ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захищена корпоративна мережа на базі CryptoIP-448»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Юрій ФЕСАЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ФЕСАЙ Юрій
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Захищена корпоративна мережа є критично важливим компонентом IT-інфраструктури будь-якого підприємства. Вона гарантує безпеку та конфіденційність даних, а також оптимізує взаємодію між співробітниками, забезпечуючи доступ до ресурсів незалежно від їхнього розташування.

Розробка захищеності корпоративної мережі є ключовим етапом у створенні інформаційної інфраструктури. Вона не лише забезпечує захист інформації, а й підвищує ефективність роботи та знижує IT-витрати підприємства.

Актуальність дослідження. Актуальність проблеми захищеності корпоративної мережі полягає у необхідності забезпечити захист конфіденційної інформації підприємства від розголошення, витоку і несанкціонованого доступу. Забезпечення безпеки корпоративних мереж у сучасному інформаційному просторі стає дуже важливим завданням для організацій у контексті зростаючих складних кіберзагроз.

Запорука успіху будь-якого підприємства - захист корпоративної мережі.

Компанії оперують значними обсягами конфіденційних даних: від важливих документів до фінансової інформації та персональних даних клієнтів. Несанкціонований доступ до цих відомостей загрожує серйозними наслідками: витоком даних, порушенням прав власності, фінансовими втратами та репутаційними ризиками.

Актуальність дослідження також полягає у потребі впровадження високонадійного методу захисту корпоративної мережі з використанням технології CryptoIP-448, що базується на криптографічному алгоритмі із значною стійкістю та підтримкою апаратної реалізації, що створює захищене середовище для обміну інформацією, і є важливим для корпоративної галузі, де передаються комерційні дані.

Об'єкт дослідження. Захищена корпоративна мережа, що включає апаратно-програмні засоби забезпечення інформаційної безпеки.

Предмет дослідження. Дослідити пристрій криптографічного захисту інформації IP-шифратор "CryptoIP-448", у корпоративну мережу для забезпечення криптографічного захисту передачі даних.

Мета роботи. Побудова захищеної корпоративної мережі з використанням пристрою криптографічного захисту CryptoIP-448, яка забезпечує високий рівень безпеки, ефективності та масштабованості мережевої інфраструктури.

Наукові завдання: Для досягнення поставленої мети у роботі вирішуються наступні наукові завдання: проведення аналізу сучасних загроз і методів захисту корпоративних мереж; дослідження дійсних апаратно-програмних засобів криптографічного захисту; перегляд особливостей реалізації захисту на основі CryptoIP-448; розроблення архітектури захищеної корпоративної мережі на базі CryptoIP-448; проведення експериментального тестування ефективності запропонованої моделі; порівняння отриманих результати з іншими рішеннями.

Методи дослідження. Проаналізувати джерела, нормативні документи, сучасні технології захисту, методи математичного моделювання, криптографічного аналізу, експериментального тестування та аналізу ефективності.

Практичне значення отриманих результатів. Можливість впровадження розробленої моделі у корпоративні мережі для підвищення рівня безпеки, на підприємствах, фінансових установах, державних структурах, IT-компаніях.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Постановка проблеми захищеності корпоративної мережі

Корпоративна мережа - це організаційна комп'ютерна інфраструктура організації, що забезпечує обмін даними між комп'ютерами та іншими пристроями на підприємстві. Основною метою корпоративної мережі є підвищення ефективності та продуктивності бізнесу шляхом спільної роботи та обміну інформацією між різними підрозділами та співробітниками [13]

Термін «корпоративна мережа» використовується для позначення об'єднання кількох мереж, кожна з яких може бути побудована на різних технічних, програмних та інформаційних принципах. [3]

Комп'ютерна, або обчислювальна, мережа - це сукупність комп'ютерів, пов'язаних між собою лініями зв'язку, які утворюються за допомогою кабелів і комунікаційних пристроїв.[8]

Основні складові корпоративної мережі:

1. Люди - спеціалісти з інформаційної безпеки, мережевих адміністраторів та користувачів мережі.

2. Програми – операційні системи, бази даних, програми для роботи з електронною поштою тощо.

3. Апарати - комп'ютери, роутери, комутатори, сервери, модеми та інші пристрої, необхідні для створення мережі.

Головним завданням корпоративної мережі є підтримка роботи підприємства, що володіє цією мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. Корпоративні мережі не надають послуг стороннім організаціям або користувачам. Дана мережа об'єднує офіси, підрозділи і інші структури, що знаходяться віддалено один від одного.

Захищена корпоративна мережа підприємства складається з комп'ютерів, серверів, маршрутизаторів та інших мережевих пристроїв, які взаємодіють між собою. Основні складові корпоративної мережі наведені в таблиці 1.1

Таблиця 1.1.

Основні компоненти корпоративної мережі

Назви компонентів корпоративної мережі	Визначення компонентів корпоративної мережі	Завдання з питань захисту
Сервери	Центральні комп'ютери, які забезпечують обробку та зберігання інформації та надання доступу до неї користувачам	Для захисту мережі важливо мати захищені сервери з встановленими захисними програмами.
Робочі станції	Комп'ютери, які використовуються працівниками підприємства для роботи з даними та програмним забезпеченням.	Важливо захищати робочі станції від вірусів та інших загроз.
Мережеві комутатори	пристрої, які забезпечують з'єднання різних комп'ютерів та інших пристроїв в мережі.	Для захисту мережі важливо використовувати комутатори з підтримкою безпеки.
Маршрутизатори	пристрої, які забезпечують маршрутизацію даних в мережі	Потрібно використовувати маршрутизатори з підтримкою безпеки та захисту мережі від зовнішніх атак
Брандмауер Firewall	пристрій або програма, яка захищає мережу від зовнішніх загроз, фільтруючи вхідні та вихідні пакети даних	Може блокувати підозрілі IP-адреси, порти або протоколи, а також виявляти спроби вторгнення або атаки тощо.
Віртуальна приватна мережа (VPN)	Технологія, яка дозволяє створювати безпечне з'єднання між двома точками в мережі Інтернет.	Використання VPN дозволяє забезпечити безпеку передачі даних між різними підрозділами підприємства та зовнішніми користувачами
Антивірусне програмне забезпечення	Програмне забезпечення, яке захищає комп'ютери від вірусів, шпигунських програм та інших загроз	Потрібно оновлювати антивірусне ПЗ, оскільки нові версії часто включають покращені технології захисту та виявлення загроз.
Системи моніторингу та логування	Технології, які дозволяють відстежувати дії	Для захисту мережі важливо мати системи моніторингу та логування з підтримкою

(Network Monitoring System)	користувачів та виявляти відхилення в роботі мережі	виявлення загроз та аналізу поведінки користувачів.
Системи контролю доступу	Технології, які дозволяють обмежувати доступ користувачів до різних ресурсів в мережі	Потрібно використовувати системи контролю доступу з підтримкою різних рівнів доступу та аутентифікації користувачів.
Фізичні засоби захисту	засоби, які використовуються для захисту компонентів мережі від фізичних атак, таких як крадіжка або пошкодження обладнання	Для захисту мережі важливо використовувати фізичні засоби захисту, такі як камери спостереження, контроль доступу до приміщень та інші.

Для забезпечення ефективної роботи підприємства та захисту його від різноманітних загроз, необхідно здійснити комплексну розробку захищеної корпоративної мережі. Цей відповідальний процес передбачає детальне вивчення сучасних технологій та методів мережевої безпеки. Кінцевою метою є створення надійної та безпечної інфраструктури, яка стане запорукою стабільності бізнесу.

1.2 Аналіз загроз корпоративної мережі та їх наслідки

Інформаційна сфера є однією з найбільш важливих у суспільстві, і її захист визначається серед пріоритетів державної політики.

Сучасні інформаційні системи стають дедалі складнішими, і разом з цим зростає кількість потенційних вразливостей корпоративних мереж. Для захисту корпоративних мереж існує поняття «інформаційна безпека мережі».

Інформаційна безпека мережі - захищеність інформації й інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприйнятної шкоди суб’єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримувальної інфраструктури. [4]

Корпоративна мережа перебуває у захищеному стані, якщо забезпечено її конфіденційність, доступність і цілісність.

Конфіденційність (confidentiality) – це гарантія того, що секретні дані будуть доступні тільки для тих користувачів, які мають дозвіл на доступ; такі користувачі називаються легальними або авторизованими.

Доступність (availability) – це гарантія того, що авторизовані користувачі завжди зможуть отримати доступ до даних.

Цілісність (integrity) – це гарантія того, що дані зберігають вірні значення. Вона забезпечується шляхом заборони неавторизованим користувачам змінювати, модифікувати, знищувати або створювати дані.[6]

Інформаційну небезпеку для корпоративної мережі створюють інформаційні загрози, які поширюються в інформаційному просторі. Інформаційні загрози – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в інформаційній сфері. [12]

Загроза – це будь-яка дія, що може бути спрямована на порушення інформаційної безпеки системи. [6]

У Державному стандарті України “Захист інформації. Технічний захист інформації. Основні положення” – ДСТУ 3396.0-96 частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися:

- технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

- несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.[18]

В інформаційній системі усі загрози поділяють на 2 групи: зовнішні та внутрішні, кожна з яких, ділитися на навмисні (зловмисні співробітники) та випадкові загрози.[1]

Випадкові загрози: помилки персоналу та користувачів; неправильне збереження інформації; випадкове знищення або заміна; збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; некоректна робота програмного забезпечення, через зараження комп’ютерними вірусами тощо.

Навмисні загрози: несанкціонований доступ до інформації і мережевих ресурсів; розкриття і модифікація даних і програм, їх копіювання; розкриття, модифікація або підміна трафіка обчислювальної мережі; розробка і поширення комп’ютерних вірусів, введення в програмне забезпечення логічних бомб; крадіжка магнітних носіїв і розрахункових документів, руйнування архівної інформації або навмисне її знищення; фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; перехоплення та ознайомлення з інформацією, яка передана по каналах зв’язку. [12]

Класифікація загроз за критеріями:

- аспект інформаційної безпеки (доступність, цілісність, конфіденційність), проти якого загрози спрямовані в першу чергу;

- компоненти інформаційних систем, на які загрози націлені (дані, програми, апаратура, підтримувальна інфраструктура);

- спосіб здійснення (випадкові/навмисні дії природного/техногенного характеру);

- розташуванням джерела загроз (усередині/поза розглянутим інформаційними системами); [6]

Найбільшими прикладами загроз безпеки корпоративних мереж на сьогоднішній день є: шкідливе програмне забезпечення (віруси, троянці, черв'яки), IPкібератаки, атака «відмова в обслуговуванні» - DDoS-атаки, програми-вимагачі, компрометація корпоративної електронної пошти або-афера (BEC – Business Email Compromise), атаки нульового дня; соціальна інженерія: (фішинг, фармінг, претекстинг, рейтинг, смішинг; підслуховування (Sniffing), перехоплення сеансу (Session Hijacking), відео- та аудіо спостереження, Кеш-трепінг (Cash Trapping - захоплення готівки), витік даних, підміна довіреного

суб'єкту (IPspoofing), атака експлоїта, аналіз мережного трафіку, мережна розвідка (Ping Sweep), зловживання довірою, застосування ботнетів, анонімний доступ в мережу тощо. [11]

Згідно останнього звіту Cybersecurity Forecast (Прогноз кібербезпеки) від Google, ландшафт загроз постійно змінюється: це і атаки на основі штучного інтелекту, і геополітична напруженість, і складні кіберзлочинні атаки [19]

Основні типи та механізми сучасних кіберзагроз для організацій згідно звіту Cybersecurity Forecast наведено в таблиці 1.2.

Таблиця 1.2.

Основні типи та механізми сучасних кіберзагроз для організацій

Тип загрози	Механізм атаки	Наслідки
Використання ШІ (Штучного інтелекту)	Фішинг, deepfake, генерація контенту	Підробка особистих даних в обхід вимоги «знай свого клієнта» (KYC), компрометація даних, втрати довіри
Геополітичні атаки	Кібершпигунство, злом edge-пристроїв, дезінформація	Злам інфраструктури, злив конфіденційної інформації
RaaS (вимагачі)	Атаки через орендоване ПЗ	Шифрування систем, вимагання викупу, зупинка роботи
Соціальна інженерія	Cold-calling, фішингові листи, підроблені резюме	Доступ до систем, втрати даних, шахрайство
Web3-компрометація	Злам smart contracts, компрометація гаманців	Втрата активів, правовий ризик, підрив екосистеми
Ланцюги постачання	Зараження через сторонні компоненти	Зараження всього середовища, витік через залежності

Проблеми забезпечення інформаційної безпеки в корпоративних комп'ютерних мережах обумовлені загрозами безпеці для локальних робочих станцій, локальних мереж і атаками на корпоративні мережі, що мають вихід в загальнодоступні мережі передачі даних. Мережні атаки настільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються великою

складністю. Інші – здатні здійснити звичайні оператори, навіть не припускаючи, які наслідки може мати його діяльність. [21]

Наслідки таких загроз можуть включати витік конфіденційної інформації, розкрадання інформації, втрата даних та маніпуляція ними, фінансові втрати, пошкодження репутації компанії та повне припинення роботи інформаційних сервісів. Тому підприємства всіх рівнів повинні впроваджувати надійні засоби захисту та постійно оновлювати свою інфраструктуру безпеки.

1.3 Аналіз сучасних практик захисту корпоративної мережі

Сьогодні корпоративні мережі потребують надійного захисту, адаптації до нових викликів. Компанії вживають заходи широкого спектра для захисту своєї інформації від несанкціонованого доступу та кібератак. Вони приділяють значну увагу технологічним інноваціям для забезпечення безпеки своїх даних, використовуючи криптографічні методи та впроваджують багаторівневі системи автентифікації.

В сучасній практиці мережного захисту інформації корпоративних мереж застосовуються різні способи:

- міжмережні екрани (Firewall) використовуються для блокування атак із зовнішнього середовища (наприклад, Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони керують проходженням мережного трафіку згідно з правилами (policies) безпеки, встановлюються на вході мережі, аби розмежувати внутрішні і зовнішні (загального доступу) мережі;

- системи виявлення вторгнень (IDS - Intrusion Detection System) застосовують для запобіганню спроб несанкціонованого доступу як із зовні, так і всередині мережі, а також захисту від атак типу «відмова в обслуговуванні» (наприклад, Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Ці системи, здатні запобігти шкідливим діям, знижуючи цим самим час простою в результаті атаки й витрати на підтримання працездатності мережі;

- віртуальні приватні мережі (VPN - Virtual PrivateNetwork) застосовують з метою організації захищених каналів передавання даних через незахищене середовище (наприклад, Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator), що забезпечить прозоре для користувача з'єднання локальних мереж, зберігаючи конфіденційність і цілісність інформації завдяки динамічному шифруванню;

- засоби аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (наприклад, Symantec Enterprise Security Manager, Symantec NetRecon). Застосовується для запобігання можливим атакам на корпоративну мережу, оптимізації витрат на захист інформації й контролю стану захищеності мережі [9];

- антивірусні програмні засоби, антивірусні програми: детектори, фаги (лікарі), ревізори та фільтри, здатні виявляти та знищувати віруси, які можуть заразити один пристрій чи усю корпоративну мережу.[14]

- SIEM-системи (Security information and event management – управління інформаційною безпекою та подіями безпеки), програми, які аналізують в онлайн режимі події інформаційної безпеки, отримані від мережевих пристроїв і застосунків. [14]

- списки контролю доступу (Access Control Lists, ACL) перевіряють звернення і потоки трафіку на основі IP-адрес і цільових за стосунків;

- криптографічні засоби-шифрування, в основі якого лежить ключ та певний криптографічний алгоритм, використовують протоколи SSL та HTTPS.

