МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Захищений канал передавання даних в корпоративній мережі»

Виконавець: _____ Ломако Д. С.
(підпис)

Керівник: _____ Бахтіяров Д. І.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Ломако Данила Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «Захищений канал передавання даних в корпоративній мережі»
затверджена наказом ректора від «06» квітня 2021 р. №559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: визначення предметної області, розгляд програмний та апаратних рішень для побудови захищених каналів корпоративних мереж, математичне моделювання продуктивності і масштабованості захищених каналів
4. Зміст пояснювальної записки: підсистема захисту каналів зв’язку в корпоративній мережі підприємства
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft Power Point

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-20.05.2021	Виконано
2	Вступ	21.05.2021-22.05.2021	Виконано
3	Предметна область і постановка задачі	23.05.2021-27.05.2021	Виконано
4	Розробка підсистеми захисту каналів зв’язку в корпоративній мережі підприємства	28.05.2021-03.06.2021	Виконано
5	Моделювання, продуктивності і масштабованості захищених каналів	04.06.2021-09.06.2021	Виконано
6	Усунення недоліків дипломної роботи	10.06.2021-14.06.2021	Виконано

7. Дата видачі завдання: “26" квітня 2021 р.

Керівник дипломної роботи _____ Бахтіяров Д. І.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Ломако Д. С.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Захищений канал передавання даних в корпоративній мережі» містить 63 сторінки, 17 рисунків, 3 таблиці, 18 використаних джерел.

КОРПОРАТИВНА МЕРЕЖА, ЗАХИЩЕНИЙ КАНАЛ, ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, КРИПТОГРАФІЧНИЙ АЛГОРИТМ, РЕЖИМ ШИФРУВАННЯ, VIPNET.

Об’єкт дослідження –. процес створення захищеного каналу підприємства.

Предмет дослідження – канал захищеного інформаційного обміну в корпоративній мережі підприємства.

Мета дипломної роботи – створити безпечне, захищене середовище для передачі конфіденційної інформації з каналами громадського та виділеного (Інтернет, фізичні, супутникові та бездротові канали зв'язку) шляхом організації віртуальних приватних мереж (VPN).

Метод дослідження – Методи математичного моделювання, статистичного аналізу, криптографії, теорії електрозв’язку.

Рішення, що описується в дипломній роботі є оптимальним щодо фінансових витрат і дозволяє забезпечити найбільш гнучкий спосіб зв’язку з віддалених користувачів з ресурсами корпоративних мереж.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

DDoS (distributed denial of servise) – розподілена відмова в обслуговуванні.

DoS (denial of servise) – відмова в обслуговуванні.

IDS (intrusion detection system) – система виявлення вторгнень.

IETF (The Internet Engineering Task Force) – робоча група з проблемних питань Інтернет.

FTP (file transfer protocol) – протокол передачі файлів.

URL (uniform resource locator) – уніфікований покажчик ресурсу.

VPN (virtual private network) – віртуальна приватна мережа.

ІБ – інформаційна безпека.

КС – комп'ютерна система.

КМ – корпоративна мережа.

ОПР – особа, яка приймає рішення.

МЕ – міжмережний екран.

ПЗ – програмне забезпечення.

СЗІ – система захисту інформації.

ЦП – цифровий підпис.

ВСТУП

Актуальність теми. У XXI-му віці, коли інформаційні технології повністю поглинаються нашим світом, коли ми не можемо уявити собі життя без комп'ютера та смартфона, коли ходити по магазину для купівлі хліба з обчислювальним обладнанням не виглядає зовсім дивним, кожен в той чи інший час починає цікавитись як передаються ці дані. Перш за все, це питання було вирішено, зберігаючи прямий кабельний зв'язок, який фізично захищений від інформаційного бар'єру, з великими матеріалами, лише великі корпорації та основні агентства можуть покривати витрати на такий зв’язок. Швидкий розвиток Інтернету створив нову тенденцію - дешеві відносини Global Company використовуються для досягнення більш доступного інтернет-транспорту. Ефективне впровадження Інтернету в корпоративну мережу сприяли наявності нової концепції - Інтранет, в якій спосіб розподілу та обробки інформації був переданий у корпоративну мережу. Однак існує чітка загроза мережевій безпеці Інтранет-підприємства, оскільки внутрішні ресурси компанії доступні для багатьох користувачів Інтернету та таємний трафік можна перехопити зловмисникам. Щоб забезпечити безпечне підключення до мережі з відділеннями сегментами компанії, організовуються віртуальні приватні мережі (VPN), використовуючи набір секретів, дані технології безпеки та цілісності, що транслюються в публічній мережі. У цьому контексті слово "конфіденційність" означає передачу даних у зашифрованій формі між віддаленими користувачами мережі корпоративного сектору, яка допомагає нам говорити про забезпечення каналу зв'язку - "тунелю". Доступ до Інтернету використовується як зашифроване середовище передавання даних [1].

Мета і завдання дослідження. Створити безпечне, захищене середовище для передачі конфіденційної інформації з каналами громадського та виділеного (Інтернет, фізичні, супутникові та бездротові канали зв'язку) шляхом організації віртуальних приватних мереж (VPN).

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Розглянути програмні, апаратні та програмно-апаратні засоби побудови VPN мереж.

2. Розглянути методи симетричної та асиметричної криптографії та режими шифрування.

3. Розглянути рішення для побудови захищених каналів в корпоративних мережах.

4. Побудувати захищений канал корпоративної мережі на базі запропонованого рішення.

5. Провести моделювання та оцінку продуктивності роботи захищених каналів.

6. Розробити моделі функціонування захищеної корпоративної мережі.

7. Провести багатомірний регресійний аналіз.

Об'єктом дослідження – процес створення захищеного каналу підприємства.

Предметом дослідження – канал захищеного інформаційного обміну в корпоративній мережі підприємства.

Методи досліджень. Методи математичного моделювання, статистичного аналізу, криптографії, теорії електрозв'язку.

Практичне значення отриманих результатів.

