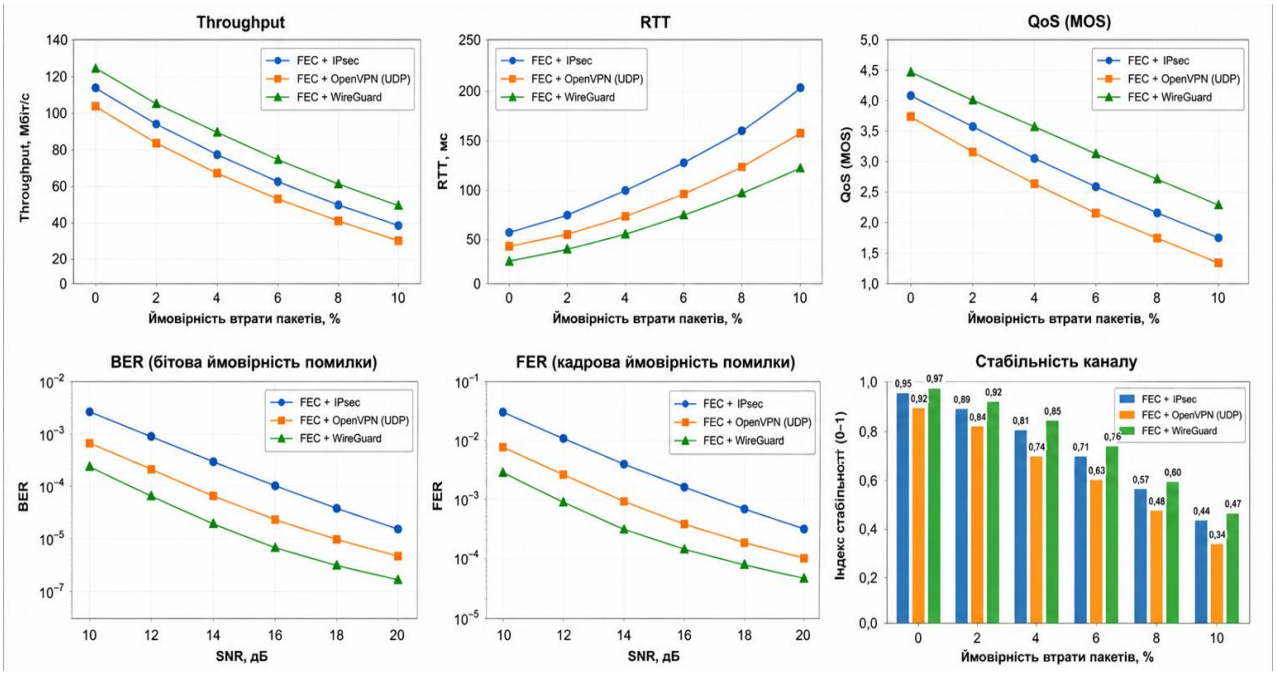


Рисунок 4.22 – Результати дослідження характеристик каналу з використанням FEC та VPN

Отримані результати підтверджують, що спільне використання FEC-кодування та VPN-тунелювання забезпечує найкращі характеристики серед усіх досліджених сценаріїв. Порівняно з базовим каналом, використання лише FEC або лише VPN дозволяє покращити окремі показники, однак саме їх поєднання забезпечує одночасне зниження BER і FER, підвищення стабільності каналу та покращення якості обслуговування. Найкращі результати продемонстрував профіль FEC + WireGuard, для якого спостерігалися найвищі значення Throughput, QoS та індексу стабільності за одночасного збереження мінімальних значень BER, FER і RTT. Це підтверджує доцільність використання інтегрованого підходу як найбільш ефективного рішення для роботи в умовах втрат пакетів і мережевих завад.

На завершальному етапі дослідження було виконано узагальнене порівняння чотирьох розглянутих сценаріїв передачі даних: базового каналу без використання FEC та VPN, сценарію із застосуванням лише FEC-кодування, сценарію з використанням лише VPN-тунелювання та інтегрованого підходу, який поєднує

механізми FEC і VPN. Для кожного сценарію було визначено усереднені значення ключових показників ефективності, отримані за результатами понад 100 незалежних запусків моделі в умовах зміни SNR від 10 до 20 дБ та ймовірності втрати пакетів від 0 до 10 %.

Отримані результати свідчать, що базовий сценарій без використання додаткових механізмів захисту характеризується найнижчою пропускною здатністю, найгіршими показниками BER і FER та мінімальною стабільністю функціонування. Використання лише FEC-кодування дозволяє суттєво знизити рівень бітових і кадрових помилок, підвищити стабільність каналу та покращити якість обслуговування, хоча це супроводжується певним збільшенням службових витрат і помірним зростанням затримки. Застосування лише VPN-тунелювання забезпечує захист трафіку та покращує окремі експлуатаційні характеристики, однак не усуває вплив фізичних помилок і втрат пакетів, унаслідок чого значення BER і FER залишаються помітно вищими порівняно зі сценаріями, що використовують FEC.