Протокол SSL (англ. Secure Sockets Layer – рівень захищених сокетів) – шифрує дані на канальному рівні моделі OSI. Цей протокол забезпечує кодування на порті. Протокол HTTPS призначений для забезпечення надійного захисту тільки гіпертекстових документів веб-сервера. [14]

- Frame Relay – це протокол канального рівня моделі OSI, що використовується для швидкої передачі кадрів до місця призначення.

- IPSec є протоколом, що працює на мережевому рівні моделі OSI та може працювати в будь-якій мережі, оскільки базується на протоколі IP і може

використовувати всі технології канального рівня. Механізм безпеки в IPSec забезпечується протоколами AH, ESP та IKE, які виконують функцію «безпечного з'єднання»;

- сервіс AAA (автентифікація, авторизація, облік) допомагає легітимним користувачам отримувати доступ до мережевих ресурсів. Автентифікація вимагає від користувачів підтвердження їхньої ідентичності, щоб переконатися, що вони дійсно є тими, за кого себе видають;

- системи запобігання вторгненням (Intrusion Prevention Systems, IPS) ідентифікують загрози, що швидко поширюються, такі як атаки нульового дня або нульові години;

- модель нульової довіри – ZTM. Одним з найважливіших аспектів нульової довіри є визначення ресурсів, що мають бути захищені: дані, застосунки, активи, сервіси, користувачі, пристрої, враховуючи пристрої категорії BYOD. Важливо зрозуміти як між ними відбувається комунікація, які є комунікаційні канали, що є основою для побудови ZTA та створення нових політик безпеки. [22]

- регулярне оновлення ПЗ та патчінг: Забезпечує актуальність програмного забезпечення та операційної системи, зменшуючи ризики використання вразливостей.

- навчання співробітників: Підвищення обізнаності співробітників про загрози кібербезпеки, фішинг та інші методи обману.

- розробка та впровадження політик безпеки: Для встановлення правил та процедур, що регулюють використання інформаційних ресурсів та мереж.

- використання хмарних служб безпеки.

В результаті аналізу використання сучасних практик захисту корпоративних мереж можна стверджувати, що в залежності від загрози необхідно застосовувати відповідний спосіб, який забезпечить надійний захист корпоративної мережі, а в результаті застосування декількох взаємодоповнюючих рішень можливо значно підвищити надійність захисту, оскільки у випадку неефективності одного компонента, інші можуть успішно виявити та нейтралізувати загрозу.[1]

2 ДОСЛІДЖЕННЯ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Методи та засоби захисту комп’ютерних мереж в організаціях

Сьогодні організації використовують багато методів та засобів для побудови надійного захисту комп’ютерних мереж, важливого завдання для забезпечення і збереження конфіденційності інформації.

Комплексне поєднання заходів чотирьох рівнів: законодавчого; адміністративного; процедурного; програмно-технічного сприяє успіху в інформаційній безпеці та допомагає зробити комп’ютерну мережу більш захищеною [1]

Законодавчий рівень захисту: Конституція, нормативні акти, стандарти, міжнародні положення – угоди, ліцензії, патенти, укази, кодекси, інструкції. Зокрема, в Україні це закони "Про інформацію", "Про технічний захист інформації", "Про державну таємницю", нормативні документи Державної служби спеціального зв’язку та захисту інформації, які регламентують правила обробки інформації [7]

Адміністративний рівень захисту: політика безпеки (Наприклад, Британський стандарт BS7799:1995);

Процедурний рівень захисту: управління персоналом, режимом безпеки, фізичний захист, підтримка працездатності; реагування на порушення режиму безпеки; планування відновних робіт.

Програмно-технічний рівень захисту: фізичні засоби – засоби, які повинні створювати фізичні перешкоди на шляху зловмисників; апаратні засоби – різні технічні конструкції, які можуть протидіяти розголошенню відповідної інформації корпоративної мережі, її витоку та спробам несанкціонованого доступу до неї; програмні засоби – програми чи програмні комплекси, що можуть забезпечити захист інформації корпоративної мережі; криптографічні засоби – алгоритми, за допомогою яких шифрується інформація корпоративної мережі, яка захищається: [14]

Існують сервіси безпеки програмно-технічних засобів захисту:

– ідентифікація та автентифікація;

– управління доступом;

– протоколювання і аудит;

– шифрування;

– контроль цілісності;

– екранування;

– аналіз захищеності;

– забезпечення відмовостійкості;

– забезпечення безпечного відновлення;

– тунелювання;

– управління.[1]

Для захисту мереж використовуються різні методи захисту, що дозволяють забезпечити конфіденційність, цілісність та доступність.

Методи ідентифікації і автентифікації - криптографічні методи, що виконуються програмним або апаратно-програмним способом. Ідентифікація визначає, конкретного користувача, автентифікація підтверджує його ідентичність.

Ідентифікація користувачів полягає у встановленні, закріпленні за кожним з них унікального ідентифікатора у вигляді номера, шифру, коду. Кожен із видів ідентифікації має свої переваги та недоліки.

Систему технологій ідентифікації та автентифікації показано на рисунку 2.1.

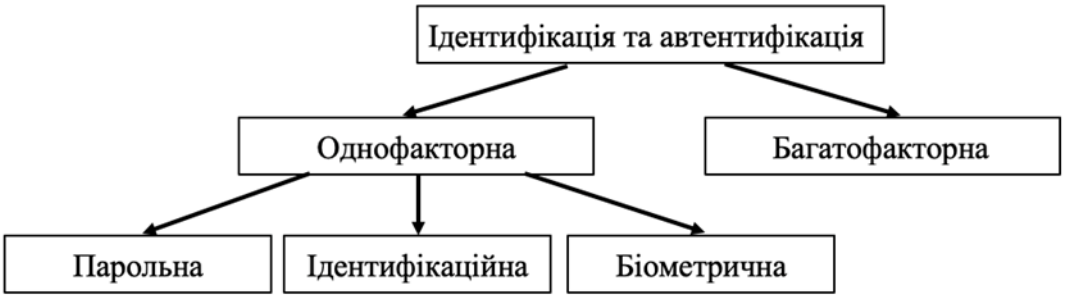


Рис. 2.1. Система технологій ідентифікації та автентифікації

Однофакторні методи автентифікації: парольні (паролі, ключові фрази, введені з клавіатури); ідентифікаційні (носієм інформації є об'єкти: дискета,

магнітна карта, смарт-карта, штрих-кодова карта тощо); біометричні, які поділяються на статичні і динамічні.

Статичні методи біометричної автентифікації - за відбитками пальців, за геометрією руки, за райдужною оболонкою ока, за сітківкою ока, за за геометрією особи; динамічні методи біометричної автентифікації - за голосом, за рукописним почерком тощо.

Багатофакторні методи автентифікації - комбінації різних методів, найчастіше ідентифікаційного та логічного.

Криптографічні методи захисту: шифрування (симетричне, асиметричне), хешування, електронний цифровий підпис, криптографічні протоколи.

Шифрування - це процедура, яка перетворює інформацію у форму, зрозумілу лише авторизованим особам. Механізми шифрування припускають використання криптографічних перетворень даних для того, щоб зробити їх нечитабельними [10]

Алгоритми криптографічних перетворень можуть бути закритими, або відкритими. Перевагу надають відкритим алгоритмам, вони надійні та стандартизовані. Шифрування досягається за допомогою математичних алгоритмів, які використовують ключі для шифрування та розшифрування даних.

Алгоритми перетворень можуть бути симетричними (коли для зашифровування і розшифровування використовуються однакові ключі) або асиметричними, у яких використовують два різні ключі. Один ключ відкритий, яким зашифровують повідомлення, а другий – закритий, який призначений для розшифровування. У цих системах немає необхідності у захищеному каналі для пересилання ключів. Одержувач генерує пару ключів і пересилає відправнику відкритий ключ. Цей ключ можна не зберігати в таємниці, бо він не дає змогу розшифровувати повідомлення. Закритий ключ одержувач зберігає в себе для розшифровування.[2]

Для захисту мереж існують наступні види шифрування: канальне, наскрізне, абонементне, комбіноване; програмне та апаратне.[20]

Для шифрування даних найбільш широко застосовують три види шифраторів: апаратні, програмно-апаратні і програмні.

Апаратні шифратори мають переваги над програмними:

- апаратний датчик випадкових чисел створює випадкові числа для формування надійних ключів шифрування та електронного цифрового підпису;

- апаратна реалізація криптоалгоритму гарантує його цілісність;

- шифрування і зберігання ключів здійснюються в самій платі шифратора, а не в оперативній пам'яті комп'ютера;

- завантаження ключів в шифрувальний пристрій з електронних ключів Touch Memory (i-Button) і смарт-карт проводиться безпосередньо, а не через системну шину комп'ютера і оперативної пам'яті, що виключає можливість перехоплення ключів;

- з допомогою апаратних шифраторів можна реалізувати системи розмежування доступу до комп'ютера і захисту інформації від несанкціонованого доступу;

- застосування спеціалізованого процесора для виконання обчислень розвантажує центральний процесор комп'ютера; також можна встановити декілька апаратних шифраторів на одному комп'ютері, що ще більш підвищує швидкість обробки інформації (це перевага притаманна шифраторам для шини PCI);

- застосування парафазних шин при створенні шифропроцесора виключає загрозу читання ключової інформації за коливаннями електромагнітного випромінювання, що виникають при шифруванні даних, в ланцюгах «земля - живлення» пристрою.

- шифрування даних проходить швидше, ніж у програмно-апаратного шифрування.[25]

VPN (Virtual Private Network – віртуальна приватна мережа) - об’єднання локальних мереж і окремих комп’ютерів через відкрите зовнішнє середовище передавання інформації в єдину віртуальну мережу, яка забезпечує захист інформації, що в ній циркулює. Така мережа формується як деяка підмножина реальної мережі, з каналами зв’язку, що моделюються реальними каналами [5]

VPN формується шляхом побудови віртуальних захищених каналів зв'язку, що створюються на базі відкритих каналів зв'язку загальнодоступної мережі. Ці

віртуальні захищені канали зв'язку називаються тунелями VPN. Мережа VPN дозволяє за допомогою тунелів VPN з'єднати центральний офіс, офіси філій, офіси бізнес партнерів і видалених користувачів і безпечно передавати інформацію через Інтернет .

Віртуальні захищені приватні мережі часто використовуються великими компаніями (банки, відомства, державні структури), і є ключовим елементом сучасної корпоративної інфраструктури, забезпечують захищений доступ до ресурсів компанії через Інтернет, що дозволяє досягати високого рівня безпеки, гнучкості та економічної ефективності в управлінні мережами.

Класифікація VPN:

- Захищені. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.
- Довірчі. Прикладом довірчих VPN є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol)

VPN за призначенням:

- Intranet VPN. Використовують для об'єднання в єдину захищену мережу декількох розподілених приватних мереж, які обмінюються даними за відкритими каналами зв'язку.

- Remote Access VPN. Використовують для створення захищеного каналу між сегментом корпоративної мережі і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера або, перебуваючи у відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

- Extranet VPN. Використовують для мереж, до яких підключаються «зовнішні» користувачі (клієнти).

- Internet VPN. Використовується для надання доступу до інтернету провайдерами, зазвичай якщо по одному фізичному каналу підключаються кілька користувачів.

Підтримка VPN на різних рівнях моделі OSI:

- Канальний рівень: протоколи L2TP, PPTP (Point-to-Point Tunneling Protocol);

- мережевий рівень:протокол L2TP/IPsec (Layer 2 Tunneling Protocol);

- транспортний рівень: SSL / TLS.

Протокол безпеки - опис розподіленого алгоритму, в процесі виконання якого два (чи більше) учасники послідовно виконують певні дії і обмінюються повідомленнями. Послідовність кроків протоколу групується в цикли.[5]

В таблиці 2.1. наведено основні переваги та недоліки VPN протоколів:

Таблиця 2.1.

VPN за протоколами

Назва протоколу	Коротка інформація	Переваги	Недоліки	Застосування
PPTP (Point-to-Point Tunneling Protocol)	Застарілий VPN-протокол	Висока швидкість, простота налаштування.	Низький рівень безпеки.	Для простих завдань, які не потребують високого рівня захисту
L2TP/IPsec (Layer 2 Tunneling Protocol)	Забезпечує більшу безпеку завдяки шифруванню IPsec.	Сумісність із більшістю пристроїв.	Зниження швидкості через подвійне шифрування.	Для захищеного з'єднання в бізнес-середовищах.
OpenVPN	Найпоширеніший протокол із відкритим кодом.	Висока безпека, гнучкість налаштування.	Складніше налаштування.	Корпоративні мережі з високими вимогами до безпеки.
WireGuard	Новітній протокол, що пропонує високу швидкість і сучасне шифрування	Швидкість роботи, простота налаштування.	Новизна, яка може спричинити сумісність із деякими пристроями.	Для сучасних бізнес-мереж.

SSTP (Secure Socket Tunneling Protocol)	Протокол від Microsoft із підтримкою SSL/TLS.	Висока сумісність із Windows, надійне шифрування.	Обмежена підтримка інших платформ.	Корпоративні мережі на базі Windows.

Розглянемо більш детально деякі протоколи VPN.

1. VPN на основі протоколу IPSec (Internet Protocol Security).

Основне призначення протоколу IPSec (Internet Protocol Security) - забезпечення безпечної передачі даних по мережах IP. Система стандартів IPSec забезпечує: автентифікацію, цілісність, конфіденційність, надійне управління ключами, тунелювання.

IPsec - це протокол «точка-точка», в якому одна сторона шифрує, інша розшифровує, і обидві сторони мають однаковий ключ або ключі. IPsec має два режими роботи: транспортний і тунельний режим.

Основу IPSec складають протоколи AH, ESP та IKE.