Розгорнуто організацію відкритих ключів (PKI) та організацію сертифікації, щоб інтегрувати електронну цифрову систему підпису в програмному забезпеченні клієнта (система управління документами та робочим офісом, електронною поштою, банківським програмним забезпеченням, електронною діловою платформою). Інші вітчизняні виробники повинні мати можливість взаємодіяти з інтерактивним програмним забезпеченням PKI

Рішення, що описується в дипломній роботі є оптимальним щодо фінансових витрат і дозволяє забезпечити найбільш гнучкий спосіб зв'язку з віддалених користувачів з ресурсами корпоративних мереж.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
ПРЕДМЕТНА ОБЛАСТЬ І ПОСТАНОВКА ЗАДАЧІ

1.1. Апаратні засоби організації захищених каналів VPN

Адміністрування віддаленого доступу та системи VPN є досить складним завданням - для підготовки та розгортання рішення, яке задовольняє потреби різних користувачів мережі підприємства разом. В даний час на ринку готуються багато рішень та технологій, щоб організувати віртуальну приватну мережу.

Щоб розробити VPN мережу, всі продукти можна розділити на два типи - програмне забезпечення та апаратне забезпечення. Програмне рішення для VPN, як правило, є готовою установкою ПЗ на комп'ютері, підключеному до мережі з стандартною операційною системою для потреб безпеки та продуктивності, встановлення додатків VPN. Деякі виробники програмних технологій та NETGARD, VPN-пакети ПЗ яких легко інтегровані з програмним брандмауером та працюють на різних операційних системах, включаючи Windows 10, Sun Solaris та Linux [1].

Для розгортання програмних рішень часто використовують більш складне обладнання. Щоб прискорити операцію шифрування створюють систему, пов'язану з налаштуванням сервера, щоб ідентифікувати цей комп'ютер та його операційну систему, пакет VPN, мережеву карту для кожного з'єднання має місце використання спеціальних таблиць. Така робота також важка для досвідчених професіоналів. З іншого боку, вартість програмного рішення відносно низька: на основі розміру мережі, ви можете придбати пакет VPN на 2-25 тисяч доларів (без обладнання, установки та обслуговування).

Все, що потрібно для підключення до апаратних рішень VPN включає: комп'ютер, операційну систему (ОС) та спеціальне програмне забезпечення. Деякі компанії, включаючи Cisco, NetScreen та Sonic, пропонують широкий спектр розширених рішень на основі кількості з'єднань VPN. Апаратні рішення дуже прості, потрібно лише кілька годин для розгортання. Інша велика перевага апаратного

рішення VPN – висока продуктивність. Дані рішення використовують спеціальні операційні системи для роботи та не мають необхідності підтримувати інші функції ОС. Використання апаратних рішень потребує високих витрат. Діапазон цін - від 10 тисяч доларів. Організація роботи віддаленого офісу для потреб бізнес сегменту – сотні тисяч доларів за VPN рішення для бізнесу.

Вибір рішення залежить від розміру мережі та кількості трафіку. Не варто забувати, що значні обчислювальні ресурси необхідні для шифрування трафіку, що можуть перевантажувати комп'ютер в процесі підключення VPN для одночасної передачі даних.

Втілення VPN на спеціальних пристроях може бути використане в цих мережах, для яких потрібна висока продуктивність. Приклад реалізації такого рішення є:

Точки доступу Xedia 1000. Точка доступу 1000-ї серії - це високоефективний маршрутизатор для доступу до Інтернету, що підтримує безліч IP-служб, включаючи Інтернет-трафік, який буде захищений тунелями IPSEC. Цей маршрутизатор може зберігатися як частина служби оператора, наприклад, частина інфраструктури постачальника послуг Інтернету або великої мережі компанії. Потужне обладнання безпеки, масштабованість та наявність відмінної продуктивності точки доступу ідеально підходять для роботи як інтегрованого VPN маршрутизатора, так і системи, що працює як VPN рішення у великих інформаційних центрах. Відповідно до веб-сайту виробника, його вартість становить 19,995 $, а також 1000 $ для пакету програмного забезпечення QVPN [2].

Пакет VPN Lucent. Пакет Lucent VPN був адаптований спеціально для максимальної безпеки. Безпека часто досягається за рахунок низької продуктивності пристрою. Ця особливість відображена в стандартах продуктивності цього продукту. На відміну від інших VPN рішень, тестування, де апаратне та програмне забезпечення знаходиться в одному продукті – апаратних засобах (інструменти для реалізації VPN) та програмного забезпечення (серверний пакет VPN, керування портами VPN) мають різні компоненти. За даними веб-сайту виробника, його ціна становить 21990 $. Пакет включає в себе два апаратних модуля VPN Lucent, програмне забезпечення для

керування програмним забезпеченням безпеки та клієнтського програмного забезпечення, а також ліцензії на 100 VPN сеансів [2].

VIP NET-1100. Продукти VIP NET-1100 є високопродуктивним VPN рішенням для захищених комерційних мережевих додатків, що може бути використане великими підприємствами, щоб створити власний VPN сервер. Мережеві постачальники послуг, які керуються постачальниками послуг VPN та ASP для корпоративних клієнтів. Продукт VIP NET-1100 підтримує повний сервіс VPN, наприклад, шифрування IPSEC, довірча асоціація асоціації міжнародної обчислювальної системи (ICSA-International-International); пакет стиснення та аутентифікації; основний ключ безпеки керування з протоколом IP; Трансляція адрес мережі (NAT) та цифровий сертифікат. Вартість становить 4995 $ за одиницю, а модуль Multi-Content VpnManager - 1995 $. Гостьовий модуль продається за 99 $ [2].

Redguard cipro-vpn Redgro-VPN продукт - це апаратний VPN з сильним механізмом безпеки, який може бути використаний у внутрішній мережі, Extranet, VPN-колективній мережі та може бути використаний для людей на віртуальних приватних каналах, які використовують мобільний телефон. Продукти CIPRO-VPN сумісні з модулями сертифікації обладнання та сумісні з стандартами IPSEC та X.50. Встановлення та експлуатація легка, немає необхідності знань про основи інформаційної безпеки, а також унікальні роботи з мережею. Середня ціна становить 14950 $ за одиницю, що включає в себе два пристрої доступу до VPN, а також функції брандмауера [2].