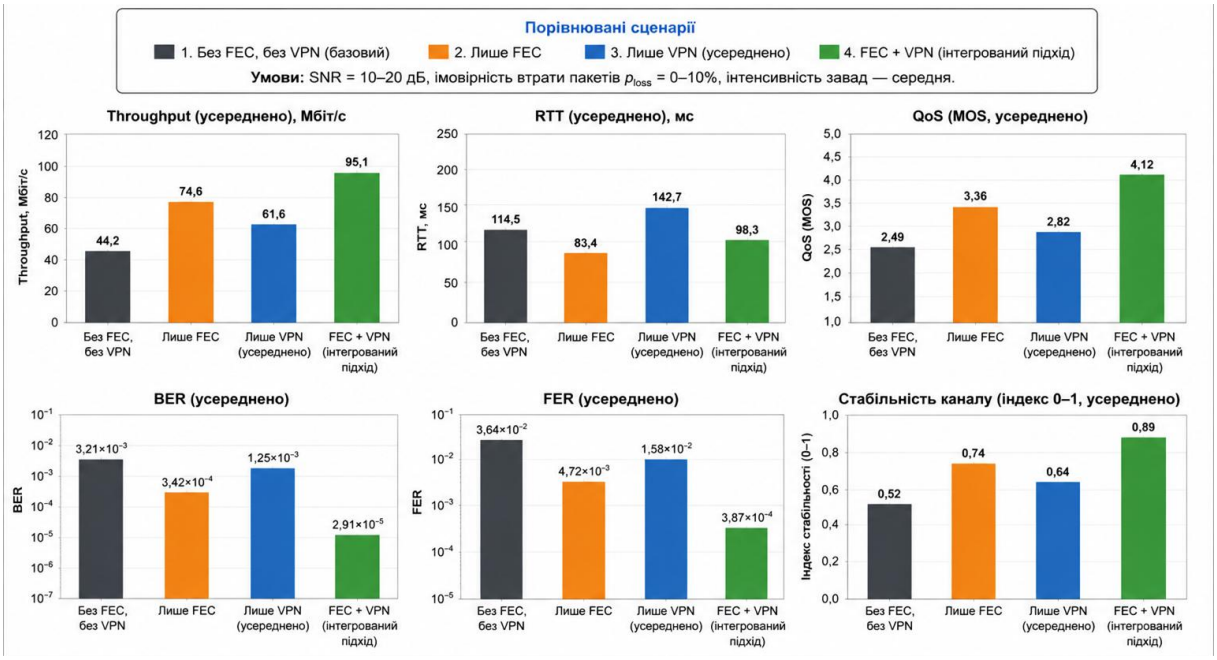


Рисунок 4.23 – Порівняльний аналіз усіх сценаріїв передавання даних

Найкращі результати продемонстрував інтегрований підхід, який поєднує механізми FEC-кодування та VPN-тунелювання. Для цього сценарію зафіксовано найбільшу середню пропускну здатність (95,1 Мбіт/с), найвищий показник якості обслуговування QoS (4,12 MOS) та найбільший індекс стабільності каналу (0,89). Одночасно спостерігаються найменші значення BER ($2{,}91 \cdot 10^{-5}$) і FER ($3{,}87 \cdot 10^{-4}$), що свідчить про найбільш ефективне придушення впливу завад та втрат пакетів. Незважаючи на наявність додаткових механізмів обробки, середнє значення RTT залишається на прийнятному рівні та є нижчим, ніж у сценарії з використанням лише VPN.

Таким чином, результати узагальненого порівняння підтверджують, що саме спільне використання FEC-кодування та VPN-тунелювання забезпечує найкращий баланс між надійністю передачі даних, якістю обслуговування, пропускною здатністю та часовими характеристиками. Це підтверджує доцільність використання запропонованої гібридної інформаційної технології як ефективного засобу підвищення стійкості та якості захищеної передачі даних у мережах зі змінними умовами функціонування.

Отже, результати порівняльного аналізу підтверджують, що розроблена гібридна інформаційна технологія відповідає вимогам, сформульованим у розділі 2, щодо надійності, швидкодії та захищеності. Найбільш доцільними є конфігурації, у яких захищений оверлей поєднується з FEC помірної надлишковості та адаптивним керуванням параметрами передавання.

4.6 Висновки за розділом

У четвертому розділі проведено тестування реалізації гібридної інформаційної технології та виконано аналіз результатів експериментальних досліджень ефективності запропонованих моделей і методів.

1. Сформовано експериментальну частину дослідження та систему тестових сценаріїв, що враховують різні умови функціонування мережі, рівні завад, втрати

пакетів і використання різних конфігурацій VPN-протоколів та механізмів завадостійкого кодування.

2. Наведено результати тестування процесів передавання та відновлення даних, досліджено вплив параметрів FEC-кодування та оверлейних технологій на стійкість системи до помилок і втрат пакетів.

3. Виконано оцінювання показників надійності та якості функціонування системи, зокрема затримок передавання, стабільності каналу, ефективності використання мережевих ресурсів та якості обслуговування трафіку.

4. Проведено аналіз ефективності реалізованих моделей і методів, визначено особливості їх функціонування в умовах різного рівня навантаження та впливу кіберзагроз.

5. Виконано порівняльний аналіз отриманих результатів із базовими підходами та узагальнено результати експериментальних досліджень.

За результатами проведених досліджень підтверджено ефективність запропонованої гібридної інформаційної технології забезпечення надійності й захищеності передавання даних. Встановлено, що спільне використання механізмів завадостійкого кодування та VPN-тунелювання дозволяє підвищити стійкість системи до помилок і кіберзагроз, зменшити втрати пакетів та забезпечити стабільність функціонування комп’ютерних мереж у складних умовах передавання даних.

ВИСНОВКИ

У висновках дисертаційної роботи вирішено актуальну науково-технічну задачу підвищення надійності та захищеності передавання даних у комп’ютерних мережах в умовах дії завад і кіберзагроз шляхом розроблення моделей, методів та інформаційної технології, заснованих на інтеграції механізмів завадостійкого кодування та оверлейних технологій. Проведені дослідження підтвердили, що ізольоване застосування засобів криптографічного захисту або механізмів корекції помилок не забезпечує необхідного рівня ефективності функціонування сучасних мережевих систем, тоді як їх комплексне поєднання дозволяє підвищити стійкість до помилок, втрат пакетів та кіберзагроз. Результати дослідження дозволяють зробити наступні висновки.

1. Виконано аналіз сучасного стану забезпечення надійності та інформаційної безпеки систем передавання даних, досліджено основні типи кібератак, методи завадостійкого кодування та сучасні VPN-протоколи. Визначено обмеження існуючих підходів та обґрунтовано доцільність побудови інтегрованої моделі захищеного каналу передавання даних, яка поєднує механізми завадостійкого кодування та оверлейні технології в межах єдиного підходу.

2. Обґрунтовано систему метрик і показників оцінювання ефективності функціонування гібридного захищеного каналу передавання даних. Розроблено концептуальну модель гібридного каналу, метод синтезу його профілю та метод адаптивного керування параметрами завадостійкого кодування і захищеного оверлею. Визначено критерії оптимізації та обмеження допустимості конфігурацій системи, що забезпечують адаптивне налаштування параметрів відповідно до стану мережі та вимог до якості обслуговування трафіку.

3. Розроблено моделі та методи побудови гібридних захищених каналів передавання даних і реалізовано програмно-алгоритмічне забезпечення інтегрованої інформаційної технології. Реалізовано модулі завадостійкого кодування, VPN-тунелювання, V2Ray/XRay та криптографічного захисту, а також виконано їх інтеграцію в межах єдиної системи. Запропоновано архітектуру

реалізації гібридної технології та сформовано критерії валідації й план експериментальних досліджень.

4. Проведено експериментальні дослідження та тестування розробленої інформаційної технології в різних умовах функціонування мережі. Отримані результати підтвердили ефективність запропонованого підходу та показали, що спільне використання механізмів FEC-кодування та VPN-тунелювання дозволяє зменшити втрати пакетів, підвищити стійкість системи до помилок і кіберзагроз, а також забезпечити стабільність передавання даних у складних умовах мережевої взаємодії.

Основними науковими результатами роботи є:

–удосконалено гібридну модель захищеного каналу передавання даних, побудовану на поєднанні механізмів завадостійкого кодування та VPN-тунелювання з урахуванням впливу завад і кіберзагроз різної природи, яка, на відміну від існуючих підходів до окремого використання зазначених механізмів, забезпечує їх комплексну взаємодію та дозволяє підвищити стійкість системи до помилок і атак, а також забезпечити стабільність передавання даних у складних умовах функціонування мереж;

– удосконалено метод адаптивного налаштування параметрів завадостійкого кодування та оверлейних протоколів на основі оцінювання стану мережі й показників ефективності передавання даних, який, на відміну від існуючих методів із фіксованими або частково змінними параметрами, забезпечує узгоджене коригування конфігурації системи та дозволяє підвищити ефективність використання мережевих ресурсів і якість обслуговування трафіку;

– отримали подальший розвиток методи формування профілю каналу передавання даних і побудови інформаційної технології багаторівневого захисту на основі комплексного врахування параметрів кодування та характеристик VPN-протоколів, які, на відміну від існуючих рішень, забезпечують інтегроване налаштування параметрів системи та дозволяють реалізувати адаптивне

конфігурування захищених каналів зв’язку відповідно до умов функціонування й вимог до надійності та інформаційної безпеки.