Завдання протоколу AH (Authentication Header) полягає у забезпеченні цілісності та автентичності даних. Протокол ESP (Encapsulating Security Payload) призначений для шифрування переданих даних і також може виконувати ті ж функції, що й протокол AH. Протокол IKE (Internet KeyExchange) грає допоміжну роль, забезпечуючи кінцевим точкам доступ до секретних ключів, необхідних для протоколів AH та ESP для встановлення безпечного каналу.[23]

2. Протокол SSL/TLS (Secure SocketsLayer/Transport Layer Security) - популярний для криптографічного захисту інформації.

SSL призначений для створення безпечного каналу або тунелю між веб-браузером і вебсервером, щоб захищати будь-яку інформацію, якою обмінюється в захищеному тунелі. Використання сертифікатів SSL дозволяє клієнтам аутентифікуватися на серверах. Щоб підтвердити свою особу, клієнти надають серверу сертифікат. [23]

Протокол SSL забезпечує захист даних між сервісними протоколами (такими як HTTP, FTP та ін.) і транспортними протоколами (TCP/IP)за допомогою сучасної

криптографії. Ядром протоколу SSL є технологія комплексного використання асиметричних і симетричних криптосистем. В якості алгоритмів асиметричного шифрування використовуються такі алгоритми, як RSA (розробки RSA Data Security Inc.), а також алгоритм Діффі-Геллмана.[1]

TLS використовує асимметричне шифрування для автентифікації, симетричне шифрування для конфіденційності та коди автентичності повідомлень для збереження цілісності повідомлення. Ядром протоколу є технологія комплексного використання асиметричних і симетричних криптосистем. [5]

3. WireGuard - це протокол VPN для створення зашифрованих мережевих з'єднань, протокол зв’язку та безкоштовне програмне забезпечення з відкритим вихідним кодом. WireGuard простий у використанні, має гарну продуктивність, надійну безпеку, високу швидкість, акцентує увагу на використанні криптографії, зокрема протоколи Noise, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF та безпечні довірені конструкції

В основі WireGuard лежить концепція під назвою Cryptokey Routing, яка працює шляхом зв'язування відкритих ключів зі списком тунельних IP-адрес, які дозволені всередині тунелю.[29]

В результаті, для досягнення високого рівня корпоративної безпеки потрібно використовувати комплекс заходів захисту. Першочергово необхідно побудувати зовнішній периметр мережі з використанням технологій VPN, систем виявлення та запобігання вторгненням, міжмережевих екранів, а також забезпечити захищені з'єднання для віддалених користувачів. [24]

2.2 Порівняльний аналіз сучасних засобів захисту

З розвитком інформаційних технологій та зростанням кіберзагроз, забезпечення надійного криптографічного захисту інформації є ключовим завданням для державних установ та приватних компаній. Особливої актуальності набуває застосування сертифікованих апаратних засобів криптозахисту, що відповідають національним стандартам України.

Проведено порівняльний аналіз сучасних апаратних засобів захисту інформації: CryptoIP-448, CryptoIP-459 та Канал-201.

IP-шифратор CryptoIP-448 – це доступний вітчизняний апаратний IP-шифратор, призначений для захисту IP-трафіку локальних мереж, терміналів і автоматизованих робочих місць. Підтримує усі національні алгоритми криптографічного захисту. Завдяки компактності та спрощеному адмініструванню підходить для малих офісів або польових структур. «CryptoIP-448» підтримує архітектуру відкритих ключів (PKI) і розроблений у відповідності із законодавчою базою України.[26]

Рисунок 2.2. IP-шифратор «CryptoIP-448»

«CryptoIP-448» забезпечує:

- підтримку повнозв’язної структури віртуальної приватної мережі (VPN);
- шифрування і інкапсуляцію пакетів IP трафіку;
- прозору передачу шифрованих пакетів по тунелях VPN;
- аутентифікацію та ідентифікацію абонентів.[26]

У пристрої реалізуються криптографічні алгоритми:

- шифрування пакетів IP-трафіку - ГОСТ 28147-89;
- електронний цифровий підпис - ДСТУ 4145-2002;
- формування сеансового ключа на еліптичних кривих;
- взаємодії з інфраструктурою відкритих ключів - X.509. [26]

«CryptoIP-448» підтримує інтерфейси:

- 10/100Base-T - для підключення до локальної мережі;
- 10/100Base-T - для підключення до комунікаційного обладнання;
- USB 1.1 - для підключення до ПЕОМ (конфігурація). [26]

Технічні характеристики:

- пропускна здатність - не менше 5 Мбіт/с або не менше 1000 пакетів/с;
- кількість VPN-тунелів - не менше 1000;
- робочий діапазон температур навколишнього середовища від +5°С до +45°С;
- живлення пристрою здійснюється від мережі змінного струму напругою 85 - 265 і номінальною частотою 50 або 60 Гц;
- пристрій виконаний у вигляді автономного блоку розмірами 160х124х28 мм. [26]

Переваги "CryptoIP-448":

- гарантований захист від компрометації ключів (використання смарт-карт, сертифікованих за Common Criteria 5+);
- генерація, розподіл і використання ключів відповідає законодавчій базі України;
- можливість дистанційного керування IP-шифратором і його ключовою системою. [26]

IP-шифратор CryptoIP-459

CryptoIP-459 - це вітчизняний апаратний засіб криптографічного захисту інформації, що призначений для забезпечення безпечного обміну даними в мережах IP. Пристрій сертифікований відповідно до ТУ У 26.2-32248356-022:2014 та має експертний висновок Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ).

Рисунок 2.3. IP-шифратор «CryptoIP-459»

IP-шифратор реалізує крізне шифрування IP-трафіку, що передається між захищеними локальними обчислювальними мережами через публічну IP-мережу. Це дозволяє будувати віртуальні приватні мережі (VPN) з високим рівнем безпеки. Реалізовані алгоритми:

- шифрування - ДСТУ ГОСТ 28147:2009;
- хешування - ГОСТ 34.311-95;
- ЕЦП - ДСТУ 4145-2002;
- формування сеансових ключів - ДСТУ ISO/IEC 15946-3:2006.
- Підтримуються криптосистеми з відкритими ключами (PKI) або з ручним розподілом сертифікатів.

Інтерфейси:

- 2 × Ethernet 10/100Base-T (WAN);
- 2 × Ethernet 10/100Base-T (LAN);
- 1 × USB 2.0 (конфігурація).

Технічні характеристики:

- швидкість шифрування — до 266 Мбіт/с;
- пропускна здатність — не менше 180 Мбіт/с;
- кількість VPN-тунелів — до 2047;
- носій ключів — SIM або CryptoCard-317;
- живлення — 85–265 В, 50/60 Гц;
- розміри — 204 × 157 × 37 мм;
- температура експлуатації — від +0°C до +45°C [16]

IP-шифратор «Канал-201»

Пристрій для захисту інформації «IP-шифратор "Канал-201"» створений для криптографічного захисту інформації в синхронних і асинхронних каналах зв’язку (RS-485, V.24 тощо). Не призначений для IP-мереж, але ідеально підходить для спеціалізованих систем зв’язку, наприклад у військових або урядових структурах. Має вбудовані криптомодулі, генератори ключів, підтримує смарт-карти для автентифікації.

Рисунок 2.4. – IP-шифратор «Канал-201»

Функції IP-шифратора:

- шифрування та контроль цілісності IP-пакетів;
- інкапсуляцію IP-пакетів та маршрутизацію між мережними інтерфейсами;
- прийом та введення в дію ключових даних;
- встановлення захищених з’єднань з іншими IP-шифраторами.[16]

Конструкція та технічні характеристики засобу:

- IP-шифратор виконаний у вигляді окремого малогабаритного мережного пристрою.[16]
- Конструктивно IP-шифратор являє собою мініатюрну системну платформу у металевому корпусі та має 2 мережних інтерфейси Ethernet 10/100. [16]

IP-шифратор реалізує наступні криптографічні алгоритми та протоколи:

- шифрування за ГОСТ 28147-89 (режим простої заміни, режим гамування та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);
- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої.
- Швидкість шифрування – до 40 Мбіт/с. [16]

Порівняння параметрів цих шифраторів наведено в таблиці 2.2.

Таблиця 2.2.

Порівняльна таблиця параметрів шифраторів

Параметр	CryptoIP-448	CryptoIP-459	Канал-201
Розробник	ТОВ «АВТОР»	ТОВ «АВТОР»	Вітчизняний виробник
Пропускна здатність	до 100 Мбіт/с	до 266 Мбіт/с	до 40 Мбіт/с
VPN-тунелі	до 1000	до 2047	Н/Д
Алгоритми	ДСТУ ГОСТ 28147:2009, ЕЦП	ДСТУ ГОСТ 28147:2009, ЕЦП	ДСТУ ГОСТ 28147:2009, ЕЦП
Інтерфейси	2×Ethernet, USB	Ethernet, USB	RS-485, V.24, оптика
Сертифікація	ДССЗЗІ України	ДССЗЗІ України	ДССЗЗІ України
Застосування	Малі офіси, мобільні групи	Великі організації	Спецканали, автономні мережі

Порівнявши технічні параметри, призначення, можна зробити такі висновки:

- CryptoIP-448 - доступний та компактний пристрій для малого бізнесу або польових підрозділів;

- CryptoIP-459 - найбільш продуктивне рішення для масштабних IP-мереж.

- Канал-201- спеціалізоване рішення для не-IP-каналів, де важливий рівень фізичної та логічної ізоляції

Завдяки розвитку вітчизняної криптографічної індустрії українські установи можуть ефективно будувати багаторівневі системи захисту відповідно до стандартів інформаційної безпеки.

2.3 Принцип роботи CryptoIP-448

Принцип роботи IP-шифратора CryptoIP-448 детально описаний в Настанові з експлуатації IP-шифратора CryptoIP-448:

IP-шифратор CryptoIP-448 призначений для організації криптографічно захищених віртуальних приватних мереж (VPN), зокрема для криптографічного захисту інформації, яка міститься у пакетах трафіку IP-мереж. [15]

CryptoIP-448 забезпечує функції криптографічного захисту конфіденційної інформації: функції шифрування, імітозахисту, електронного цифрового підпису.[15]; реалізує тунельний режим роботи VPN.

Захист інформації здійснюється шляхом інкапсуляції оригінальних IP-пакетів в нові пакети. При цьому оригінальні IP-пакети вміщуються всередину нових IP-пакетів в зашифрованому вигляді. Окрім стандартного заголовка новий IP-пакет містить UDP-заголовок - спеціальний заголовок, який несе в собі криптографічно значущу інформацію, та додатковий заголовок для захисту від повторення трафіку, який шифрується разом з відкритим пакетом. [15]

Для захисту трафіку використовується протокол, який забезпечує: конфіденційність та цілісність даних; імітозахищенність даних; автентифікацію джерела даних; захист трафіку від аналізу; приховування топології внутрішньої мережі. [15]

Шифрування інформації здійснюється відповідно до ДСТУ ГОСТ 28147:2009, забезпечує формування сеансового ключа з використанням асиметричних алгоритмів на еліптичних кривих та використанням ЕЦП, забезпечує підтримку режиму взаємодії з центром сертифікації ключів у відповідності до протоколу X.509. [15]

Носієм ключових даних використовується мікропроцесорна картка «CryptoCard» ТУ У 30.0-32248356-002:2006 у форматі SIM-картки.

Максимальна пропускна здатність IP-шифратора:

- CryptoIP-448, CryptoIP-448/5v, - не менше 5 Мбіт/с.

Кількість облікових записів протоколу ARP – 128 MAC-адрес на обидва

мережні інтерфейси.

У режимі роботи з використанням центру сертифікації ключів максимальна кількість напрямків захищеного зв’язку – 1024, та 60 - у режимі автономної роботи. Максимум пропускної здатності досягається при одночасній активності не більше 42 тунелів. [15]

Наявність IP та MAC адреси на кожному мережному інтерфейсі. [15]

Наявність функції табличного задавання списку захищених з’єднань з занесенням у тунель трафіку за ознакою «IP адреса + маска під мережі».

Робота в якості мережного шлюзу (Network Gateway).

Підтримка роботи з іншими мережними шлюзами (тобто підтримка Default Gateway для зовнішнього та внутрішнього мережних інтерфейсів).

Можливість зміни конфігурації IP-шифратора з використанням інтерфейсу USB 1.1, або віддаленого захищеного підключення по мережі IP з використанням протоколу UDP.

IP-шифратор має наступні інтерфейси:

CryptoIP-448, CryptoIP-448/5v: два інтерфейси 10/100BASE-T для підключення до локальної мережі та до комунікаційного обладнання; USB 1.1 – для підключення до ПЕОМ.

Живлення IP-шифратора здійснюється від мережі змінного струму напругою 220 В ± 20% і номінальною частотою 50 Гц. Споживана потужність IP-шифратора не перебільшує 10 В·А

Живлення IP-шифраторів CryptoIP-448/5v, CryptoIP-428/5v здійснюється від постійного струму напругою (5±0,5) В. Споживана потужність не перебільшує 5 Вт.

Діапазон температур навколишнього середовища в умовах експлуатації CryptoIP-448, CryptoIP-448/5v від плюс 5 до плюс 45 ºС. Діапазон температур навколишнього середовища в умовах зберігання - від мінус 40 до плюс 60 ºС. Підвищена відносна вологість навколишнього середовища в умовах експлуатації - до 80 %, при температурі плюс 25 ºС.

IP-шифратор складається з окремого електронного пристрою – блоку обробки трафіку (БОТ), кабелів для його підключення та програмного забезпечення.

БОТ має світлову індикацію, два з'єднувачі для підключення IP- шифратора до мережного обладнання, з'єднувач для підключення до порту комп'ютера, що відповідає Universal Serial Bus Specification Revision 1.1 і мережний перемикач.