Слід зазначити, що використання списку апаратного забезпечення VPN рішень з вартістю більше 10000 $ для багатьох компаній є неприйнятними. Висока вартість цих пристроїв не є їх єдиним недоліком.

1.2. Програмні реалізації VPN

Способи побудови захищених каналів на основі розгортання програмного забезпечення VPN включають [1-2]:

- ✓ Безкоштовні рішення IPSEC (безпека Інтернет-протоколу). Таким чином, FreeSwan або FreeBSD може реалізувати IPSec.
- ✓ Комерційні рішення. Наприклад: Cisco VPN або Securepoint VPN-сервер, також заснований на IPSec.
- ✓ Програмне забезпечення, що застосовує всі механізми VPN.
- ✓ ПЗ з використанням PPTP (точка до точки тунельного протоколу).
- ✓ Пакет OpenVPN.

Розглянемо докладніше про переваги та недоліки кожного з вищезгаданих програмних засобів VPN.

Під час реалізації VPN за останні кілька років IPSEC вважається практичним стандартом. Цей загальний тип не потребує сервери VPN та сумісність клієнтів. Унікальні стандарти дуже зручні. Такий спосіб хороший, оскільки він не вимагає великих фізичних витрат, а також забезпечує безперервний захист даних. Але його переваги для цього закінчуються. Основним недоліком IPSEC є неправильна робота з брандмауером, особливо якщо використовується технологія NAT. Монітор контролює стан брандмауера, розташованого між двома віртуальними тунелями, і не може пропустити пакети IPSEC або інші пакети IPSEC, керованими постачальником. Платформи різного розгортання IPSEC повинні внести повну зміну в ядро операційної системи та IP-стек, щоб розгорнути функції IPSEC [1].

Другий підходить для тих, хто готовий інвестувати великі гроші (менші, ніж на розгортання апаратного забезпечення). Перевага цього рішення полягає в тому, що буде надано високу якість технічної допомоги виробником. Крім того, безкоштовна допомога незалежних фахівців, або відповідно до ваших інструкцій, визначить, як підключити мережу для досягнення найкращих результатів.

Третій варіант найбільш підходить для тих, хто потребує розгортання VPN без затрат великого часу, сил та інвестицій. Також, ви повинні знати, що такі програми написані для людей, які не хочуть займатися робочими принципами та методами встановлення IPSEC. З часом такі програми поступово покращуються тому, що кожен автор використовує свій власний криптоалгоритм. Звичайно, вони забезпечують

певний рівень безпеки, але представлення такого рішення захищатиме дані від нових зловмисників, але не від експертів у галузі промислової шпигунської діяльності.

Четвертий спосіб використовується послідовниками Microsoft. Цей стандарт реалізує автентифікацію послідовного шифрування. Побудована на глибині великої групи Redmond, вони не знайшли спеціального розповсюдження в World Unix.

Більшість адміністраторів, які не використовують конкретні запропоновані варіанти, зупинилися на OpenVPN (проектна сторінка http://openvpn.net).

Офіційно OpenVPN успішно працює на ОС: Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X, Windows 10 / Server. Це дозволяє створювати складні багатоформатні тунелі без необхідності експортувати OpenVPN в будь-якій іншій системі, включаючи драйвери пристроїв Tune / Tap.

Підтримуються два типи тунелів: IP та Ethernet, відповідно їх називають корінь і міст. Тому можна підключити обидва IP-підставки та віртуальні адаптери Ethernet.

Це дозволяє працювати з будь-яким механізмом шифрування, побудованим у OpenSSL, щоб захистити потік. І в обміні, кожен клієнт має основний тип ключа, режим роботи (CBC, CFB, OFB).

Якщо є повторна послідовність у даних передачі, IV алгоритм буде використовуватися для приховування їх.

Кожна дейтаграма позначена за допомогою спеціального ідентифікатора, створеного на основі номерів часу відправлення та замовлень.

Як додатковий захід безпеки, використання протоколів TLS може бути заданим для сертифікації сеансу обміну динамічним сертифікатом. Під час обміну динамічним ключем SSL / TLS дозволяє досягти використання декількох бібліотек. Тому навіть з розміром понад 2048 байт, обмін між серверами та клієнтами не впливає на швидкість передачі тунельних даних.

OpenVPN створено за допомогою сценаріїв та інших додатків високого рівня, які можуть легко створювати та знищувати тунелі. Це дозволяє легко працювати через брандмауер з статусом підключення.

Створити віртуальну приватну мережу між системами Windows та Unix, сьогодні є оптимальним рішенням для використання OpenVPN найбільш

економічним та надійним варіантом. Тому, щоб розгорнути безпечний канал, я буду використовувати OpenVPN.

1.3. Платформи реалізації захищеного каналу в корпоративних мережах

Через високу сумісність проекту OpenVPN він може працювати на Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X та операційній системі Windows 10 / Server.

Для створення мережі компанії, моделювання та оцінка продуктивності захищеного каналу, операційну систему сервера була вибрана як:

- ✓ Fedora Core.
- ✓ Windows 10 Serve.

Для клієнтів була обрана система:

- ✓ Windows 10 Pro.

Ці операційні системи були обрані для організації корпоративної мережі через стабільність, функціональність та легку конфігурацію. Крім того, система FreeBSD вважається серверною операційною системою, але через відсутність офіційної підтримки програмного забезпечення, що використовується в бізнес процесах підприємства, ця операційна система виключена з подальшого розгляду.

1.4. Структура і склад інформаційної системи підприємства

Всі підпроекти об'єднуються в загальну інформаційну мережу підприємства, щоб організувати управління та контроль всіх технологічних процесів. Інформаційна мережа побудована за технологією Ethernet.