Практичне значення отриманих результатів полягає у можливості використання розроблених моделей, методів та інформаційної технології при побудові захищених комп’ютерних мереж, корпоративних інформаційних систем, телекомунікаційної інфраструктури, систем управління та критично важливих мережевих сервісів. Реалізовані рішення забезпечують адаптивне налаштування параметрів передавання даних, підвищення ефективності використання мережевих ресурсів і стабільності функціонування систем в умовах дії завад та кіберзагроз.

Результати дисертаційної роботи підтверджують досягнення поставленої мети дослідження та свідчать про доцільність подальшого розвитку інтегрованих підходів до забезпечення надійності й захищеності передавання даних у комп’ютерних мережах. Перспективами подальших досліджень є розширення механізмів адаптивного керування, інтеграція засобів інтелектуального аналізу трафіку та застосування запропонованих моделей у високонавантажених розподілених мережах і системах нового покоління.

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. – Wiley, 2020. – 1232 p.
2. Trend Micro. *Cybersecurity Report 2023*. – Tokyo: Trend Micro, 2023. – 116 p.
3. McAfee. *Global Threat Report 2022*. – Santa Clara: McAfee, 2022. – 101 p.
4. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. – Pearson, 2022. – 592 p.
5. Bishop M. *Computer Security: Art and Science*. 2nd ed. – Addison–Wesley, 2018. – 1368 p.
6. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 20th Anniversary ed. – Wiley, 2015. – 784 p.
7. Хакінг та кіберзагрози: сучасні виклики безпеці. – К.: Наукова думка, 2021. – 312 с.
8. National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. – Gaithersburg, MD: NIST, 2018. – 55 p.
9. FireEye. *Mandiant Security Effectiveness Report 2022*. – Reston: FireEye, 2022. – 84 p.
10. CrowdStrike. *Global Threat Report 2023*. – Sunnyvale: CrowdStrike, 2023. – 80 p.
11. Check Point Research. *Cyber Attack Trends: 2023 Mid–Year Report*. – Tel Aviv: Check Point, 2023. – 77 p.
12. European Union Agency for Cybersecurity (ENISA). *Threat Landscape 2022*. – Luxembourg: Publications Office of the European Union, 2022. – 198 p.
13. PwC. *Global Digital Trust Insights 2023*. – London: PricewaterhouseCoopers, 2023. – 98 p.
14. Cisco. *Annual Cybersecurity Report 2023*. – San Jose: Cisco Press, 2023. – 142 p.
15. Symantec. *Internet Security Threat Report 2022*. – Mountain View: Symantec Corporation, 2022. – 110 p.

16. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2023. – The Hague: Europol, 2023. – 86 p.
17. IBM. *Cost of a Data Breach Report 2023*. – Armonk: IBM Security, 2023. – 87 p.
18. Verizon. *2023 Data Breach Investigations Report*. – New York: Verizon, 2023. – 124 p.
19. Microsoft Security Team. *Digital Defense Report 2022*. – Redmond: Microsoft, 2022. – 140 p.
20. Palo Alto Networks. *Unit 42 Threat Report 2023*. – Santa Clara: PAN, 2023. – 93 p.
21. Kuchuk H ., Matvieiev M.. MODELING THE PROCESS OF LOADING 3D MODELS IN A CLIENT APPLICATION. *Advanced Information Systems, 9(4)*, 2022. P. 11–16.
22. Semenov, S., Zhang, M., Mozhaiev, O., Kuchuk, N., Tiulieniev, S., Gnusov, Y., Mozhaiev, M., Strukov, V., Onishchenko, Y., & Kuchuk, H. (2023). Construction of a model of steganographic embedding of the UAV identifier into ADS-B data. *Eastern-European Journal of Enterprise Technologies, 5(4 (125)*, 2020. 6 с.
23. В. М. Рудницький, Н. В. Лада, Г. А. Кучук, Д. А. Підласий. Архітектура СЕТ-операцій і технології потокового шифрування. *Architecture of CET-operations and stream encryption technologies*, монографія, Черкаси : видавець Пономаренко Р.В, 2024. – 374 с.
24. Kopp, A., Orlovskyi, D., Kizilov, O., & Halatova, O. (2024). Research on error probability assessment in user personal data processing in gdprcompliant business process models. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 1 (11)*, 2020. – 34 с.
25. Kopp, A. M., & Orlovskyi, D. L. (2020). Capturing software requirements for business process model analysis and improvement. *Bulletin of National Technical University "KhPI". Series: System Analysis, Control and Information Technologies, 2 (4)*, 2020. – 23 с.
26. Kopp, A., & Orlovskyi, D. The approach and the software tool to calculate semantic quality measures of business process models. *Bulletin of National Technical*

University "KhPI". Series: System Analysis, Control and Information Technologies, 1 (7), 2022– 66 с.

27. О. В. Шматко, О. Є. Рагулін, П. О. Кравченко, П. В. Буслов Дослідження архітектурних рішень для побудови безпечної системи зберігання та передачі конфіденційних даних. *Том 2 № 80 Системи управління, навігації та зв'язку,*2025 – 217с.
28. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. *Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 29 (128)*, – 36 p.
29. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A., Shestak, Y., Oriekhov, S., Korsunov, S., & Kravchenko, S. *Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2(9) (128)*, 2024. –36 p.
30. Shmatko, O., Yevseiev, S., Milov, O., Sporyshev, K., Opirskyy, I., Glukhov, S., Rudenko, Y., Nalyvaiko, A., Dakov, S., & Sampir, O. *Development of a model of the information and analytical system for making decisions on detecting failures of information transmission channels. Eastern-European Journal of Enterprise Technologies, 3(9 (129)*, 2024. –28 p.
31. Toliupa S., Buchyk S., Nakonechnyi V., Brailovskyi M., Shtanenko S. Design of security protection and management systems based on game theory. *CEUR Workshop Proceedings*. – 2023. 334p.
32. Наконечний В., Сайко В., Наритник Т. Метод підвищення ефективності керування енергетичним потенціалом захищених радіоліній терагерцового діапазону з використанням штучного інтелекту *Безпека інформаційних систем і технологій, № 1(6),*2023. – 43с.

33. Дудикевич В.Б., Партика О.О., Наконечний Т.І. Впровадження систем одноразового входу (SSO) для підвищення кібербезпеки. *Сучасний захист інформації.* Т. 1(61), 2025. –60 с.
34. Pevnev, V., Tsuranov, M., Zemlianko, H., Amelina, O. Conceptual Model of Information Security. In: Nechyporuk, M., Pavlikov, V., Kritskiy, D. (eds) *Integrated Computer Technologies in Mechanical Engineering, 2020. ICTM 2020. Lecture Notes in Networks and Systems, vol 188.* Springer, Cham, *2020.*
35. V. Pevnev, M. Tsuranov and A. Zhmyrov, Noise-immune encoding: The aspects of cybersecurity assurance, *IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Kyiv, Ukraine, 2018. –248p.
36. Sharov V.O., Berdnikov A.G. Model of a noise-resistant data transmission channel. *Computer modeling in science-intensive technologies (KMNT-2020),* Kharkiv: V.N. Karazin Kharkiv National University, 2020. 4 p.
37. Sharov V.O., Berdnikov A.G. Modeling of corrective cascade code in data transmission channels of the control system. *Computer modeling in science-intensive technologies (KMNT-2021),* Kharkiv: V.N. Karazin Kharkiv National University, 2021. 5 p.
38. Sharov V.O., Nikulina O.M., Severyn V.P. Development of a model of noise-tolerant data transmission for information technology of optimization of dynamic systems control. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 2 (8),* 2022, pp. 57–62.
39. Sklar B. Digital Communications: Fundamentals and Applications. 3rd ed. – Pearson, 2021. – 944 p.
40. Lin S., Costello D.J. Error Control Coding. 3rd ed. – Boston: Pearson, 2021. – 1280 p.
41. Proakis J.G., Salehi M. Digital Communications. 6th ed. – New York: McGraw–Hill, 2019. – 1072 p.