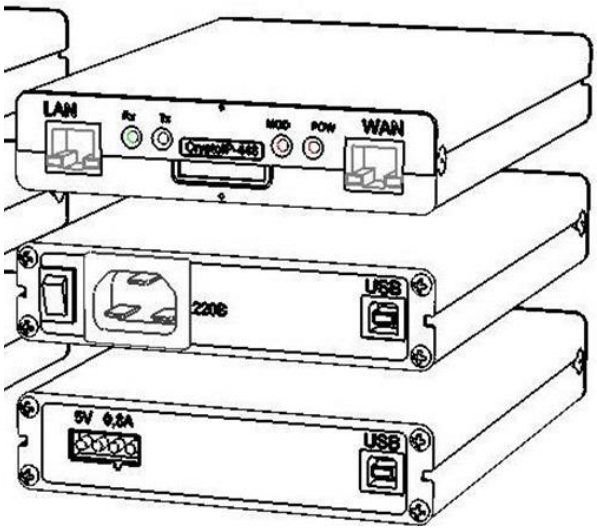


Рис. 2.5. Вигляд спереду «CryptoIP-448», «CryptoIP-448/5v», вигляд ззаду «CryptoIP-448», вигляд ззаду «CryptoIP-448/5v» [15]

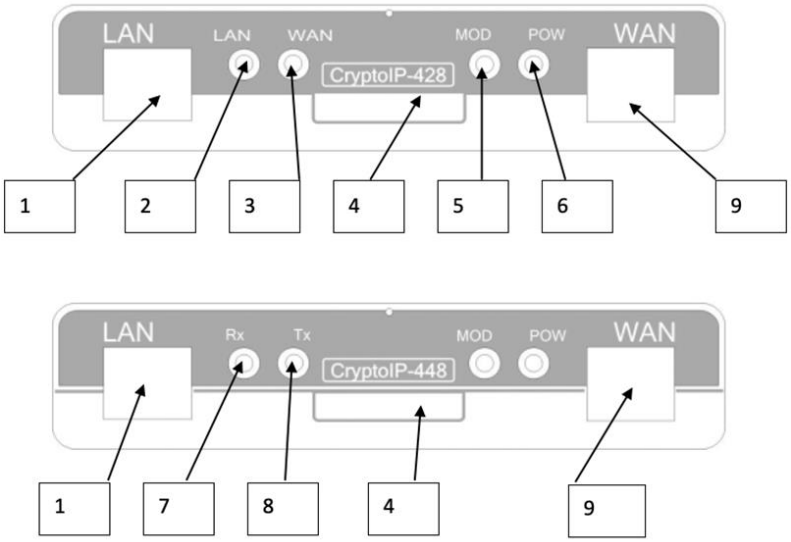


Рис. 2.6. Зовнішній вигляд передньої панелі БОТ [15]

1. З'єднувач RJ-45 підключення по інтерфейсу 10/100 Base T до внутрішньої мережі.
2. Сигнальний світлодіод LAN - «Внутрішня мережа».
3. Сигнальний світлодіод WAN - «Зовнішня мережа».
4. Тримач SIM модулів
5. Сигнальний світлодіод MOD - «Режим».
6. Сигнальний світлодіод POW - «Живлення».
7. Сигнальний світлодіод RX - «Прийом».

8. Сигнальний світлодіод ТХ - «Передача».

9. З’єднувач підключення по інтерфейсу 10/100 Base T до зовнішньої мережі.

Основний режим роботи IP-шифратора – з підтримкою центра сертифікації ключів. У цьому режимі роботи криптографічна система IP- шифратора передбачає звернення до центра сертифікації ключів у процесі входження до сеансу захищеного зв’язку з метою отримання сертифіката відкритого ключа сторони, з якою встановлюється сеанс.

Узагальнена схема мережних з’єднань при роботі IP-шифраторів в цьому режимі представлена на рисунку 2.7.

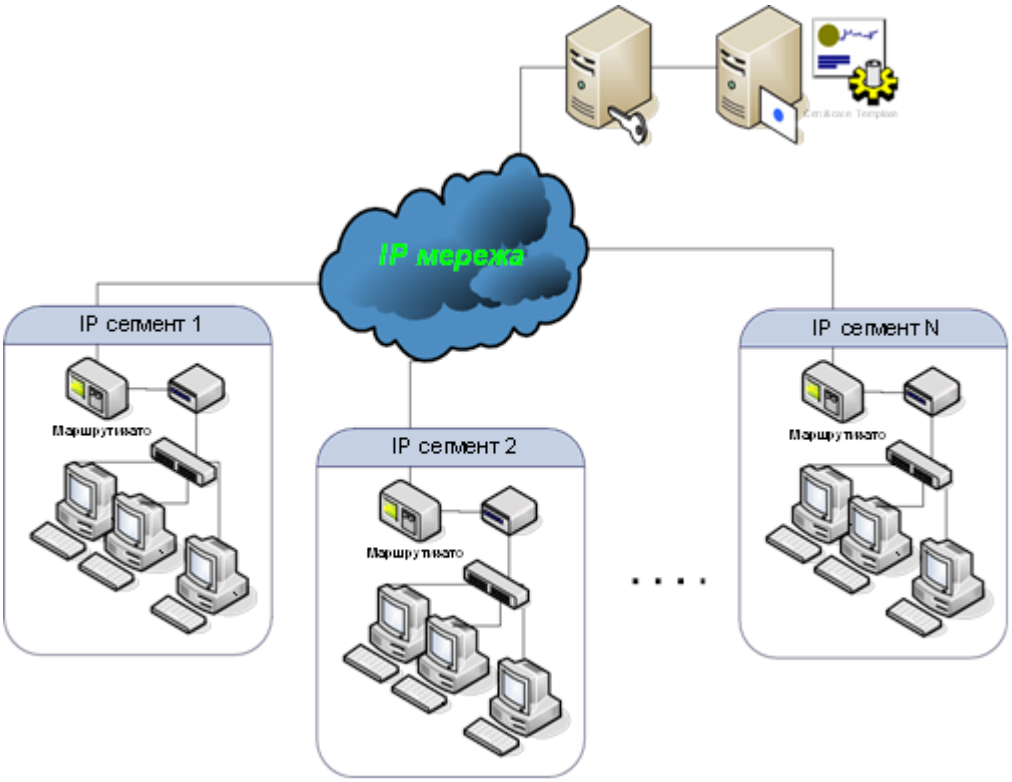


Рис. 2.7. Схема організації VPN з використанням центру сертифікації ключів [15]

Другий режим IP-шифратора – режим ручної доставки ключів. У цьому режимі роботи передбачається, що відкриті ключі усіх сторін, які складають захищену VPN, містяться на носії ключових даних (НКД) и замінюються за необхідністю в ручному режимі. Як правило, генерація ключових даних для даного режиму здійснюється в центрі управління ключами з використанням спеціального програмного забезпечення.

Як носій ключових даних використовується мікропроцесорна картка. IP-шифратор переходить до відповідного режиму роботи, у залежності від того, мікропроцесорна картка якого типу встановлена до інтерфейсного пристрою для карток (далі – „карткоприймач”).

Схема організації VPN у режимі з ручної доставкою ключів

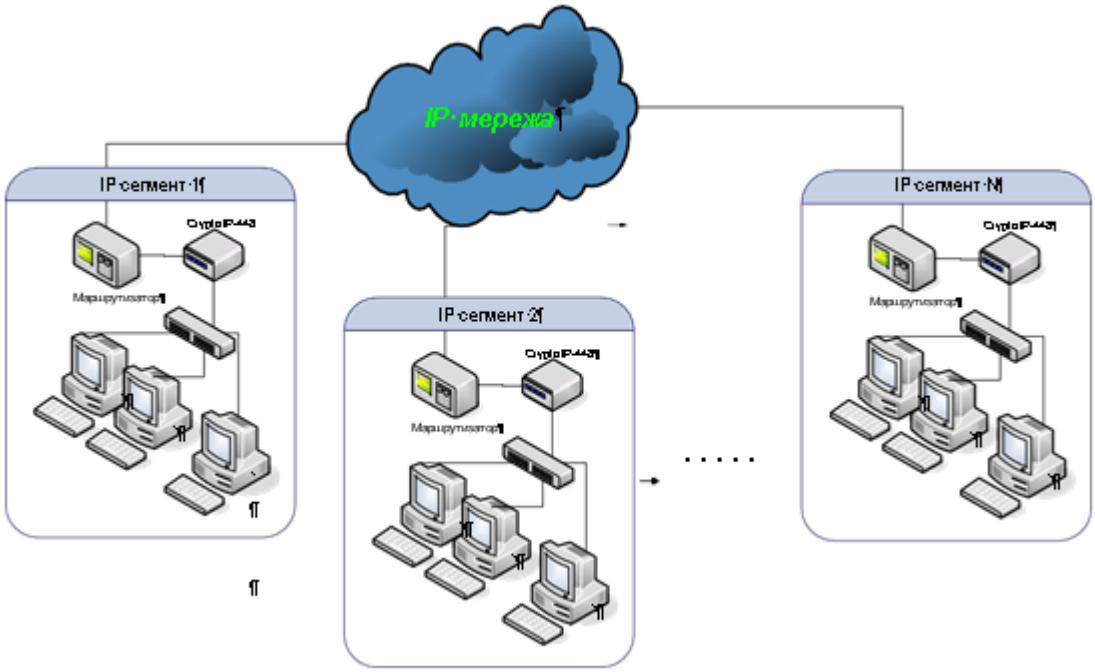


Рис. 2.8. Схема організації VPN у режимі з ручної доставкою ключів [15]

Типові схеми включення для організації VPN.

Організація захищеної VPN шляхом з’єднання засобами локальної мережі.

У даній схемі IP-шифратори з’єднуються засобами Ethernet. Центр сертифікації ключів може знаходитися у межах IP-сегмента (IP-адреса та маска підмережі), яким з’єднані зовнішні інтерфейси IP-шифраторів. У іншому випадку трафік повинен маршрутизуватися до ЦСК.

IP-сегменти: «LAN сегмент 1», «LAN сегмент 2», …, «LAN сегмент N» повинні знаходитись у різних підмережах (IP-адреса та маска підмережі повинні бути вказаними таким чином, щоб діапазон IP-адрес був унікальним для кожної підмережі). Схему зображено на рисунку 2.9.

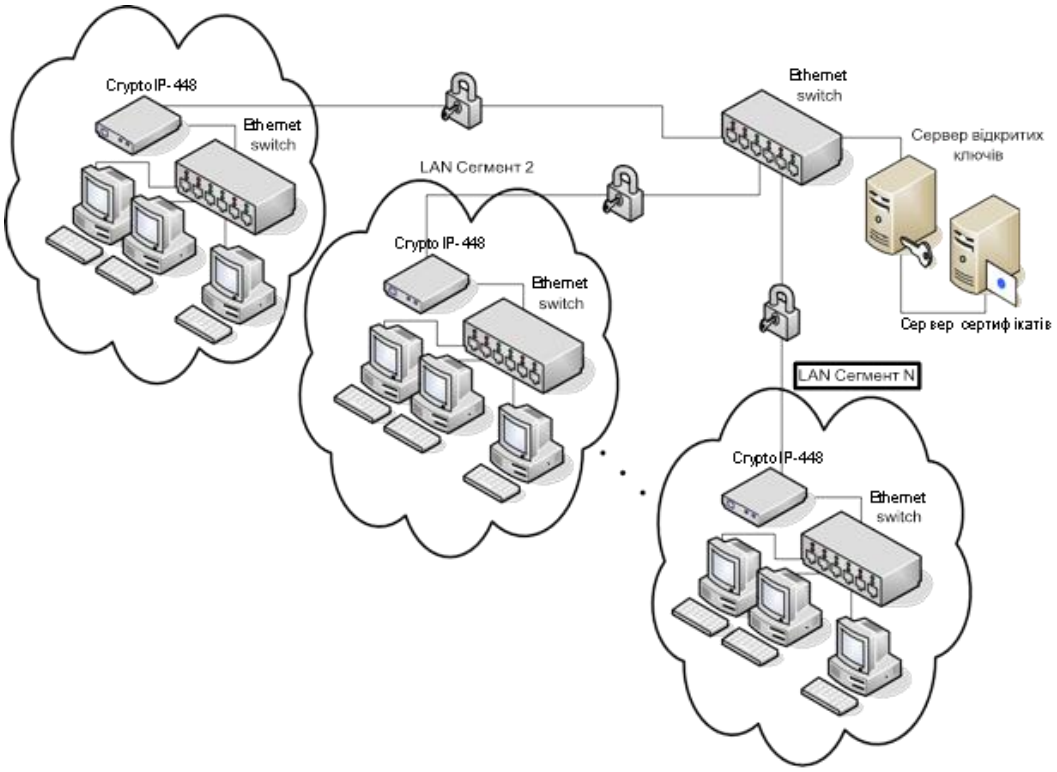


Рис. 2.9. Схема організації захищеної VPN на засобах LAN [15]

Як видно зі схеми, зовнішні з’єднання здійснюються за допомогою засобів комутації Ethernet. Наявність ЦСК у даному випадку опціональна у залежності від вибраного режиму роботи IP-шифраторів.

Організація VPN з використанням корпоративної IP-мережі або мережі загального користування IP-шифратори підтримують повнозв'язну структуру захищеної VPN мережі і не обмежуються “Клієнт-Сервер” структурою. Проте, необхідно враховувати реальні обмеження, які має будь-яке мережне устаткування. Зокрема, для побудови працездатної мережі необхідно, щоб базова мережа була зв'язною.

Необхідно, щоб хоча б один вузол VPN мав фіксовану IP- адресу (не динамічну). При цьому пакети, які повинні передаватися між вузлами з динамічною трансляцією адреси, передаватимуться через вузли з фіксованою адресою. Тому доцільно, щоб центральний VPN вузол і інші вузли, у напрямку яких передається велике число пакетів, і вузли, для яких існують жорсткі обмеження за часом доставки пакетів, мали фіксовану IP- адресу.

У схемі з використанням корпоративної IP-мережі, IP-шифратори з’єднуються один з іншим через мережне обладнання, яке здійснює перехід до

транспортної частини IP-мережі (як правило, через IP-маршрутизатори, які підтримують роботу з заданими каналами). IP-сегменти «LAN сегмент 1»,

«LAN сегмент 2», …, «LAN сегмент N» повинні знаходитись у різних підмережах (IP-адреса та маска підмережі повинні бути вказаними таким чином, щоб діапазон IP-адрес був унікальним для кожної підмережі).

Організація VPN за комбінованою схемою

Комбінована схема організації VPN представляє собою поєднання двох попередніх схем. Схема VPN, організована за комбінованою схемою, показана на рисунку 2.10.