Для використання алгоритмів керування застосовується додаткове обладнання, то контролер, що дозволяє легко збільшити можливість встановлення додаткових модулів. Рівень DP CS забезпечується диспетчером FUPPI Engine Engineering (Control Low-рівня, ACS). Існує механізм розподілу прав керування між АС.

Спеціальний сервер SCADA забезпечує бази даних та обслуговування в режимі реального часу.

SCADA SERVER називається основним інформаційним сервером. Головний сервер відіграє роль сервера інтерфейсу SCADA. Організувати та впроваджувати процес спілкування з системами автоматизації (з програмуванням логічних контролерів), безпосередньо підключено до локальної комп'ютерної мережі (LAN). Серверний процес забезпечує короткострокові колекції випадкових подій дійсної обробки даних на об'єкті. Поточне значення, процес позиції та їх параметри записуються у об'єктно-орієнтованому зразку.

Основний інформаційний сервер повністю зарезервований. Основні сервери підключені до локальної комп'ютерної мережі та підключені до іншої дисперсійної робочої станції з протоколом TCP / IP.

Основна клавіатура сервера, екран та значки повинні встановлювати систему обслуговування та пошук інцидентів та їх подій у звичайній роботі системи SCADA.

LPMG здійснюється через сервери спілкування з рівнями DP, що представляє розподілене програмне забезпечення та апаратні пристрої, які контролюють основне обладнання технічного процесу підприємства.

Програмне забезпечення підсистеми ядра та технічні засоби керування ACS для експлуатації та забезпечення реалізації всіх функціональних та контрольних функцій на основному технічному обладнанні. Ядро включає в себе:

- ✓ Автоматичну система управління;
- ✓ Надзвичайний та пульт дистанційного керування;
- ✓ SCADA SERVER;
- ✓ Координатор AWS;
- ✓ ACS TP (Ethernet).

Структура АСС базується на використанні інтегрованих інформаційних мереж. Для створення такої мережі використовується оптичний кабель промислового зразку (волоконно-оптичні - FOC). Мережа базується на швидкої технології Ethernet (1000 Мбіт / с). Має місце використання оптичних конверсійних модулів для підключення до мережі різних пристроїв.

Структура корпоративної мережі підприємства показана на рисунку 1.1.

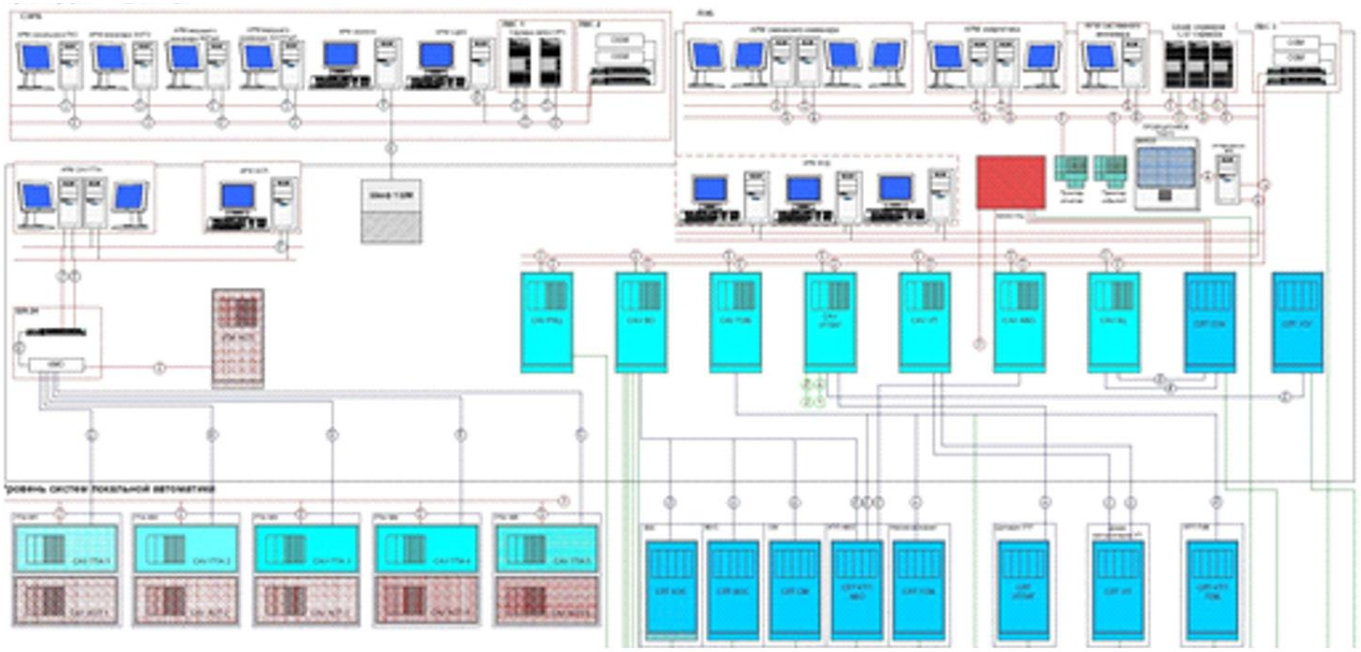

Рис. 1.1. Схема корпоративної мережі підприємства

ВИСНОВКИ ДО РОЗДІЛУ 1

Ця глава реалізувала детальний аналіз тематичної зони для розробки захищеного сегмента мережі.

Що стосується результатів системного аналізу, в якому визначається посилання безпеки, інформація була відтворена в сегменті мережі для її захисту. Запропоновано використання технології безпеки мережі на базі користувацької програми VIPNET в сегменті RVS.

Процес експлуатації був описаний з точки зору інформації, якою обмінюються користувачі корпоративної мережі. Показано структуру корпоративної мережі підприємства.