42. Comparative benchmarks: various independent studies comparing WireGuard, OpenVPN and IPSec (academic and industry reports) – aggregated analysis, 2019–2023. (See examples: Phoronix tests, networking research papers).
43. Touch J., Fairhurst G., Eggert S. RFC 8900: *IP Fragmentation Considered Fragile* (BCP 230), 2020. Electronic source, URL: https://www.rfc-editor.org/rfc/rfc8900.pdf. (дата звернення 10.05.2025)
44. Shu Lin, Daniel J. Costello, Jr., Mitsuru U. Practical Applications of Error Control Coding in Communication Systems. – Wiley–IEEE Press, 2020. – 432 p.
45. ETSI. 5G; NR; Multiplexing and channel coding *(3GPP TS 38.212 version 17.3.0 Release 17). – Sophia Antipolis*: ETSI, 2022. – 146 p.
46. IETF RFC 6363. Adamson B. et al. Forward Error Correction (FEC) Framework. RFC Editor, 2011. – URL: https://datatracker.ietf.org/doc/html/rfc6363 (дата звернення: 16.10.2025).
47. Watson M. et al. RFC 6363: *Forward Error Correction (FEC) Framework*, 2011 – URL: https://www.rfc-editor.org/rfc/rfc6363.html (дата звернення: 16.10.2025).
48. Richardson T., Urbanke R. Modern Coding Theory. – Cambridge: Cambridge University Press, 2008. – 576 p.
49. IETF RFC 8680. Roca V., Teibi S. Forward Error Correction (FEC) Framework Extension to Sliding Encoding Window Codes. RFC Editor, 2020. – URL: https://www.rfc–editor.org/rfc/rfc8680.html (дата звернення: 16.10.2025).
50. Roca V., Teibi S. RFC 8680: FECFRAME Extension to Sliding Encoding Window Codes, 2020 – URL: https://www.rfc-editor.org/rfc/rfc8680.pdf (дата звернення: 17.11.2025).
51. NASA. Space Communications and Navigation (SCaN) Code Recommendations. – Washington: NASA, 2020. – 84 p.
52. 3GPP TS 38.212 *NR; Multiplexing and channel coding*. ETSI/3GPP, Release 16–18 URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3214 (дата звернення: 9.5.2025).

53. CCSDS 131.x–series / NASA SCaN: *LDPC Codes for Near–Earth and Deep–Space Links*, 2006–2024 – URL: https://ccsds.org/Pubs/131x1o1s.pdf (дата звернення: 2.5.2025).
54. Cloudflare Research. Post–Quantum Cryptography and VPN Tunneling. – Cloudflare, 2022. – URL: https://www.rfc–editor.org/rfc/rfc8680.html (дата звернення: 16.10.2025).
55. Google Security Blog. Experimenting with Post–Quantum VPN. – Google LLC, 2026. – URL: https://blog.google/innovation-and-ai/technology/safety-security/the-quantum-era-is-coming-are-we-ready-to-secure-it/ (дата звернення: 7.2.2026).
56. ITU–T Recommendation X.200. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. – Geneva: ITU, 2016. – 138 p.
57. Saxena M. C., Bajaj P., et al. A Novel Method to Enhance the Reliability of Transmission over Secured SD–WAN Overlays (Reed–Solomon FEC + WireGuard). JATIT, 2023. – URL: https://www.jatit.org/volumes/Vol101No14/7Vol101No14.pdf (дата звернення: 16.10.2025).
58. Jones T., Fairhurst G., Tüxen T. RFC 8899: *Datagram PLPMTUD*, 2020 – URL: https://www.rfc-editor.org/rfc/rfc8899.pdf (дата звернення: 6.6.2024).
59. ENISA. Quantum–Safe Cryptography: Current State and Roadmap 2022–2035. – Luxembourg: *Publications Office of the EU*, 2022. – 88 p.
60. Sharov V.O., Nikulina O.M., Severyn V.P. Modeling and analysis of noise-resistant cascade code encoders for dynamic systems. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 1 (9)*, 2023, pp. 64–69.
61. Sharov V.O., Nikulina O.M., Loshkareva S.E. Development of a flexible model of noise-resistant data transmission for controlling dynamic systems. Information technologies: science, engineering, technology, education, health: *Abstracts of the XXI international scientific and practical conference MicroCAD-2023, May 17-20*, 2023, Kharkiv, NTU "KhPI", p. 1048.

62. Sharov V.O., Nikulina O.M. Two-level concept for modeling a single noise-resistant digital data transmission. *Bulletin of NTU "KhPI". Series: System Analysis, Management and Information Technologies, No. 1 (11)*, 2024, pp. 70–75.
63. Donenfeld J. WireGuard: Next Generation Kernel Network Tunnel. *Whitepaper & project documentation*. 2017–2020.
64. OpenVPN Community Documentation. OpenVPN Features and Comparisons. – OpenVPN.net. 2023.
65. Wouters P., Migault D., Mattsson J. P., Nir Y., Kivinen T. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH*). RFC 8221. IETF / RFC Editor*, 2017.
66. Bruce Schneier, Mudge, Wagner D. Cryptanalysis of Microsoft's PPTP Authentication Extensions. – *Proceedings of USENIX Security Symposium*, 1999. – 12 p.
67. Kent S., Seo K. Security Architecture for the Internet Protocol. *RFC 4301. – IETF*, 2005. – 84 p.
68. Kaufman C., Hoffman P., Nir Y., Eronen P., Kivinen T. Internet Key Exchange Protocol Version 2 (IKEv2). *RFC 7296. – IETF*, 2014. – 142 p.
69. Schneier B. Secrets and Lies: Digital Security in a Networked World. – Wiley, 2015. – 448 p.
70. V2Ray / XRay project documentation and articles (project repos and community guides). 2015–2022.
71. Cisco Systems. SD–WAN and VPN Integration: Technical White Paper. – San Jose: Cisco, 2022. – 42 p.
72. ETSI. Network Functions Virtualisation and Cloud–native VPN. – Sophia Antipolis: ETSI, 2021. – 72 p.
73. Palo Alto Networks. SASE and the Future of Enterprise VPN. – Santa Clara: PAN, 2022. – 48 p.