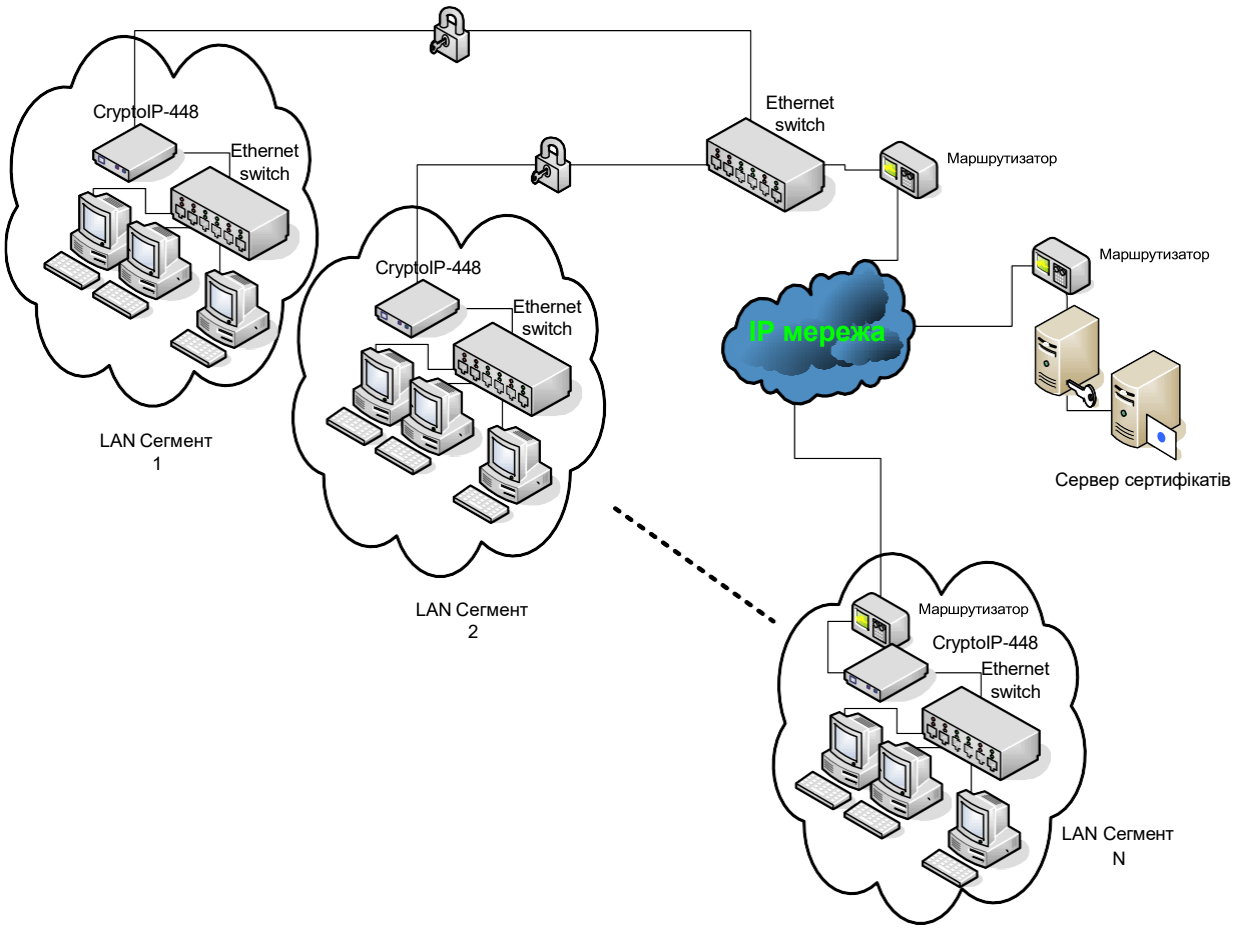


Рис. 2.10. Організація VPN за комбінованою схемою [15]

Як і у попередніх схемах, наявність ЦСК опціональна, у залежності від режиму роботи IP-шифратора. VPN може поєднувати у собі певну кількість логічно об’єднаних IP шифраторів з можливою наявністю ЦСК. IP-сегменти «LAN сегмент 1», «LAN сегмент 2», …, «LAN сегмент N» повинні знаходитись у різних під

мережах (IP-адреса та маска підмережі повинні бути вказаними таким чином, щоб діапазон IP-адрес був унікальним для кожної підмережі).

Організація VPN з використанням PKI архітектури:

PKI архітектура розподілу відкритих ключів в захищених VPN, побудованих на базі IP-шифраторів "CryptoIP-448" реалізована в своєму загальноприйнятому варіанті.

У цьому режимі роботи в конфігурацію мережі додається сервер ЦСК, до якого звертаються IP-шифратори для отримання відкритих ключів кореспондентів.

IP-шифратори взаємодіють з ЦСК не безпосередньо, а через протокольний шлюз, функції якого виконує спеціальний сервер

Сервер “CryptoProxy” повинен мати статичну IP-адресу. IP-адреса сервера “CryptoProxy” вводиться в IP- шифратори в процесі конфігурації. Заміна IP-адрес сервера “CryptoProxy” вимагатиме реконфігурування всіх IP-шифраторів, що працюють з даним сервером. Такого роду реконфігурування може бути виконане дистанційно.

Звернення IP-шифратора до сервера “CryptoProxy” здійснюється при необхідності встановлення зв'язку з певним абонентом і лише в разі, якщо відкритого ключа відповідного абонента в IP-шифраторі на даний момент немає. Якщо напрям резервований, то запит формується лише за наявності зв'язності з шифратором абонента.

Захищена VPN може використовувати для доступу до відкритих ключей більш, ніж один ЦСК та більш, ніж один сервер “CryptoProxy”. Однак кожний IP-шифратор може взаємодіяти тільки з однім сервером “CryptoProxy”.

Уведення до експлуатації

- Підключення мережного кабелю

Підключення IP-шифраторів до мережного обладнання здійснюється за допомогою мережного кабелю «скручена пара» видів STP або UTP, категорії 5 або 5e, який обтиснутий для перехресного з’єднання. Таблиця відповідності контактів та проводів для обтискання кабелю приведена нижче.

Таблиця. 2.3.

Таблиця відповідності контактів та проводів для обтискання кабелю

Розміщення проводів на лівому з'єднувачі:	Розміщення проводів на правому з'єднувачі:
1 – білий (помаранчевий) 2 - помаранчевий 3 - білий (зелений) 4 - синій 5 - білий (синій) 6 - зелений 7 - білий (коричневий) 8 – коричневий	1 – білий (зелений) 2 - зелений 3 - білий (помаранчевий) 4 - синій 5 - білий (синій) 6 - помаранчевий 7 - білий (коричневий) 8 – коричневий

При підключенні кабелю до мережного обладнання, при ввімкненні живлення, повинен засвітитися зеленим кольором правий сигнальний світлодіод відповідного з'єднувача RJ-45 на передній панелі IP-шифратора, що свідчить про встановлення мережного з'єднання. У іншому випадку необхідно перевірити працездатність мережного кабелю та мережного обладнання, до якого здійснюється підключення.

- Конфігурування параметрів роботи IP-шифратора здійснюється відповідно до плануючих документів по організації мережі захищеного зв'язку.

Установлення параметрів мережних інтерфейсів виконується за допомогою конфігураційного програмного забезпечення у відповідності до розділу 2 даного документа. Конфігурування може виконуватися як на етапі до ініціалізації НКІ (при включеному живленні та підключенні по інтерфейсу USB 1.1), так і після, у процесі роботи у захищеній мережі.

Конфігурування IP шифратора полягає у призначенні IP та MAC адрес на кожному мережному інтерфейсі та табличному задаванні списку тунельних з'єднань. У випадку використання зовнішніх шлюзів (маршрутизаторів, тощо), вказуються їх адреси. У режимі роботи з підтримкою центру сертифікації ключів також вказується його IP - адреса та порт.

Діагностика мережних з'єднань здійснюється за допомогою штатних засобів, які є у наявності у адміністратора мережі.

Конфігурування роботи ПЕОМ, які входять до складу захищеної (внутрішньої) мережі, здійснюється за допомогою конфігураційного програмного забезпечення (КПЗ) та полягає у призначенні відповідних властивостей мережного адаптера та протоколу TCP/IP, див. розділ 2.

Таблиця тунелів описує всі з'єднання IP-шифратора з IP-шифраторами абонентів.

- Ініціалізація НКІ здійснюється в Центрі генерації та запису ключових даних “Менеджер ключів” . Ініціалізація полягає у генерації ключових даних, з наступним їх занесенням до НКІ/SIM, задаванні режиму роботи IP- шифраторів, та параметрів взаємодії з ЦСК (при відповідному режимі роботи).

НКІ/SIM для IP-шифраторів постачається у вигляді смарт-картки.

„CryptoCard» ТУ У 30.0-32248356-002:2006, яка є носієм ключової інформації, що визначає режим роботи пристрою.

Для IP-шифраторів можуть бути два види ключових документів:

- E-SM – асиметричні ключі (режим попереднього розподілу ключів).

- PK-SM - асиметричні ключі (режим роботи з Центром сертифікації ключів (ЦСК)).

Запуск IP-шифраторів

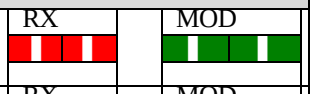
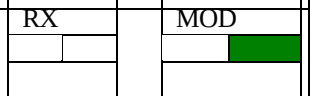
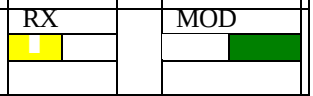
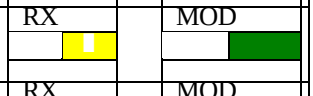
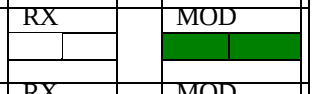
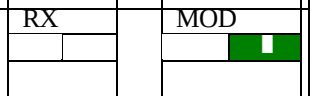
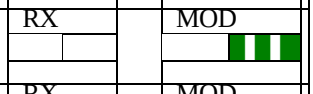
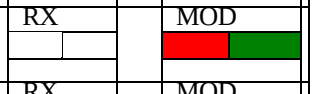
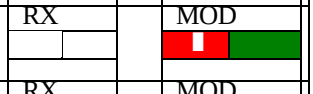
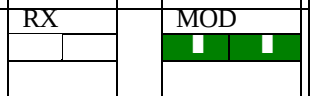
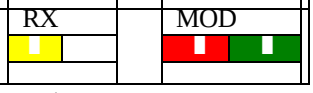
НКІ, який проініціалізований, необхідно вставити до приймальної кишені карткоприймача IP-шифратора та ввімкнути живлення. Повинен засвітитися зелений сигнальний світлодіод «Р».

У процесі запуску IP-шифратора здійснюється тестування його апаратної частини, та криптографічного інтерфейсу. У випадку успішного проходження усіх перевірок повинен засвітитися сигнальний світлодіод

В таблиці 2.4 наведені статусні світлодіоди для CryptoIP 448 та події.

Таблиця 2.4.

Статусні світлодіоди для CryptoIP 448

н\ п	стан \ подія	індикація
0	Початок завантаження пристрою	
1	Готовий до роботи, покажчики датчиків у нормі, внутрішні тести успішні.	
2	Готовий до роботи, ведеться прийом захищеного трафіку	
3	Готовий до роботи, ведеться передача захищеного трафіку	
4	Конфігураційний режим	
5	Готовий до роботи, покажчики датчиків вище/нижче норми	
6	Покажчики датчиків критичні	
7	Відсутня SIM-картка	
8	Помилка обміну з SIM-карткою	
9	Перший старт пристрою, потрібне введення серійного номеру	
10	Внутрішня помилка	

У випадку успішного проходження усіх перевірок IP-шифратор готовий до експлуатації.

Зміна НКІ в процесі роботи захищеної IP мережі може здійснюватися шляхом одночасного виключення всіх IP-шифраторів, заміни старих НКІ на нові і включенням IP-шифраторів.

Передбачена також процедура зміни НКІ, при який не потрібна одночасна заміна НКІ в усіх IP-шифраторах захищеної мережі. Суть процедури полягає в кешуванні ще діючих ключів старого НКІ в енергонезалежній захищеній області пам'яті процесора IP-шифратора до моменту початку дії нових НКІ.

Для обох режимів роботі з асиметричними ключами для зміни НКІ у процесі роботи виконується команда

cache enable <date begin> <date end>,

<date begin> - поточна дата

<date end> - дата закінчення використання кеша та його автоматичного знищення.

Команда може бути сформована та введена засобами локального (консолі КПЗ) або дистанційного керування (ЦУ VPN). Після одержання такої команди пристрій копіює зміст НКІ у захищену енергонезалежну пам'ять центрального процесора.

По завершенні виконання команди в рядку консолі буде виведена інформація про дату початку і дату кінця дії кеша.

Для активізації кеша і вивільнення НКІ необхідно виконати рестарт IP-шифратора. Рестарт IP-шифратора може бути виконаний локально, шляхом виключення і включення живлення не менше ніж на 2 секунди або шляхом локального або дистанційного введення команди “reboot”, виконання якої приведе до перевантаження IP-шифратора.

Після рестарту пристрою він стартує з використанням ключових даних, збережених в кеші. В цей період часу КД з установлених НКІ не використовуються і наявність НКІ в карткоприймачі не є обов'язковою, тому старі НКІ можуть бути витягнуті з карткоприймача без блокування пристрою. На місце старих НКІ повинні бути установлені нові НКІ. Заміна НКІ повинна бути проведена до дати закінчення використання кеша вказаній у відповіді на виконання команди “cache enable”.

Після заміни НКІ перехід на їх використання звичайно здійснюється не відразу після їх установки. Перехід на використання нових НКІ буде виконаний автоматично в момент вичерпання періоду дії кеша (відповідає часу дії кеша, вказаному у відповіді на виконання команди “cache enable”).

Якщо потрібно перевести на нові НКІ, не чекаючи дати закінчення кеша, потрібно локально або віддалено віддати команду “cache disable”. Для читання статусу та дати закінчення кеша віддається команда “cache status”.

У багатьох випадках заміна НКІ в режимі з відкритими ключами обумовлена необхідністю оновлення сертифікату відкритих ключів абонентів захищеної VPN. У таких випадках необхідно синхронізувати виконання процедури заміни НКІ в шифраторі з процедурою заміни сертифіката в сховищі сертифікатів ЦСК.

Для запобігання перервам в зв'язку і забезпечення такої синхронізації необхідно так визначити тимчасові рамки дії кеша, щоб заміна сертифікату в сховищі ЦСК відбувалася протягом часу дії кеша. Друга умова швидкого установлення зв'язку з новими КД полягає у видаленні з оперативної пам'яті всіх кореспондентів старого відкритого ключа абонента, у якого замінені КД (у т.ч. відкритий ключ).

Видалення з оперативної пам'яті IP-шифратора абонента відкритих ключів кореспондентів (одержаних раніше від ЦСК) може бути реалізоване шляхом виконання спеціальної команди “keys -drop”, команди “reboot”, (локально або віддалено) або шляхом виключення і включення живлення.

Запобіжні заходи безпеки під час експлуатації IP-шифратора

Під час експлуатації IP-шифратора:

- не розміщувати IP-шифратори поблизу джерел електромагнітного поля (трансформаторів, розподільчих щитків, силових кабелів, та інших джерел електромагнітного поля);

- заземляти усі елементи мережного обладнання, якщо заземлення IP-шифратора здійснюється через третій заземлюючий провідник мережі живлення – перевірити наявність та якість заземлення шляхом вимірювання опору контуру заземлення;

- розміщувати кабелі живлення, при можливості, у екранованих металевих оболонках;

- обладнати, при можливості, місця групового підключення мережних пристроїв екранованими щитками живлення з необхідною кількістю розеток;

- не використовувати не штатні подовжувачі („переноски”) або саморобні фільтри живлення, виконані у вигляді „переносок”.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ЗАХИЩЕНОЇ МЕРЕЖІ НА БАЗІ CRYPTOIP-448

3.1 Розгортання та налаштування захищеної мережі

Шифратор CryptoIP-448 розміщується на периметрі внутрішньої мережі організації, між захищеним сегментом та зовнішніми мережами (Інтернетом або каналами VPN). Він виконує роль криптографічного шлюзу, який забезпечує шифрування, автентифікацію та контроль цілісності даних.