РОЗДІЛ 2
РОЗРОБКА ПІДСИСТЕМИ ЗАХИСТУ КАНАЛІВ ЗВ'ЯЗКУ В КОРПОРАТИВНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

2.1. Алгоритми шифрування в захищених каналах

Алгоритми шифрування діляться на два великі класи: симетричні (AES, Blowfish, DES) і асиметричні (RSA, El-Gamal). Симетричні алгоритми шифрування використовують один і той же ключ для зашифровування інформації і для її розшифрування, а асиметричні алгоритми використовують два ключі: один для зашифровування, інший для розшифрування.

В асиметричних системах необхідно застосовувати довгі ключі (512 бітів і більше). Довгий ключ різко збільшує час шифрування. Крім того, генерація ключів вельми тривала. Зате розподіляти ключі можна по незахищеним каналам.

У симетричних алгоритмах використовують більш короткі ключі. Шифрування відбувається швидше. Але в таких системах складно організувати розподіл ключів [3].

Треба зауважити, що в урядових і військових системах зв'язку використовують лише симетричні алгоритми, так як немає строго математичного обґрунтування стійкості систем з відкритими ключами, як, втім, не доведено і зворотне.

2.1.1. Асиметричні алгоритми шифрування

Створення алгоритмів асиметричного шифрування є найбільшим і, можливо, єдиним революційним досягненням в історії криптографії. Алгоритми шифрування з відкритим ключем розроблялися для того, щоб вирішити дві найбільш складні задачі, що виникли при використанні симетричного шифрування.

Першим завданням є розподіл ключа. При симетричному шифруванні потрібно, щоб обидві сторони вже мали загальний ключ, який якимось чином повинен бути їм заздалегідь переданий. Діффі, один з основоположників шифрування з відкритим

ключем, зауважив, що ця вимога заперечує всю суть криптографії, а саме можливість підтримувати загальну секретність при комунікаціях.

Другим завданням є необхідність створення таких механізмів, при використанні яких неможливо було б підмінити кого-небудь з учасників, тобто потрібен цифровий підпис. При використанні комунікацій для вирішення широкого кола завдань, наприклад, в комерційних і приватних цілях, електронні повідомлення і документи повинні мати еквівалент підпису, що міститься в паперових документах [3]. Необхідно створити метод, при використанні якого всі учасники будуть переконані, що електронне повідомлення було послано конкретним учасником.

Початок асиметричним шифрів було покладено в 1976 році в роботі Уитфилда Діффі і Мартіна Хеллмана «Нові напрямки в сучасній криптографії». Вони запропонували систему обміну загальним секретним ключем на основі проблеми дискретного логарифма. Взагалі, в основу відомих асиметричних криптосистем кладеться одна зі складних математичних проблем, яка дозволяє будувати односторонні функції і функції-пастки. Наприклад, криптосистема Ривеста-Шаміра-Адельмана використовує проблему факторизації великих чисел, а криптосистеми Меркля-Хеллмана і Хору-Ривеста спираються на так звану задачу про укладання рюкзака [7].

Діффі і Хеллман досягли значних результатів, запропонувавши спосіб вирішення обох завдань, який радикально відрізняється від всіх попередніх підходів до шифрування.

2.1.2. Симетричні алгоритми шифрування

Спосіб шифрування, в якому для шифрування і розшифрування застосовується один і той же криптографічний ключ. До винаходу схеми асиметричного шифрування, єдиним існуючим способом, було симетричне шифрування. Ключ алгоритму повинен зберігатися в секреті обома сторонами. Ключ алгоритму вибирається сторонами до початку обміну повідомленнями.

Переваги:

- ✓ Швидкість (за даними Applied Cryptography - на 3 порядки вище).

- ✓ Простота реалізації (за рахунок більш простих операцій).
- ✓ Менша необхідна довжина ключа для порівнянної стійкості.
- ✓ Вивченість (за рахунок більшого віку).

Недоліки:

- ✓ Складність управління ключами у великій мережі. Це означає квадратичне зростання числа пар ключів, які треба генерувати, передавати, зберігати і знищувати в мережі. Для мережі в 10 абонентів потрібно 45 ключів, для 100 вже 4950, для 1000 - 499500 і т.д.
- ✓ Складність обміну ключами. Для застосування необхідно вирішити проблему надійної передачі ключів кожному абоненту, так як потрібен секретний канал для передачі кожного ключа обом сторонам [3-4].

2.2. Режими шифрування

Для будь-якого симетричного блокового алгоритму шифрування визначено чотири режими виконання.

ECB - Electronic Codebook - кожен блок з 64 бітів незашифрованого тексту шифрується незалежно від інших блоків, із застосуванням одного і того ж ключа шифрування [4]. Типові програми - безпечна передача одиночних значень (наприклад, криптографічного ключа).

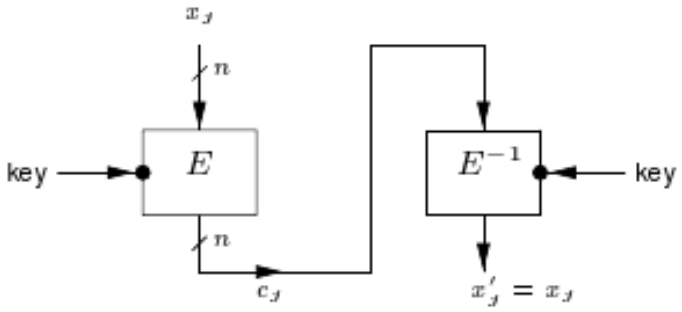

Рис 2.1. Схема режиму шифрування ECB

CBC - Cipher Block Chaining - вхід криптографічного алгоритму є результатом застосування операції XOR до наступного блоку незашифрованого тексту і

попереднього блоку зашифрованого тексту [2]. Типові програми - загальна блок-орієнтована передача, аутентифікація.