74. Gartner. Market Guide for Virtual Private Networks. – Stamford: Gartner Inc., 2023. – 65 p.
75. IDC. Worldwide VPN Market Forecast, 2023–2030. – Framingham: IDC, 2023. – 54 p.
76. Forrester. Zero Trust and VPN Convergence. – Cambridge: Forrester Research, 2023. – 39 p.
77. Phoronix. Comparative Benchmarks of WireGuard, OpenVPN, IPSec and XRay. – Phoronix.com, 2023.
78. Mackey S., Mihov S., et al. A Performance Comparison of WireGuard and OpenVPN. ACM SAC'20, 2020.
79. Chua C.H., et al. Open–Source VPN Software: Performance Comparison, ACM (2022).
80. Anyam J., Singh R.R., Larijani H., Philip A. Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments. MDPI Computers, 2025.
81. Dekker E. Performance Comparison of VPN Implementations: WireGuard, OpenVPN, IPsec. OS3 Report, 2020.
82. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Bulletin of NTU "KhPI". Series: System analysis, management and information technologies, No. 2 (12),* 2024, pp. 92–97.
83. Sharov V.O., Nikulina O.M. Model of a noise-resistant control system taking into account artificial higher-level interference. *Information technologies: science, engineering, technology, education, health: Abstracts of the XXII international scientific and practical conference MicroCAD-2024*, May 22-24, 2024, Kharkiv, NTU "KhPI", p. 1270.
84. Sharov V.O., Nikulina O.M. The model control system resistant to interference from higher-level artificial sources. *XVIII International Scientific and Practical Conference of Masters and Postgraduates "Theoretical and Practical Research of*

Young Scientists”, November 19–22, 2024, Kharkiv: NTU “KhPI”, pp. 56–57.2024 р., Харків: НТУ «ХПІ», с. 56–57.

85. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Bulletin of NTU "KhPI". Series: System Analysis, Management and Information Technologies, No. 1 (13)*, 2025, pp. 112–116.

ДОДАТОК А
СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

ШАРОВА Владислава Олеговича

Наукові праці, які відображають основні наукові результати дисертації.

Статті у періодичних наукових виданнях, що увійшли до переліку наукових фахових видань України:

1. Шаров В.О., Нікуліна О.М., Северин В.П. Розробка моделі завадостійкої передачі даних для інформаційної технології оптимізації управління динамічними системами. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (8)*, 2022, с. 57–62.(Б)

DOI: https://doi.org/10.20998/2079-0023.2022.02.09

2. Шаров В.О., Нікуліна О.М., Северин В.П. Моделювання та аналіз кодерів завадостійких каскадних кодів для динамічних систем. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (9)*, 2023, с. 64–69.(Б)

DOI: https://doi.org/10.20998/2079-0023.2023.01.10

3. Шаров В.О., Нікуліна О.М. Дворівнева концепція для моделювання єдиної завадостійкої передачі цифрових даних. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (11)*, 2024, с. 70–75.(Б)

DOI: https://doi.org/10.20998/2079-0023.2024.01.11

4. Sharov V.O., Nikulina O.M. Study of compatibility of methods and technologies of high-level protocols and error-correcting codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 2 (12)*, 2024, с. 92–97.(Б)

DOI: https://doi.org/10.20998/2079-0023.2024.02.14

5. Sharov V.O., Nikulina O.M. Layered Defense in Communication Systems: Joint Use of VPN Protocols and Linear Block Codes. *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології, № 1 (13)*, 2025, с. 112–116.(Б)

DOI: https://doi.org/10.20998/2079-0023.2025.01.17

Інші публікації:

Опубліковані праці апробаційного характеру:

6. Шаров В.О. Модель завадостійкого каналу передачі даних / Шаров В.О., Бердніков А.Г.// *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2020)*, Харків: ХНУ ім. В.Н. Каразіна, 2020. 4 с.

URL: https://discovery.kpi.ua/Record/000634216

7. Шаров В.О. Моделювання коригувального каскадного коду в каналах передачі даних системи управління / Шаров В.О., Бердніков А.Г.// *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2021)*, Харків: ХНУ ім. В.Н. Каразіна, 2021. 5 с.

URL: https://odnb.odessa.ua/vnn/book/13913

8. Шаров В.О. Розробка гнучкої моделі завадостійкої передачі даних для управління динамічними системами / Шаров В.О., Нікуліна О.М., Лошкарьова С.Є.// *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я:* Тези доповідей XXXI міжнародної науково-практичної конференції MicroCAD-2023, 17-20 травня 2023 р., Харків, НТУ «ХПІ», с. 1048.

URL: https://repository.kpi.kharkov.ua/items/ea5b83c5-0561-47cb-a4d0-67aacd51c994

9. Шаров В.О. Модель завадостійкої системи управління з урахуванням штучних перешкод вищого рівня / Шаров В.О., Нікуліна О.М. // *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я:* Тези доповідей XXXII міжнародної науково-практичної конференції MicroCAD-2024, 22-24 травня 2024 р., Харків, НТУ «ХПІ», с. 1270.

URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/6c1dd37f-bc26-4c91-af1c-a7eec5d2d9b5

10. Sharov V.O. The model control system resistant to interference from higher-level artificial sources. / Sharov V.O., Nikulina O.M. // XVIII Міжнар. наук.-практ. конф. магістрантів та аспірантів «Теоретичні та практичні дослідження молодих вчених», 19–22 листопада 2024 р., Харків: НТУ «ХПІ», с. 56–57.

URL: https://repository.kpi.kharkov.ua/items/78bb4ab5-ac4b-4c40-aa1f-6ff555b2823f

ДОДАТОК Б
МАТЕРІАЛИ ЩОДО ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ

ЗАТВЕРДЖУЮ
Проректор
Національного технічного
університету «Харківський
політехнічний інститут»
Руслан МИГУЩЕНКО
"__" грудня 2025 р.

АКТ

про використання результатів дисертаційної роботи
ШАРОВА Владислава Олеговича
в навчальному процесі кафедри інформаційних систем та технологій
Національного технічного університету «ХПІ»

Ми, що нижче підписалися, завідувачка кафедри інформаційних систем та технологій НІКУЛІНА Олена Миколаївна, професор кафедри інформаційних систем та технологій МОСКАЛЕНКО Валентина Володимирівна, доцент кафедри інформаційних систем та технологій ХАЦЬКО Наталія Євгеніївна склали акт про те, що результати дисертаційної роботи ШАРОВА Владислава Олеговича впроваджені в навчальний процес на кафедрі інформаційних систем та технологій.

Модель оцінки ефективності комбінування завадостійких кодів з VPN впроваджено в дисципліну «Математичне моделювання та аналіз систем».

Метрики і оцінки вірогідних перешкод і завад впроваджено в дисципліну «Операційні системи мережевих технологій».

Модель ефективної взаємодії протоколів різних рівнів впроваджено в дисципліну «Основи комп'ютерних мереж».

Завідувачка кафедри
інформаційних систем та
технологій НТУ «ХПІ» Олена НІКУЛІНА

Професор кафедри
інформаційних систем та
технологій НТУ «ХПІ» Валентина МОСКАЛЕНКО

Доцент кафедри
інформаційних систем та
технологій НТУ «ХПІ» Наталія ХАЦЬКО

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Національного технічного
університету «Харківський
політехнічний інститут»
Андрій МАРЧЕНКО
"22" грудня 2025 р.