Основні елементи архітектури:

- Робочі станції (ПК) – кінцеві користувацькі пристрої, підключені до локального комутатора (switch).
- Внутрішній комутатор (LAN Switch) – об’єднує робочі станції та сервери в локальній мережі.
- Маршрутизатор (Router) – з’єднує внутрішню мережу з зовнішньою інфраструктурою. Він приймає трафік з комутатора і спрямовує його на криптошлюз.

CryptoIP-448 встановлений на межі локальної мережі та зовнішнього каналу зв’язку. Внутрішній Ethernet-порт пристрою підключається до маршрутизатора або локальної мережі, зовнішній – до каналу провайдера або до лінії зв’язку з іншим офісом [27]. CryptoIP-448 шифрує IP-пакети, інкапсулює їх у VPN-тунелі та передає через зовнішню мережу (Інтернет або VPN) [27].

- Зовнішня мережа – це Інтернет або віддалена корпоративна мережа філії. На віддаленій стороні для прийому зашифрованих даних повинен бути встановлений аналогічний CryptoIP-448, який розшифровує пакети і передає їх локальній мережі отримувача.

Таким чином, CryptoIP-448 розташовується між внутрішньою мережею та зовнішніми каналами, виконуючи роль шлюзу-шифратора і забезпечуючи захищений обмін даними. У типовій захищеній мережі малого масштабу компоненти розташовуються так, щоб весь зовнішній трафік проходив через CryptoIP-448 перед виходом у Інтернет чи іншу мережу.

Основні етапи маршруту трафіку:

1. Робоча станція (ПК) →
2. Внутрішній комутатор (Switch) →
3. Внутрішній маршрутизатор (Router) →
4. CryptoIP-448 (LAN-порт) →
5. CryptoIP-448 (шифрування) →
6. CryptoIP-448 (WAN-порт) →
7. Зовнішня мережа.

Інтеграція CryptoIP-448 у корпоративну інфраструктуру передбачає:

- Фізичне підключення шифратора двома інтерфейсами:
- Порт Trusted (LAN) підключається до маршрутизатора внутрішньої мережі.
- Порт Untrusted (WAN) - до каналу зв'язку провайдера або маршрутизатора зовнішньої мережі.
- Логічне налаштування:
- Присвоєння IP-адрес обом портам відповідно до підмереж.
- Визначення шифрувальних політик (криптопрофілів).
- Створення правил фільтрації, маршрутизації та доступу.
- Увімкнення журналювання та сповіщень для контролю подій.

CryptoIP-448 підтримує інфраструктуру відкритих ключів (PKI) і працює з цифровими сертифікатами. Це дозволяє автентифікувати пристрої при з’єднанні та формувати захищені VPN-тунелі між об'єктами. [25]

Інсталяція програмного забезечення

Під час своєї роботи, установник запропонує вибір варіантів встановлюваних компонентів. При цьому на вибір будуть доступні дві опції:

- Encryptor and Monitor

- Configurator

Опція *Encryptor and Monitor* виконує установку трьох програмних компонентів IP-шифратора, а саме драйвера, шифратора і монітора, в той час як опція *Configurator* відповідає за установку тільки конфігуратора.

При виборі двох опцій одночасно буде встановлено повний комплект з усіх чотирьох компонентів.

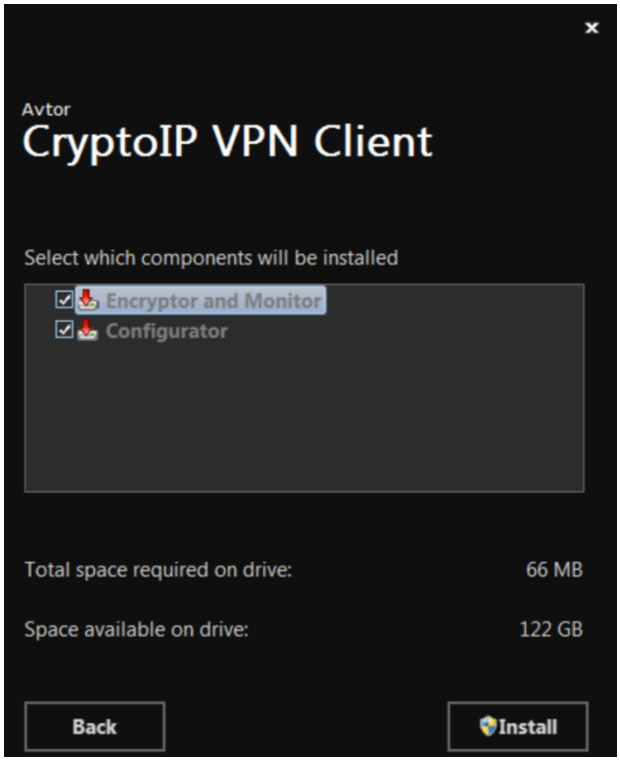


Рис. 3.1 Інсталяція програмного забезечення

Це дозволяє, наприклад, адміністратору, якому не потрібен власне функціонал шифратора, встановити собі на комп'ютер тільки конфігуратор. Згодом він може використовувати його для віддаленого доступу до шифраторів, які їм обслуговуються. З іншого боку, якщо обслуговування шифраторів виконується адміністратором, установка конфігуратора на комп'ютери клієнтів необов'язкова.

Якщо необхідно змінити склад встановлених на комп'ютері програмних компонентів IP-шифратора, необхідно запустити установник повторно. Установник виведе наступне вікно вибору:

На вибір доступні три опції інсталяції, які зображено на рисунку 3.2

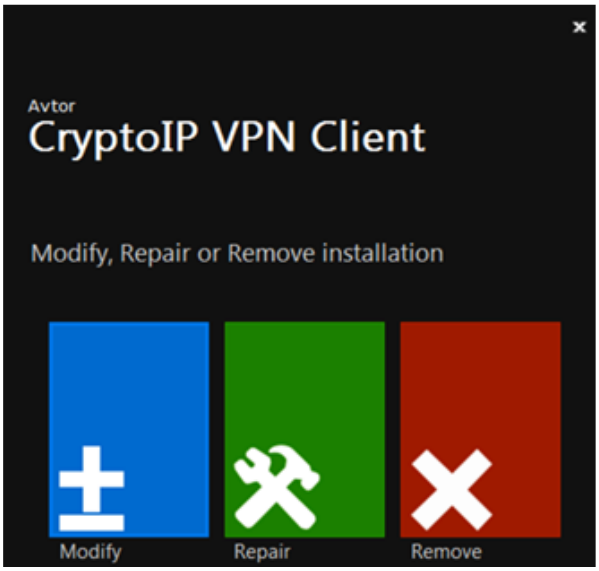


Рис. 3.2. Опції інсталяції

Modify –дозволяє змінити склад встановлених компонент. При виборі опції з'явиться вікно вибору компонент, представлений раніше.

Remove – видалення всіх встановлених компонентів, аналогічно повному видаленню програми засобами операційної системи.

Repair – відновлення пошкодженої програми.

Після запуску файлу на виконання, починається процес установки.

Першим з'являється запит шляху установки. Рекомендується установку компонента шифратора здійснювати в таку папку, для доступу до якої потрібно мати права адміністратора. Установник за замовчуванням пропонує саме таку папку. Після вказівки шляху установки, необхідно натиснути кнопку "Next" для переходу до наступного етапу.

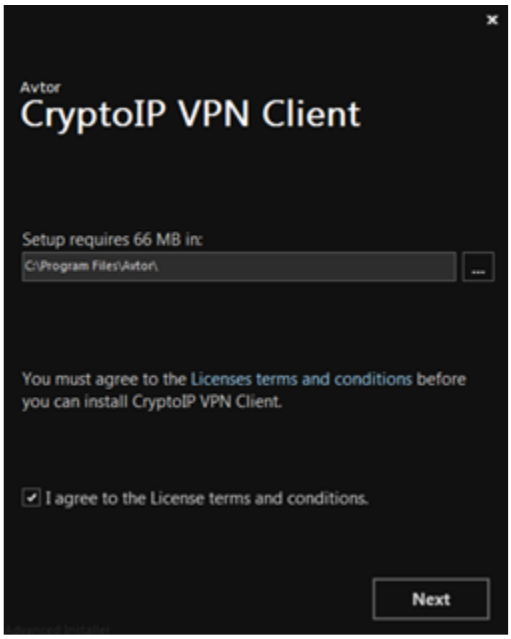


Рис. 3.3. Інсталяція шифратора

Після цього, починається процес установки, який триває 1-2 хвилини. Якщо установка передбачає інсталяцію програмного компонента драйвера IP-шифратора, то в процесі установки буде виданий запит на підтвердження установки драйвера в систему.

Успішне завершення процесу установки обраних компонент супроводжується виведенням на екран вікна з відповідним повідомленням.

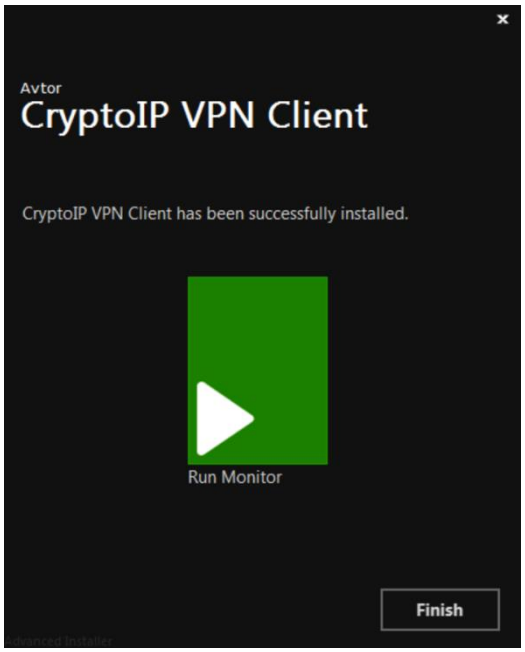


Рис. 3.4. Завершення інсталяції шифратора

Основна програма управління усіма параметрами IP-шифратора – конфігуратор, який є призначеним для користувача інтерфейсом до всієї кількості налаштувань шифратора. Шифратор, будучи службою Windows, не має власного інтерфейсу.

Для своєї роботи конфігуратор не вимагає прав адміністратора, за винятком функції додавання в систему логічного мережевого адаптера, що є необхідним для режиму станції. Відповідно, додавання та налаштування логічного адаптера повинні виконуватися адміністратором.

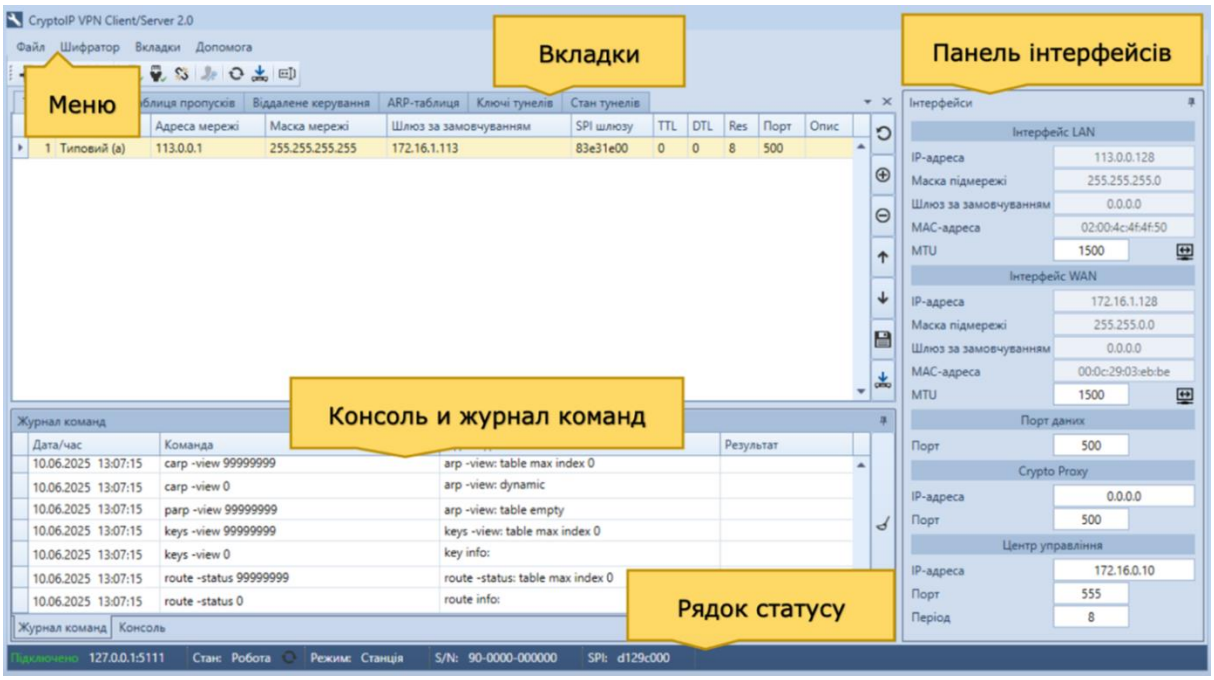


Рис. 3.5. Вікно інтерфейсу конфігуратора.

Головне вікно призначеного для користувача інтерфейсу конфігуратора містить наступні елементи управління: система меню, кнопки швидкого доступу , вкладки таблиць настроювання і відображення стану, панель настройки мережевих інтерфейсів, вкладки консолі і журналу команд, рядок статусу.

Важливим кроком в налагодженні шифратора є авторизація. Шифратор приймає налаштування від конфігуратора тільки після проходження авторизації: запросити у користувача вибір носія ключових даних і пароль до нього, після чого виконати читання необхідної інформації з носія і з файлу налаштувань

IP-шифратора. Після успішної авторизації, конфігурація шифратора зчитується і відображається програмою.

Якщо конфігуратором в IP-шифратор раніше вже був переданий комплект налаштувань, то успішна процедура авторизації відразу переведе IP-шифратор в стан "Робота".

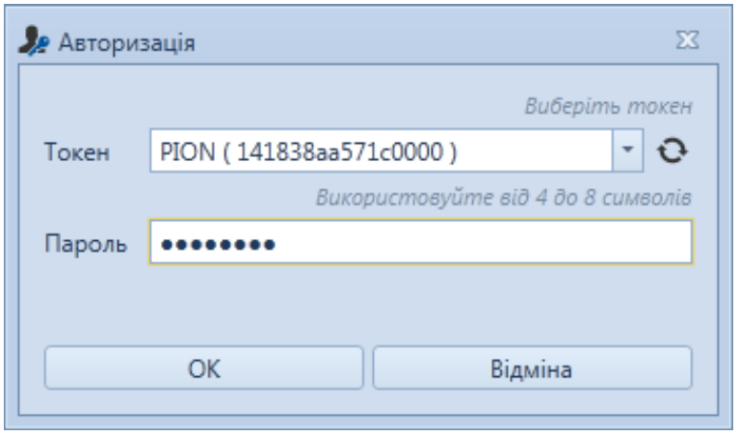


Рис. 3.6. Вкладка «Авторизація» в налагодженні шифратора

Вкладка паролі надає можливість управління паролями. Дозволяє користувачеві змінити поточний пароль носія ключових даних, а також задати пароль для віддаленого підключення.