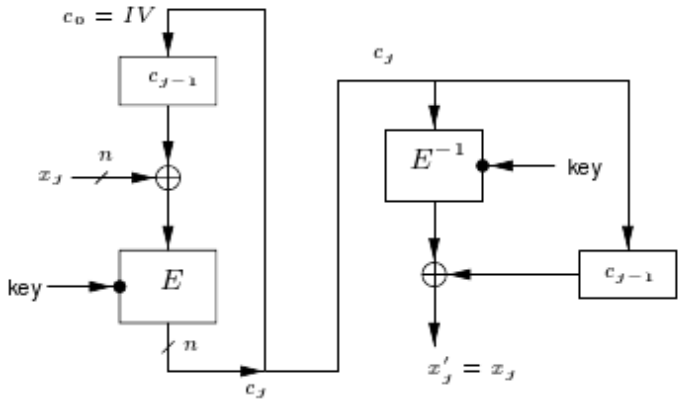

Рис 2.2. Схема режиму шифрування CBC

CFB - Cipher Feedback - при кожному виклику алгоритму обробляє J бітів вхідного значення. Попередній зашифрований блок використовується в якості входу в алгоритм; до J бітам виходу алгоритму і наступного незашифрованому блоку з J бітів застосовується операція XOR, результатом якої є наступний зашифрований блок з J бітів [4]. Типові програми - аутентифікація.

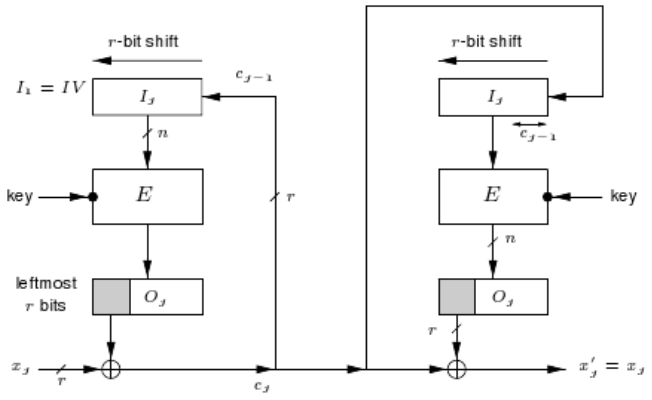

Рис 2.3. Схема режиму шифрування CFB

OFB - Output Feedback - аналогічний CFB, за винятком того, що на вхід алгоритму шифрування наступного блоку подається результат шифрування попереднього блоку; тільки після цього виконується операція XOR з черговими J

бітами незашифрованого тексту [4-5]. Типові програми - потокоорієнтована передача по зашумленому каналу (наприклад, супутниковий зв'язок).

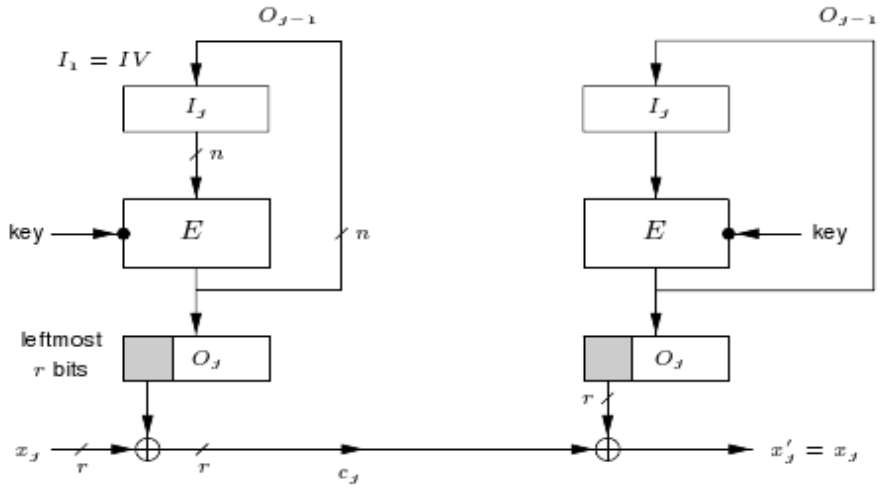

Рис 2.4. Схема режиму шифрування OFB

Для наочної ілюстрації різниці в них наведено рис. 2.5.

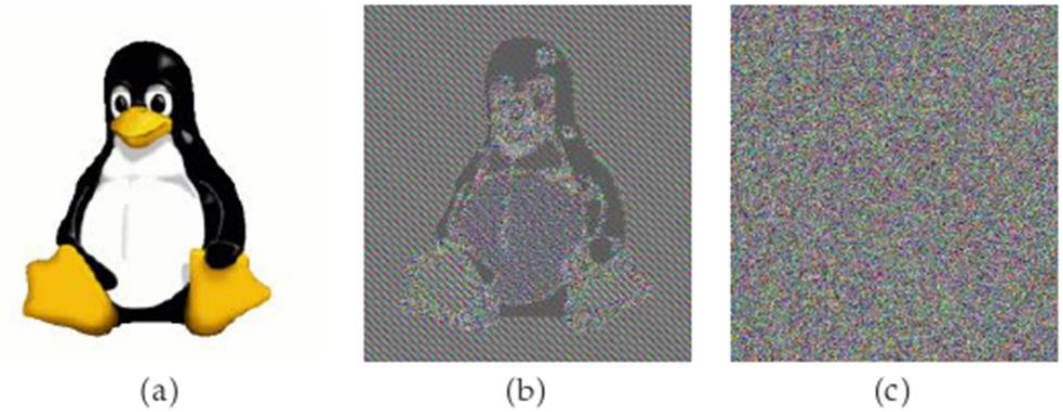

Рис 2.5. Проблема при шифруванні блоковими алгоритмами:
(a) оригінальна картинка; (b) зашифровано в режимі ECB;
(c) зашифровано в режимі CBC

На рис. 2.5. при режимі електронної книги (ECB) видно, що загальні обриси ще можна розрізнити, а при використанні зчеплення блоку, картинка перетворюється в «білий шум», який близький за своєю природою до випадкових чисел.

2.3. Розробка захищеної структури сегмента мережі підприємства на базі технології VIPNet

В ході дипломного проектування захищеного каналу інформаційного обміну на підприємстві запропоновано таку загальну структуру захищеної розподіленої обчислювальної мережі.