АКТ

про використання результатів дисертаційної роботи
аспіранта кафедри інформаційних систем та технологій
ШАРОВА Владислава Олеговича
в науково-дослідній роботі, виконаній відповідно до тематичного плану
Національного технічного університету «ХПІ»

Ми, що нижче підписалися, завідувачка кафедри інформаційних систем та технологій НІКУЛІНА Олена Миколаївна, професор кафедри інформаційних систем та технологій МОСКАЛЕНКО Валентина Володимирівна склали акт про те, що результати дисертаційної роботи ШАРОВА Владислава Олеговича впроваджені в науково-дослідних роботах:

1. «Розробка математичних моделей та програмних додатків для управління складними системами з використанням штучного інтелекту» (ДР№ 124U001390). Здобувач брав участь у виконанні робіт за вказаною темою в якості виконавця. В межах виконання робіт здобувачем розроблені: 1) модель оцінки надійності і завадостійкості систем передачі даних; 2) модель вибору ефективних завадостійких кодів і протоколів; 3) система вибору кодів для використання у системах управління.

2. «Розробка математичних моделей для оптимізації процесів управління складними динамічними системами з використанням обчислювального інтелекту» (ДР№ 0124U001511). Здобувач брав участь у виконанні робіт за вказаною темою в якості виконавця. В межах виконання робіт здобувачем розроблені: 1) модель оцінки надійності і завадостійкості систем передачі даних; 2) модель оцінки ризиків для достовірної передачі даних; 3) система обирання оптимальних завадостійких протоколів верхнього рівня для формування захищених тунелів при передачі даних.

Завідувачка кафедри
інформаційних систем та
технологій НТУ «ХПІ» Олена НІКУЛІНА

Професор кафедри
інформаційних систем та
технологій НТУ «ХПІ» Валентина МОСКАЛЕНКО

ДОДАТОК В

РЕЗУЛЬТАТИ ЕКСПЕРЕМЕНТІВ

Таблиця В.1 – Часові залежності у динамічному сценарії зміни SNR

Час, с	γ, дБ	τ95, мс	Gapp, Мбіт/с	φ
0	3.1	89	15.5	0.78
5	3.2	89	15.0	0.78
10	3.5	78	14.5	0.78
15	5.2	68	12.2	0.78
20	7.8	49	9.0	0.78
25	10.1	28	6.0	0.78
30	9.0	38	8.0	0.78
35	7.0	58	10.5	0.78
40	5.1	68	13.2	0.78
45	5.3	77	14.3	0.78
50	5.4	77	14.3	0.78
55	5.0	72	13.3	0.78
60	5.3	72	13.3	0.78

Таблиця В.2 – Залежність P_{dec} та P_{dec}^{mdl} від φ для ε = 0,02

φ	P_{dec}^{mdl}	P_{dec}
0,04	0,937	0,927
0,10	0,990	0,982
0,17	0,999	0,992
0,24	1,000	0,994
0,28	1,000	0,996
0,33	1,000	0,998
0,40	1,000	0,999
0,47	1,000	0,999
0,54	1,000	0,999
0,60	1,000	0,999

Таблиця В.3 – Залежність P_{dec} та P_{dec}^{mdl} від φ для ε = 0,05

φ	P_{dec}^{mdl}	P_{dec}
0,04	0,721	0,707
0,10	0,901	0,888
0,17	0,971	0,962
0,24	0,992	0,984
0,28	0,996	0,992
0,33	0,998	0,996
0,40	0,999	0,998
0,47	1,000	0,999
0,54	1,000	0,999
0,60	1,000	0,999

Таблиця В.4 – Залежність P_{dec} та P_{dec}^{mdl} від φ для ε = 0,1

φ	P_{dec}^{mdl}	P_{dec}
0,10	0,682	0,668
0,17	0,807	0,793
0,24	0,918	0,904
0,28	0,965	0,955
0,33	0,988	0,978
0,40	0,997	0,989
0,47	0,999	0,994
0,54	1,000	0,995
0,60	1,000	0,995

Таблиця В.5 – Порівняння коефіцієнта успішної доставки Π_{e2e} для різних значень φ та VPN-профілів при SNR=3 і 6 дБ

φ	WireGuard, 3 дБ	IPsec, 3 дБ	OpenVPN, 3 дБ	WireGuard, 6 дБ	IPsec, 6 дБ	OpenVPN, 6 дБ
0.00	0.45	0.41	0.38	0.63	0.59	0.56
0.10	0.77	0.73	0.69	0.90	0.88	0.85
0.20	0.94	0.92	0.90	0.97	0.95	0.94
0.30	0.98	0.97	0.95	0.995	0.988	0.978
0.40	0.985	0.980	0.975	0.997	0.994	0.990
0.53	0.990	0.988	0.982	0.998	0.996	0.994

Таблиця В.6 – Залежність τ_{95} та частки фрагментованих пакетів від φдля профілів IPsec, OpenVPN і WireGuard

φ	IPsec, τ95 (мс)	OpenVPN, τ95 (мс)	WireGuard, τ95 (мс)	IPsec, ξfrag (%)	OpenVPN, ξfrag (%)	WireGuard, ξfrag (%)
0.00	113	118	109	1.1	5.0	0.9
0.05	120	126	116	0.8	3.8	0.6
0.10	126	132	121	0.5	2.2	0.3
0.20	133	141	129	0.1	0.7	0.0
0.30	140	149	136	0.0	0.0	0.0

Таблиця В.7 – Порівняння Π_{vpn} та Π_{prx} для профілів IPsec, OpenVPN і WireGuard за різних умов каналу

SNR, дБ	IPsec, Пvpn	IPsec, Пprx	OpenVPN, Пvpn	OpenVPN, Пprx	WireGuard, Пvpn	WireGuard, Пprx
3	0.955	0.969	0.948	0.962	0.964	0.974
6	0.980	0.985	0.975	0.982	0.987	0.991
9	0.992	0.995	0.989	0.993	0.996	0.998

Таблиця В.8 – Залежність goodput та завантаження CPU від коефіцієнта надлишковості φ для профілів IPsec, OpenVPN і WireGuard

φ	IPsec goodput, Мбіт/с	OpenVPN goodput, Мбіт/с	WireGuard goodput, Мбіт/с	IPsec u_cpu, %	OpenVPN u_cpu, %	WireGuard u_cpu, %
0.00	9.82	9.23	10.53	33	30	27
0.05	9.50	8.90	10.22	38	34	31
0.10	9.20	8.60	9.80	44	39	34
0.20	8.65	8.18	9.15	58	49	42
0.30	8.28	8.00	8.78	71	60	46

Таблиця В.9 – Порівняння часу підготовки захищеного каналу τ_{setup} для профілів IPsec, OpenVPN, WireGuard та XRay

Тип захищеного оверлею	τsetup, мс
IPsec	185
OpenVPN	142
WireGuard	38
XRay	76

Таблиця В.10 – Залежність коефіцієнта успішної доставки $П_{e2e}$ від коефіцієнта надлишковості φ для профілів IPsec, OpenVPN і WireGuard при SNR=3та 6 дБ

φ	WireGuard, 3 дБ	IPsec, 3 дБ	OpenVPN, 3 дБ	WireGuard, 6 дБ	IPsec, 6 дБ	OpenVPN, 6 дБ
0.00	0.42	0.39	0.36	0.58	0.55	0.51
0.10	0.76	0.72	0.68	0.90	0.87	0.84
0.20	0.95	0.93	0.90	0.98	0.97	0.96
0.30	0.99	0.985	0.97	1.00	0.995	0.99
0.40	0.995	0.992	0.985	1.00	0.998	0.995
0.50	0.998	0.997	0.992	1.00	1.00	0.998