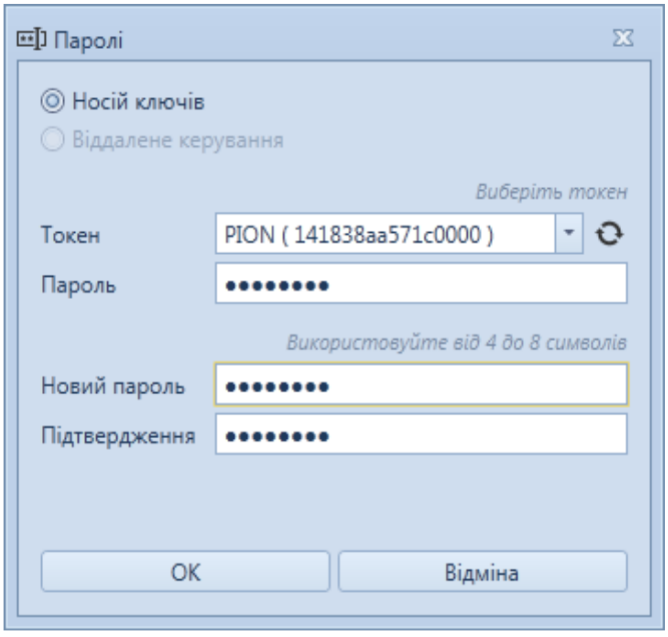


Рис. 3.7 Вкладка «Паролі» в налагодженні шифратора

IP-шифратор оперує двома мережевими інтерфейсами персонального комп'ютера: один з інтерфейсів належить WAN і пов'язує комп'ютер з мережею

загального користування. У цій мережі конфіденційна інформація повинна з'являтися в захищеному вигляді. Для будь-якого режиму роботи шифратора цей інтерфейс буде представлений фізичною мережевою картою. Другий інтерфейс – той, на якому конфіденційна інформація присутня у відкритому вигляді і доступна для обробки користувачами або програмами. Цей інтерфейс у разі режиму шлюзу також повинен бути представлений окремою мережевою картою, включеною в LAN. В цьому режимі IP-шифратор розташовується між двома сегментами мережі, передаючи інформацію з одного в інший, одночасно зашифровуючи або розшифровуючи її.

У режимі станції відбувається подібне, але сегмент мережі, в якому інформація присутня у відкритому вигляді, знаходиться всередині цього ж комп'ютера і представлений одною адресою. Для реалізації, всередині комп'ютера встановлюється логічний мережевий адаптер, який і представлятиме інтерфейс LAN. Цей інтерфейс буде мати свої мережеві параметри, а IP-шифратор, буде передавати інформацію між двома мережевими інтерфейсами, зашифровуючи і розшифровуючи її.

Для того, щоб IP-шифратор функціонував, йому необхідно вказати, який мережевий інтерфейс буде використовуватися в якості WAN, а який – як LAN.

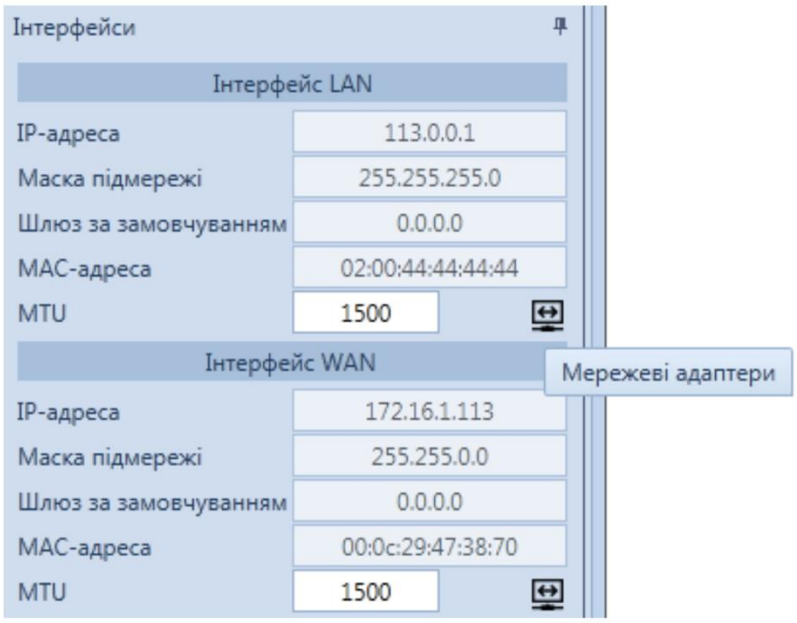


Рис. 3.7. Мережеві інтерфейси

Таблиця тунелів описує всі можливі з'єднання даного IP-шифратора з іншими шифраторами захищеної мережі.

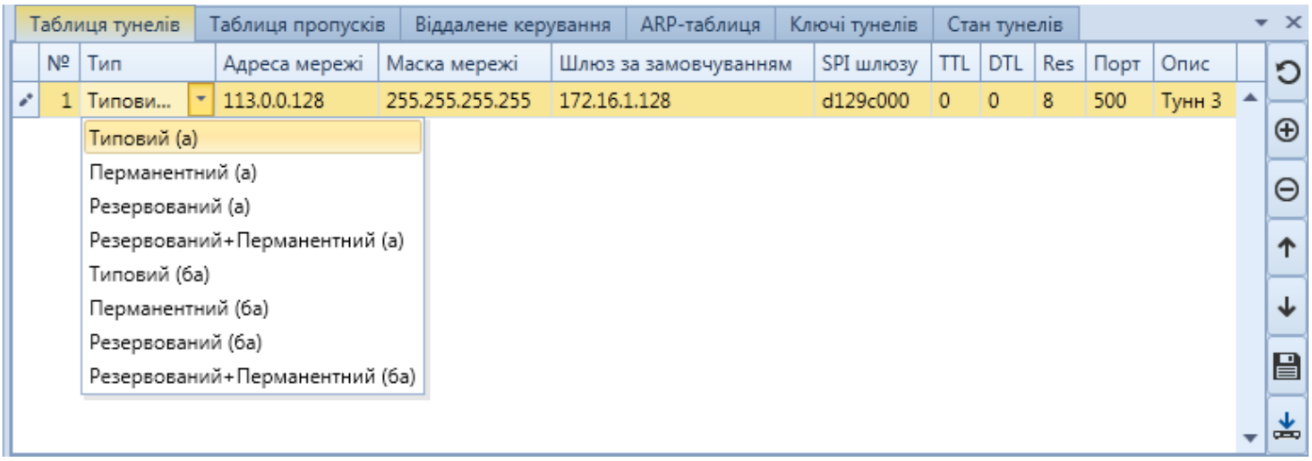


Рис. 3.8. Таблиця тунелів

- Тип тунелю
- Адреса LAN-сегмента одержувача (Адреса мережі)
- Маску LAN-сегмента одержувача (Маска мережі)
- Адреса WAN одержувача (Шлюз за замовчуванням)
- SPI IP-шифратора одержувача (SPI шлюзу)
- TTL
- DTL
- Res
- Порт даних IP-шифратора одержувача (Порт)
- Опис

Стан тунелів

Вкладка "Стан тунелів" не містить налаштувань і призначена тільки для відображення поточного стану тунелів.

Стан тунелів представлений у вигляді таблиці, кожен запис відповідає одному тунелю. Кількість рядків в таблиці відповідає числу тунелів в таблиці тунелів.

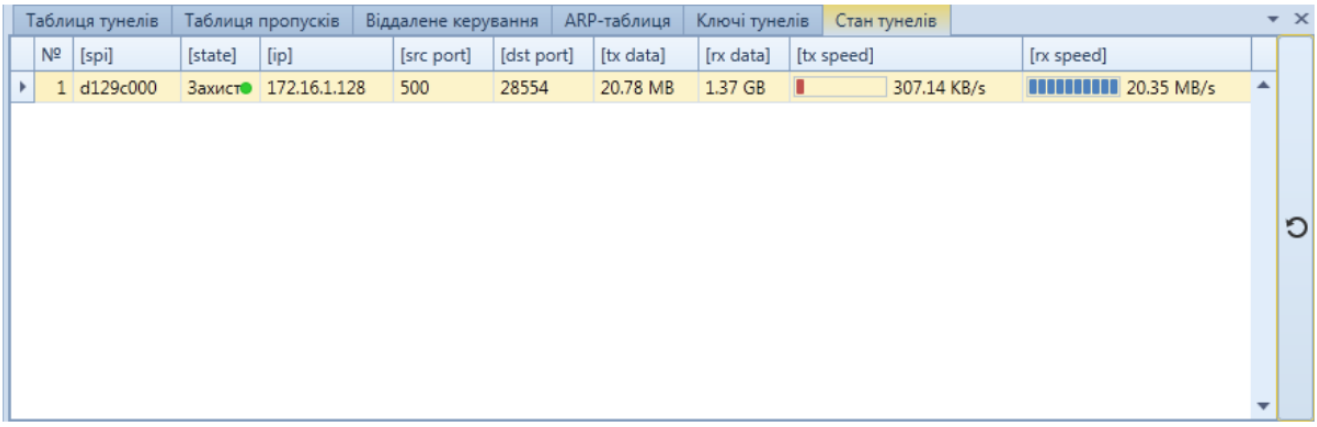


Рис. 3.9. Стан тунелів

Для оновлення інформації в таблиці необхідно натиснути на кнопку праворуч від таблиці.

Журнал команд

На вкладці "Журнал команд" можна бачити історію виконання команд шифратором, незалежно від того, були вони віддані конфігуратором або користувачем в ручному режимі через консоль.

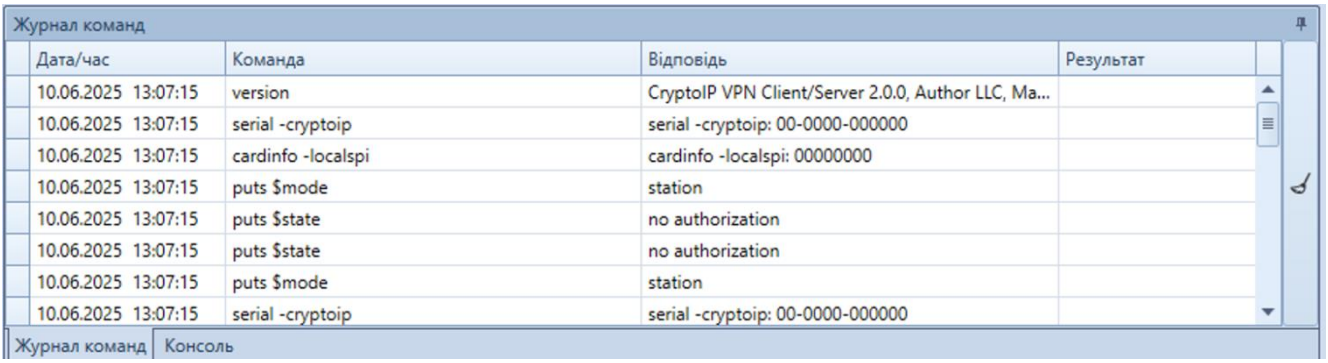


Рис. 3.10 . Журнал команд

IP-шифратор в режимі станції та в режимі шлюзу

Налаштування IP-шифратора в режимі станції та в режимі шлюзу мають низку відмінностей, пов’язаних як з призначенням пристрою, так і з особливостями організації доступу, конфігурації та експлуатації.

Режим станції передбачає використання шифратора безпосередньо на комп’ютері користувача, який водночас виконує роль адміністратора. Налаштування відбувається локально, і користувач має повний контроль над

процесом. Перед початком роботи адміністратор повинен мати установчий пакет *CryptoIP VPN Client*, носій ключових даних, пароль до нього та інформацію про конфігурацію захищеної мережі. Після входу в систему з правами адміністратора виконується встановлення програмного забезпечення з усіма необхідними компонентами. Після інсталяції монітор повідомляє, що шифратор не авторизований, що свідчить про працездатність системних компонентів.

Далі користувач підключає носій ключових даних через USB та виконує авторизацію через конфігуратор. Після успішної авторизації шифратор переходить у стан «Немає конфігурації». Наступним кроком є створення логічного мережевого інтерфейсу, якому призначається статична IP-адреса в рамках захищеної мережі. MAC-адреса при цьому може залишатися незмінною. Потім фізичному мережевому інтерфейсу комп'ютера призначається роль WAN-інтерфейсу, а створеному логічному адаптеру — роль LAN-інтерфейсу.

Після передавання конфігурації шифратор переходить у стан «Робота». З цього моменту всі мережеві пакети, що проходять через визначені інтерфейси, обробляються згідно з таблицями тунелів і пропусків. При перезавантаженні комп'ютера шифратор повертається в стан «Не авторизований» і не втручається в обробку трафіку, однак мережевий сегмент LAN при цьому не працює. Також обов'язковою вимогою є зміна пароля за замовчуванням до носія ключових даних.

На відміну від цього, режим шлюзу використовується в інфраструктурі з виділеним комп'ютером, який, як правило, фізично або логічно ізольований від загального користування. Цей комп'ютер часто керується дистанційно, а адміністратор, який налаштовує шифратор, не обов'язково має доступ до інформації, що ним захищається. Для налаштування використовується установчий пакет *CryptoIP VPN Server*, носій ключових даних, пароль до нього, а також відомості про структуру мережі та конфігурацію клієнтів.

Особливістю є можливість встановлення носія ключових даних безпосередньо всередину корпусу комп'ютера через внутрішній USB-роз'єм. Решта операцій може виконуватись дистанційно. Після встановлення програмного

забезпечення та авторизації шифратор також переходить у стан «Немає конфігурації».

Оскільки в режимі шлюзу комп’ютер зазвичай розміщений у віддаленій локації, перед призначенням мережевих інтерфейсів рекомендується попередньо налаштувати таблицю пропусків. Це дозволяє уникнути втрати зв’язку з пристроєм після переходу в робочий режим. Потім наявні фізичні мережеві інтерфейси комп’ютера призначаються як WAN- та LAN-інтерфейси шифратора. Після передачі конфігурації шифратор переходить у стан «Робота», де обробляє пакети згідно з таблицями тунелів і пропусків.

Після перезавантаження комп’ютера шифратор знову буде перебувати в стані «Не авторизований», і мережеві інтерфейси WAN і LAN не будуть взаємодіяти між собою. Як і в режимі станції, обов’язковим кроком є зміна пароля до носія ключових даних.

У підсумку, режим станції зручний для кінцевого користувача, тоді як режим шлюзу оптимізований для централізованого захисту мережевого трафіку з обмеженим фізичним доступом до пристрою. Відмінності полягають у способі доступу, структурі мережі, типах інтерфейсів і порядку конфігурації.