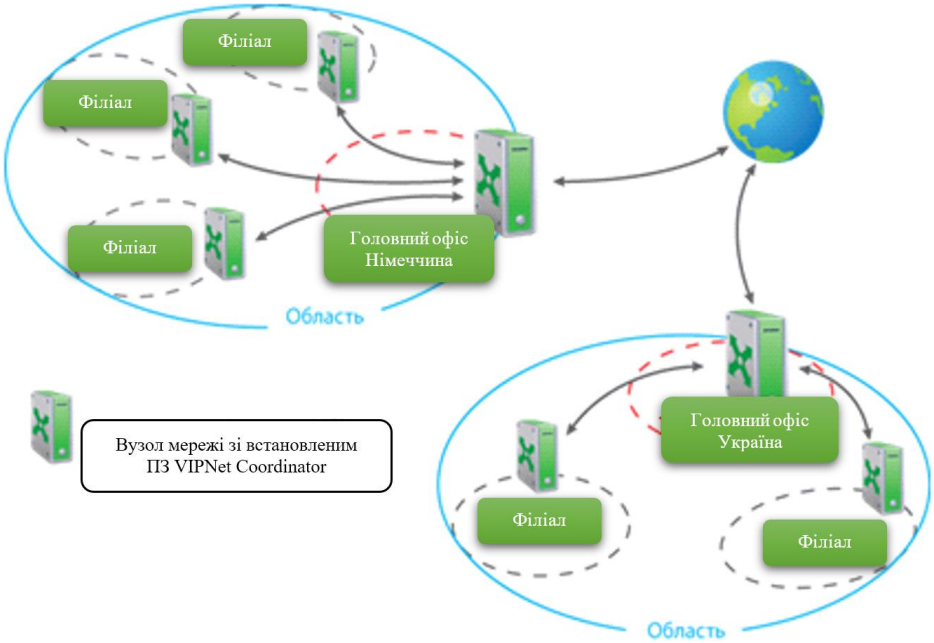

Рис. 2.6. Загальна структура захищеної розподіленої обчислювальної мережі

Для виконання такої структури була розроблена загальна форма, згідно з визначеними зв'язками між різними вузлами цих мереж, безпечною структурою взаємодії між іншими VIPNet мережами, яка показана на рис. 2.7.

Перевага цієї структури полягає в тому, що немає необхідності переконфігурувати RV мережі, оскільки можливості програмного забезпечення дозволяють без витрат на апаратну та програмну частину мережі розробляти таку необхідну для виконання структуру [6]:

1. Додати або видалити мережеві вузли (координатори клієнтів);
2. Додати або видаляти посилання між мережевими вузлами;
3. Створювати ключі та довідкові відомості, змініть та видалити;
4. Змінити права клієнтів.

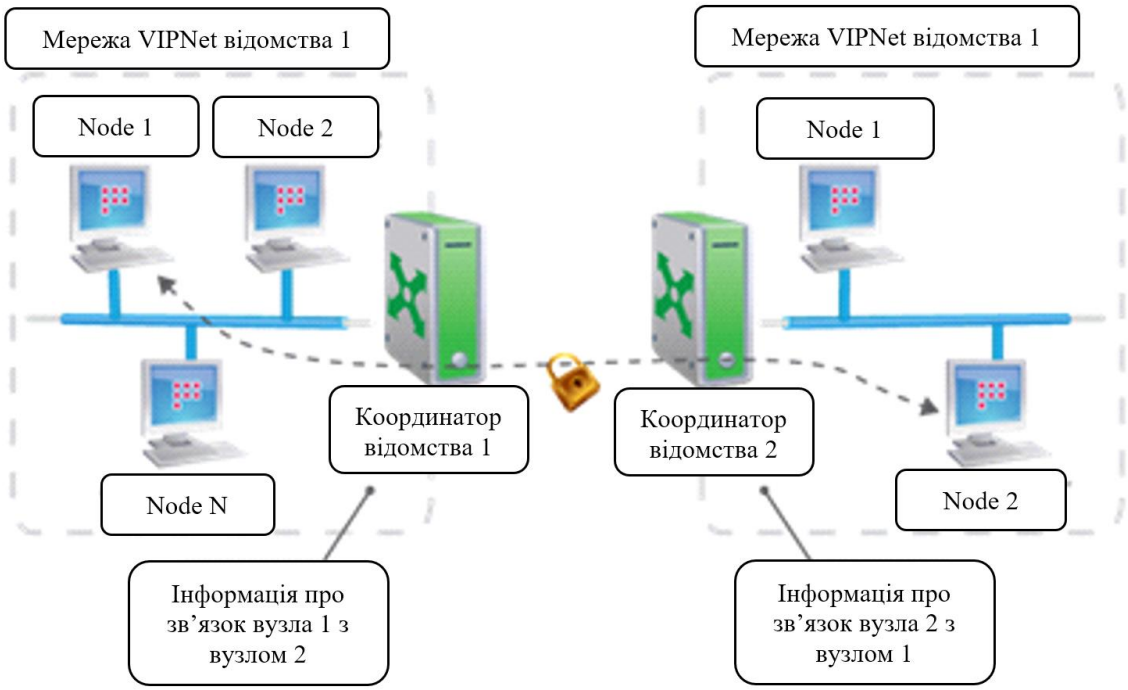

Рис. 2.7. Загальна структура корпоративної мережі з використанням продуктів ViPNet

Використання технології VIPNet надає функції брандмауера, розгорнуті для відкритих з'єднань та зберігання; системи виявлення вторгнень (IDS); клієнта поштової служби (фільтрація SPAM та розмежування доступу), віртуальна адресація.