Таблиця В.11 – Залежності BER(SNR) для профілів без FEC і з FEC за різних значень φ та для IPsec

SNR, дБ	Без FEC	FEC φ=0,10	FEC φ=0,20
0	0.26	0.18	0.11
2	0.11	0.065	0.032
4	0.032	0.013	0.0050
6	0.0050	0.0018	0.00050
8	0.00050	0.00015	0.000040
10	0.000040	0.000040	0.000040

Таблиця В.12 – Залежності BER(SNR) для профілів без FEC і з FEC за різних значень φ та для OpenVPN

SNR, дБ	Без FEC	FEC φ=0,10	FEC φ=0,20
0	0.28	0.20	0.13
2	0.12	0.075	0.035
4	0.036	0.016	0.0060
6	0.0065	0.0022	0.00070
8	0.00070	0.00020	0.000050
10	0.000060	0.000050	0.000050

Таблиця В.13 – Залежності BER(SNR) для профілів без FEC і з FEC за різних значень φ та для WireGuard

SNR, дБ	Без FEC	FEC φ=0,10	FEC φ=0,20
0	0.24	0.15	0.10
2	0.09	0.050	0.027
4	0.027	0.010	0.0035
6	0.0032	0.0011	0.00030
8	0.00030	0.000080	0.000020
10	0.000020	0.000020	0.000020

Таблиця В.14 – Залежності BER(SNR) для профілів без FEC і з FEC за різних значень φ та для XRay

SNR, дБ	Без FEC	FEC φ=0,10	FEC φ=0,20
0	0.25	0.12	0.11
2	0.10	0.030	0.014
4	0.032	0.0035	0.0055
6	0.0055	0.00030	0.00060
8	0.00060	0.000020	0.000040
10	0.000050	0.000020	0.000040

Таблиця В.15 – Виграш кодування G_{code} для профілів IPsec, OpenVPN, WireGuard та XRay за різних значень φ

φ	IPsec, Gcode (дБ)	OpenVPN, Gcode (дБ)	WireGuard, Gcode (дБ)	XRay, Gcode (дБ)
0.00	0.0	0.0	0.0	0.0
0.05	0.9	0.8	1.1	1.0
0.10	1.8	1.6	2.1	2.0
0.20	3.0	2.7	3.5	3.3
0.30	3.8	3.4	4.3	4.0

Таблиця В.16 – Часові залежності SNR, коефіцієнта надлишковості φ та коефіцієнта успішної доставки $П_{e2e}$ при роботі адаптивного методу керування.

Час, с	SNR, дБ	φ	Пе2е
0	6.0	0.10	0.989
10	6.0	0.10	0.991
20	5.0	0.15	0.983
30	4.0	0.22	0.972
40	3.0	0.30	0.961
50	4.5	0.20	0.978
60	6.0	0.10	0.992

Таблиця В.17 – Порівняння значень M_{eff} для профілів IPsec, OpenVPN та WireGuard.

Профіль	M_eff, байт
IPsec	1320
OpenVPN	1280
WireGuard	1360

Таблиця В.18 – Порівняння η та структури h_{tot} для профілів IPsec, OpenVPN та WireGuard

Профіль	h_net	h_FEC	h_VPN	h_prx	h_tot	η
IPsec	0.04	0.18	0.125	0.000	0.345	0.83
OpenVPN	0.04	0.18	0.165	0.000	0.385	0.77
WireGuard	0.04	0.18	0.080	0.000	0.300	0.86

Таблиця В.19 – Порівняння коефіцієнта успішної доставки $П_{e2e}$в для профілів IPsec, OpenVPN і WireGuard при SNR=3 дБ та різних значеннях коефіцієнта надлишковості

Профіль VPN	Пе2е, φ = 0	Пе2е, φ = 0,2	Пе2е, φ = 0,3
IPsec	0.39	0.93	0.98
OpenVPN	0.36	0.92	0.97
WireGuard	0.42	0.94	0.98

Таблиця В.20 – Залежності BER(SNR) та FER(SNR) для профілів без FEC і з FEC при різних значеннях φ

SNR, дБ	BER без FEC	BER φ=0,10	BER φ=0,20	BER φ=0,30	FER без FEC	FER φ=0,10	FER φ=0,20	FER φ=0,30
0	$2.3\cdot10^{-1}$	$1.3\cdot10^{-1}$	$8.5\cdot10^{-2}$	$5.5\cdot10^{-2}$	0.85	0.78	0.72	0.68
1	$1.5\cdot10^{-1}$	$8.5\cdot10^{-2}$	$5.2\cdot10^{-2}$	$2.8\cdot10^{-2}$	0.80	0.63	0.42	0.30
2	$8.5\cdot10^{-2}$	$4.5\cdot10^{-2}$	$2.3\cdot10^{-2}$	$1.0\cdot10^{-2}$	0.60	0.38	0.15	0.08
3	$4.0\cdot10^{-2}$	$1.8\cdot10^{-2}$	$7.0\cdot10^{-3}$	$2.5\cdot10^{-3}$	0.38	0.19	0.05	0.025
4	$1.0\cdot10^{-2}$	$4.0\cdot10^{-3}$	$1.3\cdot10^{-3}$	$3.5\cdot10^{-4}$	0.18	0.08	0.02	0.008
5	$3.0\cdot10^{-3}$	$1.0\cdot10^{-3}$	$3.5\cdot10^{-4}$	$8.0\cdot10^{-5}$	0.07	0.025	0.006	0.002
6	$8.0\cdot10^{-4}$	$2.5\cdot10^{-4}$	$7.0\cdot10^{-5}$	$1.5\cdot10^{-5}$	0.025	0.008	0.0018	0.0005
7	$2.0\cdot10^{-4}$	$5.0\cdot10^{-5}$	$1.2\cdot10^{-5}$	$2.0\cdot10^{-6}$	0.010	0.0025	0.0004	0.0001
8	$4.0\cdot10^{-5}$	$8.0\cdot10^{-6}$	$1.5\cdot10^{-6}$	$1.0\cdot10^{-7}$	0.003	0.0005	0.00008	0.00002
9	$8.0\cdot10^{-6}$	$1.0\cdot10^{-6}$	$2.0\cdot10^{-7}$	$1.0\cdot10^{-7}$	0.0008	0.0001	0.00001	0.00001

Таблиця В.21 – Порівняння профілів IPsec, OpenVPN і WireGuard за показниками τ_{95} – ξ_{frag}

Профіль	φ	τ95, мс	ξfrag, %
IPsec	0.00	111	1.25
IPsec	0.05	120	0.92
IPsec	0.10	127	0.45
IPsec	0.20	135	0.20
IPsec	0.30	141	0.00
OpenVPN	0.00	114	4.70
OpenVPN	0.05	124	3.50
OpenVPN	0.10	133	2.10
OpenVPN	0.20	143	0.80
OpenVPN	0.30	151	0.00
WireGuard	0.00	107	0.80
WireGuard	0.05	115	0.52
WireGuard	0.10	121	0.22
WireGuard	0.20	129	0.00
WireGuard	0.30	136	0.00

Таблиця В.22 – Порівняння профілів IPsec, OpenVPN і WireGuard за показниками goodput та завантаження CPU