3.2 Перевірка безпеки мережевого каналу

Для оцінки безпеки мережевого каналу після налаштування захищеної мережі на основі апаратного засобу CryptoIP-448 було проведено тестування з використанням аналізатора трафіку Wireshark.

Було здійснено перехоплення мережевого трафіку між двома кінцевими точками захищеного каналу. Після активації захищеного з’єднання через CryptoIP-448, аналіз мережевих пакетів показує, що передані дані шифруються.

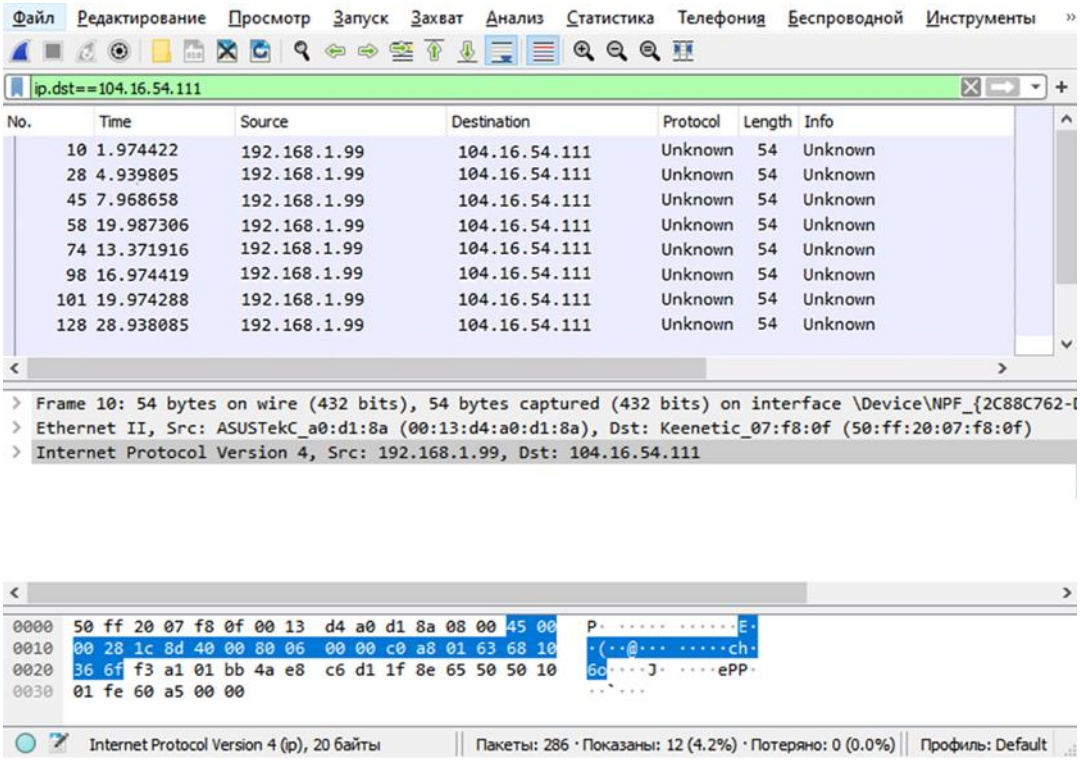


Рис. 3.11. Перехоплення мережевого трафіку з Wireshark.

На риснку 3.11. наведено приклад перехоплення трафіку між хостом 192.168.1.99 та віддаленим сервером 104.16.54.111. Видно, що всі пакети мають невизначений протокол (Unknown), що підтверджує факт відсутності розпізнаваної інформації.

Крім того, поле Info не містить інформативних даних, а вміст пакету представлений у вигляді байтів, що не мають читабельного представлення. Це вказує на те, що навіть у разі перехоплення трафіку стороння особа не може отримати доступ до переданої інформації, оскільки шифрування приховує як вміст, так і структуру протоколів вищого рівня.

За результатами проведеного тестування було підтверджено, що після активації захищеного каналу дані передаються у зашифрованому вигляді, що унеможливлює їх перехоплення та несанкціоноване ознайомлення з передаваною інформацією сторонніми особами. Механізми шифрування, які реалізує CryptoIP-448, ефективно приховують як самі дані, так і службову інформацію вищих рівнів.

Навіть маючи файл із перехопленими ESP-пакетами, без знання секретних ключів вміст не піддається відновленню. Wireshark може розшифрувати ESP тільки за умови, що в нього завантажено правильні сеансові ключі [30].

Якщо ключі невідомі – він показує зашифровані, а не реальні дані. Аналогічно, будь-який спробований «брутфорс» чи дешифрація невірна через високу криптостійкість (алгоритм ГОСТ 28147-89) та налаштування CryptoIP-448 [25]

Отже, без ключа вміст пакетів не прочитується.

3.3 Рекомендації щодо впровадження та застосування захищеної мережі на базі CryptoIP-448

На сьогоднішній день використання конфіденційної інформації супроводжується передачею інформації через незахищений канал (як правило - Інтернет). Але і в такому випадку можна знайти вихід. Для того щоб забезпечити безпечний канал передачі даних, рекомендується оптимальне рішення з застосуванням захищеної мережі на базі CryptoIP-448.

Вітчизняний апаратний IP-шифратор, призначений для криптографічного захисту інформації в сучасних телекомунікаційних системах. «CryptoIP-448» підтримує архітектуру відкритих ключів (PKI) і розроблений у відповідності із законодавчою базою України.

IP-шифратор "CryptoIP-448"- пристрій криптографічного захисту інформації, призначений для захисту IP-трафіку локальних мереж, терміналів і автоматизованих робочих місць.

"CryptoIP-448" забезпечує: підтримку повно зв’язної структури віртуальної приватної мережі (VPN); шифрування і інкапсуляцію пакетів IP трафіку; прозору передачу шифрованих пакетів по тунелях VPN; аутентифікацію та ідентифікацію абонентів;

У пристрої реалізуються криптографічні алгоритми:шифрування пакетів IP-трафіку - ГОСТ 28147-89; хешування - ГОСТ 34.311-95; електронний цифровий

підпис - ДСТУ 4145-2002;формування сеансового ключа на еліптичних кривих;взаємодії з інфраструктурою відкритих ключів - X.509.

"CryptoIP-448" підтримує інтерфейси:10/100Base-T - для підключення до локальної мережі;10/100Base-T - для підключення до комунікаційного обладнання; USB 1.1 - для підключення до ПЕОМ (конфігурація).

Переваги "CryptoIP-448": гарантований захист від компрометації ключів (використання смарт-карт, сертифікованих за Common Criteria 5+), генерація, розподіл і використання ключів відповідає законодавчій базі України, можливість дистанційного керування IP-шифратором і його ключовою системою, на ринку це найкраще співвідношення "ціна-якість".

Встановлення та експлуатація IP-шифратора здійснюється відповідно до вимог експлуатаційних документів з урахуванням „Інструкції по забезпеченню безпеки експлуатації, генерації ключових даних та поводження з ключовими документами ”. Поточний ремонт IP-шифратора не передбачений. Ремонт несправних складових частин IP-шифратора здійснюється підприємством – виробником.

Для забезпечення цілісності конфігурації та ключових матеріалів CryptoIP-448 рекомендується: регулярно виконувати резервне копіювання конфігураційних файлів пристрою, зберігаючи копії у захищеному сховищі з обмеженим доступом; зберігати резервні копії ключів і сертифікатів окремо від основного обладнання, щоб уникнути їх втрати у разі виходу пристрою з ладу; використовувати засоби резервного копіювання, які підтримують шифрування для захисту резервних даних.

Ефективний моніторинг стану захищеної мережі на базі CryptoIP-448 забезпечує: виявлення спроб несанкціонованого доступу або аномальної активності; контроль працездатності IP-шифраторів та їх взаємодії; реагування на інциденти інформаційної безпеки у режимі реального часу.

Рекомендується використовувати системи моніторингу мережевого трафіку, а також системи управління подіями безпеки (SIEM), які інтегруються з апаратними засобами захисту.

Для забезпечення актуальності криптографічних алгоритмів і виправлення можливих уразливостей: регулярно оновлюйте прошивку CryptoIP-448, використовуючи офіційні оновлення від виробника; перед оновленням створюйте резервні копії конфігурації та ключових матеріалів; проводьте тестування працездатності пристрою після оновлення в тестовому середовищі.

Впровадження захищеної мережі на базі CryptoIP-448 дозволяє побудувати надійний захист інформації при передачі в мережах з відкритим доступом. Дотримання рекомендацій щодо резервного копіювання, моніторингу і своєчасного оновлення забезпечить стабільну і безпечну роботу мережі, захист від компрометації ключів і відповідність нормам безпеки, визначеним українським законодавством

ВИСНОВКИ

У ході виконання роботи було досліджено та реалізовано підхід до побудови захищеної корпоративної мережі з використанням шифратора CryptoIP-448.

Актуальність теми обумовлена постійним зростанням кіберзагроз і необхідністю забезпечення надійного захисту інформації в корпоративних інформаційно-телекомунікаційних системах.

У результаті дослідження:проведено аналіз сучасних загроз інформаційній безпеці та методів їхнього усунення. Розглянуто принципи роботи та функціональні можливості шифратора CryptoIP-448. Розроблено структуру захищеної корпоративної мережі, у якій пристрій CryptoIP-448 забезпечує шифрування трафіку, автентифікацію вузлів і контроль цілісності переданих даних.

Запропоновано рекомендації щодо впровадження системи захисту, а також заходи щодо підтримки її безперервної та безпечної роботи.

Впровадження такого рішення дозволяє значно підвищити рівень захищеності корпоративної мережі, забезпечити конфіденційність переданої інформації, мінімізувати ризики витоку або несанкціонованого доступу до даних, а також відповідає вимогам нормативних документів у сфері криптографічного захисту інформації.

Таким чином, поставлені в роботі цілі були досягнуті, а завдання - виконані. Отримані результати можуть бути використані як основа для впровадження захищених мереж у державних установах, підприємствах оборонно-промислового комплексу та інших організаціях з підвищеними вимогами до інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. Підручник / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – Київ: КУБГ, 2019. – 218 с.

2. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. / В.М.Вишняков. – Київ: КНУБА, 2022. – 120 с.

3. Городецька, О. С.Комп’ютерні мережі : навчальний посібник / О. С. Городецька, В. А. Гикавий, О. В. Онищук. − Вінниця : ВНТУ, 2017. – 129 с.

4. Дудикевич, В. Б.Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.

5. Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

6. Захарченко С. М. Основи побудови захищених мереж на базі обладнання компанії Cisco : навчальний посібник / С. М. Захарченко, Т. І. Трояновська, О. В. Бойко. – Вінниця : ВНТУ, 2017. – 136 с.

7. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.

8. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — Київ: Видавнича група BHV, 2009. -608 с.: іл.

9. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— Київ: ДУТ, 2015.— 288 с.

10. Захист інформації в комп’ютерних системах та мережах : навч. посіб. /С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.

11. Якименко Ю.М., Поляков Д.А. Методичні підходи до захисту інформаційних ресурсів від сучасних загроз: збірник тез Всеукраїнської науково-

практичної конференції «Актуальні проблеми безпеки інформаційно-телекомунікаційних систем» м. Київ, 3 - 5 листопада 2024 року, Київ: РВЦ ДУІКТ. – 2024. – 126 с.

12. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*. № 3 (9). 2013.с. 105-120

13. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. *Математичне та комп'ютерне моделювання. Серія:Технічні науки,* 2019, с. 56-62.

14. Чинчик Д. М., Коробейнікова Т.І. Методи та засоби комплексного захисту корпоративної мережі.*Стратегічні напрямки розвитку науки: фактори впливу та взаємодії*. 07.04.2023 рік. Рівне, Україна МЦНД, с.97-102

15. Настанова з експлуатації АЧСА.465653.002 НЕ. IP-шифратор«CryptoIP-448», «CryptoIP-448/5v» ,«CryptoIP-428», «CryptoIP-428/5v». 2013

16. Апаратно-програмний комплекс DigiScan EX URL: https://tzi.com.ua/digiscan_ex.html (дата звернення 23.04.2025)

17. АТ ІІТ Засоби та комплекси: URL: https://iit.com.ua/index.php?page=itemdetails&p=3&gtype=1&type=1&id=95 (дата звернення 23.04.2025)

18. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96.– [Чинний від 1997.01.01]. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf (дата звернення 20.04.2025)

19. Cybersecurity Forecast 2025 report. URL: https://cloud.google.com/security/resources/cybersecurity-forecast (дата звернення 23.04.2025)

20. Карачка А.Ф. Технології захисту інформації Текст лекцій Тернопіль, ТНЕУ, 2017 URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf (дата звернення 25.04.2025)

21. Конспект лекцій з дисципліни «Захист інформації в комп’ютерних системах» Краматорськ, 2020 URL:

http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/%D0%97_%D0%9A%D0%A1%20%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86_%D0%B9.pdf (дата звернення 26.04.2025)

22. Коробейнікова Т. І., Журавель І. М., Бодак А. О., Бороденко Д. В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах//*Вісник ЛДУБЖД*, №30, 2024 URL:https://journal.ldubgd.edu.ua/index.php/Visnuk/article/download/2769/2655/ (дата звернення 27.04.2025)

23. Коробейнікова Т. І., Куцак Ю. В. Методи та засоби безпечної передачі даних в корпоративних мережах. Вінниця.Зб. мат.XLVIII наук.-техн. конф. ФІТКІ (2019). URL :https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki2019/paper/viewFile/6606/5491 (дата звернення 10.05.2025)

24. Тертичний В.О. Мережна безпека, системи виявлення та протидії атакам, відмовостійкість мереж. с. 100-101. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7234e22b-f216-42d3-ade4-f665f2f0cb80/content (дата звернення 11.05.2025)

25. Шифрування. Вебсайт : URL: https://uk.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F (дата звернення: 12.05.2025).

26. IP-шифратор CRYPTOIP-448 URL: https://tzi.com.ua/510.html

27. IP-шифратор CRYPTOIP-448 URL: https://ispn.kyivcity.gov.ua/PROD_ID/14239#:~:text=%D0%BF%D1%96%D0%B4%D1%82%D1%80%D0%B8%D0%BC%D1%83%D1%94%20%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81%D0%B8%3A%2010%2F100%20BASE,%D0%A2%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D1%96%20%D1%85%D0%B0%D1%80%D0%B0%D0%BA%D1%82%D0%B5%D1%80%D0%B8%D1(дата звернення 11.05.2025)

28. IP-шифратор CRYPTOIP-448 URL: https://tzi.ua/ua/ip-shifrator_cryptoip-448.html#:~:text=%C2%ABCryptoIP%20(дата звернення 11.05.2025)

29. WireGuard : веб-сайт. URL: https://www.wireguard.com (дата звернення 12.05.2025)

30. Wireshark. веб-сайт. URL : https://wiki.wireshark.org