Профіль	φ	Goodput, Мбіт/с	Завантаження CPU, %
IPsec	0.00	9.85	36
IPsec	0.05	9.62	40
IPsec	0.10	9.42	49
IPsec	0.20	8.72	59
IPsec	0.30	8.25	70
OpenVPN	0.00	9.18	34
OpenVPN	0.05	8.95	39
OpenVPN	0.10	8.66	45
OpenVPN	0.20	8.22	54
OpenVPN	0.30	8.02	61
WireGuard	0.00	10.55	30
WireGuard	0.05	10.15	36
WireGuard	0.10	9.85	39
WireGuard	0.20	9.22	48
WireGuard	0.30	8.88	55

Таблиця В.23 – Результати дослідження характеристик каналу без використання FEC та VPN (p_{loss})

p_loss, %	Throughput, Мбіт/с	RTT, мс	QoS (MOS)	Індекс стабільності
0	85	40	4.2	0.92
2	76	60	3.6	0.78
4	63	85	3.0	0.61
6	48	115	2.3	0.44
8	33	152	1.8	0.28

Таблиця В.24 – Результати дослідження характеристик каналу без використання FEC та VPN (SNR)

SNR, дБ	BER	FER
10	6.0×10^{-3}	2.8×10^{-1}
12	2.5×10^{-3}	1.1×10^{-1}
14	9.0×10^{-4}	4.5×10^{-2}
16	3.5×10^{-4}	2.3×10^{-2}
18	1.5×10^{-4}	1.2×10^{-2}
20	7.0×10^{-5}	8.0×10^{-3}

Таблиця В.25 – Результати дослідження характеристик каналу з використанням FEC (p_{loss})

p_loss, %	Throughput, Мбіт/с	RTT, мс	QoS (MOS)	Індекс стабільності
0	100	45	4.5	0.96
2	96	54	4.2	0.90
4	88	67	3.8	0.84
6	78	83	3.3	0.76
8	69	102	2.9	0.66

Таблиця В.26 – Результати дослідження характеристик каналу з використанням FEC (SNR)

SNR, дБ	BER без FEC	BER FEC (Хеммінг 7,4)
10	6.0×10^{-3}	1.0×10^{-3}
12	2.5×10^{-3}	3.0×10^{-4}
14	9.0×10^{-4}	7.0×10^{-5}
16	3.5×10^{-4}	2.0×10^{-5}
18	1.5×10^{-4}	8.0×10^{-6}
20	7.0×10^{-5}	4.0×10^{-6}

Таблиця В.27 – Результати дослідження характеристик каналу з використанням VPN (p_{loss})

p_loss, %	Профіль	Throughput, Мбіт/с	RTT, мс	QoS (MOS)	Індекс стабільності
0	IPsec	95	70	3.8	0.82
2	IPsec	82	92	3.2	0.65
4	IPsec	69	122	2.6	0.50
6	IPsec	58	155	2.2	0.36
8	IPsec	49	192	1.8	0.24
10	IPsec	40	238	1.7	0.14
0	OpenVPN	88	50	4.1	0.78
2	OpenVPN	73	67	3.5	0.60
4	OpenVPN	57	86	2.9	0.46
6	OpenVPN	45	112	2.5	0.32
8	OpenVPN	36	145	2.0	0.21
10	OpenVPN	29	182	1.4	0.10
0	WireGuard	108	32	4.5	0.90
2	WireGuard	98	45	4.0	0.83
4	WireGuard	85	62	3.4	0.71
6	WireGuard	73	83	2.9	0.57
8	WireGuard	64	108	2.6	0.43
10	WireGuard	55	138	2.3	0.31

Таблиця В.28 – Результати дослідження характеристик каналу з використанням VPN (SNR)

SNR, дБ	BER IPsec	BER OpenVPN	BER WireGuard	FER IPsec	FER OpenVPN	FER WireGuard
10	2.0×10^{-3}	5.0×10^{-3}	5.0×10^{-4}	2.0×10^{-2}	5.0×10^{-2}	5.0×10^{-3}
12	8.0×10^{-4}	2.0×10^{-3}	1.5×10^{-4}	7.0×10^{-3}	2.0×10^{-2}	1.5×10^{-3}
14	3.0×10^{-4}	8.0×10^{-4}	5.0×10^{-5}	2.5×10^{-3}	8.0×10^{-3}	5.0×10^{-4}
16	1.2×10^{-4}	3.0×10^{-4}	2.0×10^{-5}	1.0×10^{-3}	3.5×10^{-3}	2.0×10^{-4}
18	5.0×10^{-5}	1.2×10^{-4}	1.0×10^{-5}	5.0×10^{-4}	1.8×10^{-3}	1.0×10^{-4}
20	2.5×10^{-5}	6.0×10^{-5}	5.0×10^{-6}	2.5×10^{-4}	8.0×10^{-4}	5.0×10^{-5}

Таблиця В.29 – Результати дослідження характеристик каналу з використанням FEC + VPN (p_{loss})

p_loss, %	Профіль	Throughput, Мбіт/с	RTT, мс	QoS (MOS)	Індекс стабільності
0	FEC + IPsec	115	58	4.1	0.95
2	FEC + IPsec	96	76	3.6	0.89
4	FEC + IPsec	78	99	3.0	0.84
6	FEC + IPsec	64	128	2.5	0.71
8	FEC + IPsec	50	162	2.1	0.57
10	FEC + IPsec	39	205	1.7	0.44
0	FEC + OpenVPN	105	42	3.7	0.92
2	FEC + OpenVPN	85	55	3.1	0.84
4	FEC + OpenVPN	67	73	2.6	0.74
6	FEC + OpenVPN	53	95	2.1	0.63
8	FEC + OpenVPN	41	123	1.7	0.48
10	FEC + OpenVPN	30	158	1.3	0.34
0	FEC + WireGuard	125	25	4.5	0.97
2	FEC + WireGuard	106	39	4.0	0.92
4	FEC + WireGuard	89	55	3.5	0.85
6	FEC + WireGuard	74	75	3.0	0.71
8	FEC + WireGuard	61	96	2.6	0.60
10	FEC + WireGuard	49	120	2.3	0.47

Таблиця В.30 – Результати дослідження характеристик каналу з використанням FEC +VPN (SNR)

SNR, дБ	BER FEC+IPsec	BER FEC+OpenVPN	BER FEC+WireGuard	FER FEC+IPsec	FER FEC+OpenVPN	FER FEC+WireGuard
10	3.0×10^{-3}	8.0×10^{-4}	1.5×10^{-4}	3.0×10^{-2}	8.0×10^{-3}	3.0×10^{-3}
12	9.0×10^{-4}	2.0×10^{-4}	5.0×10^{-5}	1.0×10^{-2}	2.5×10^{-3}	9.0×10^{-4}
14	3.0×10^{-4}	6.0×10^{-5}	2.0×10^{-5}	4.0×10^{-3}	8.0×10^{-4}	3.0×10^{-4}
16	1.0×10^{-4}	2.0×10^{-5}	8.0×10^{-6}	1.5×10^{-3}	3.0×10^{-4}	1.3×10^{-4}
18	3.5×10^{-5}	8.0×10^{-6}	3.5×10^{-6}	7.0×10^{-4}	1.5×10^{-4}	7.0×10^{-5}
20	1.5×10^{-5}	4.0×10^{-6}	1.5×10^{-6}	3.0×10^{-4}	7.0×10^{-5}	4.0×10^{-5}