2.4. Засоби для захисту сегмента корпоративної мережі підприємства на базі комплексу VIPNet

Щоб розгорнути мережу VIPNET, достатньо встановити програмне забезпечення VIPNet на робочу станцію. Крім того, практично не потрібно змінювати топологію існуючої мережі або отримати додаткове обладнання. Щоб організувати безпечне з'єднання, схема автоматично розподіляється на етапі встановлення за допомогою **ключа шифрування** та процесу їх синхронного оновлення. Кожен пакет, надісланий до мережі, автоматично зашифрований, використовуючи унікальну похідну клавішу без процедур налаштування з'єднання (рукостискання). Це дозволяє організувати передачу даних, захищених неймовірними каналами, що

характеризується великим рухом LOS, а також забезпечити безперебійну роботу локальної мережі. Затримка неприйнятна у такому зв'язку [5].

За допомогою цього підходу до структури мережевого сегмента, не втрачаючи якість комплексу, технологія VIPNet забезпечує стійкість властивостей збережених сполук, які значно впливають на безпеку. А саме: безперервне шифрування всього IP-пакета з джерелом IP-адреси та протоколом, безперервна підтримка пакета (безпека від реалізації фальшивих пакетів), шифрування є лише частиною трафіку. Протокол, який використовується як частина технології VIPNet, забезпечує захищену передачу даних на будь-які канали зв'язку через будь-які канали NAT / PAT, навіть якщо підключення до інтернет-провайдера, обмежується VoIP або IPSEC.

Технологія VIPNet використовує з'єднання Perge, що забезпечує автоматичні сповіщення про пов'язані вузли та параметри доступу. Це дозволяє застосувати класичну схему з’єднання IPSec, але також з можливістю поєднання комп'ютера та комп'ютера автоматично.

Це дозволяє організувати однорангове з'єднання між підмережами та вузлами, розташованими в межах іншої захищеної мережі. Координатор HW 1000.

Призначення:

✓ Криптошлюз і FireWall, побудований на апаратній платформі телекомунікаційних серверів компанії "Aqua". Він легко інсталюється в існуючу інфраструктуру, надійно захищає передану по каналах зв'язку інформацію від несанкціонованого доступу і підміни. Використання адаптованої ОС Linux і надійної апаратної платформи серверів AquaServer дозволяє застосовувати ViPNet Coordinator HW1000 в якості корпоративного рішення, до якого пред'являються найжорсткіші вимоги по функціональності, зручності експлуатації, надійності та відмовостійкості.

Переваги:

✓ Використання в якості апаратної платформи надійного промислового сервера типорозміру 19" в стійку 1U;

✓ Програмне забезпечення створено на базі перевірених багаторічною експлуатацією ПЗ ViPNet Coordinator Linux і технології захисту інформації ViPNet;

✓ Кількість одночасно встановлених з'єднань через криптошлюз не обмежується;

✓ Підтримка роботи в сучасних мультисервісних мережах зв'язку з серверами DHCP, WINS, DNS і перетворенням адрес (NAT, PAT);

✓ Використання в якості центру генерації ключів шифрування сертифікованого ПЗ ViPNet Administrator зі складу СКЗІ «Домен-КС2 / КМ» • Низька вартість у порівнянні з аналогічними за можливостями СЗІ інших вітчизняних компаній.

Область застосування:

✓ ІСПДн К1 / клас АС - 1В.

2.5. Запропонований склад комплексу VIPNet CUSTOM

В даний час VIPNet CUSTOM включає понад 15 різних компонентів, які дозволяють виконувати багато сценаріїв з захисту інформації в сучасних багаторангових комунікаційних мережах.

Client IOS - це програма, яка працює за допомогою операційної системи Apple IOS, призначену для забезпечення захисту iPad та iPhone від мережевих атак та дозволяють доступ через технологію VPN до захищених ресурсів корпоративних мереж.

Адміністратор - це базовий програмний пакет для налаштування та управління мережами безпеки, включаючи: NCC (центр керування мережею, TSUS) - програмне забезпечення, призначене для управління конфігурацією та віртуальною безпекою VIPNET мережі; KC & CA (Certification and Key Center, UKC) - програмне забезпечення для виконання функцій ключа шифрування користувача та персонального ключа Конференц-центру, а також функції сертифікаційного центру.

Центр моніторингу - це ПЗ, розгорнуте технологією клієнтського сервера та призначене для моніторингу стану захищених вузлів VIPNET мережі.

VIPNet StateWatcher - це сервер програмного забезпечення з стандартною базою даних SQL мережевих вузлів, встановлених з клієнтом VIPNET, з можливістю

доступу до цих даних та результатів операцій правил рукотворного аналізу новин через дистанційне використання веб-доступу за допомогою браузера.

Видавнича служба VIPNET призначена для автоматизації процедур VIPNET (адміністратор, користувач, перехресний сертифікат) та список (SOS) на точках розподілу даних. Також забезпечити імпорт SOS, відкинуту стороннім СС.

Пакет реєстрації VIPNET призначений для створення безпечних послуг для користувачів, зберігання даних реєстрації, створення вимог до сертифікату та технічного обслуговування в UKZ, а також запит на обслуговування в основних дистрибутивах користувачів мережі VIPNET в UKZ.

Координатор (Linux) - повнофункціональний програмний сервер VIPNET - захист встановлений на Linux OS 2.4.2 / 31 -2.6.2 / 26 (RedHat, SUSE та ін.) Залежно від налаштувань координатора VIPNET, можна представити наступні функції :

- ✓ IP-адресний сервер;
- ✓ Проксі-сервери захищених сполук;
- ✓ Тунельний сервер (Cryptoclusa);
- ✓ Брандмауери для відкритих, безпечних та тунельних ресурсів;
- ✓ Безпечний поштовий сервер;
- ✓ VIPNET мережа захищена перемикачем резервного копіювання у конфігурації захисту від відмови VIPNET.

Кластер (Windows) VIPNet Cluster Package - це програмне забезпечення для Windows 10, засноване на високодоступних та розподілених принципах. **Cluster PC VIPNET** має можливість обробляти мережевий трафік з декількох мереж, пов'язаних безпосередньо з нею. Всі кластерні фактори представлені в кожній підключеній мережі з тією ж IP-адресою, і працює на всіх кластерних чинниках. Це забезпечує перерозподіл функцій у кластері у разі невдачі одного з вузлів. VIPNET CLUSTER PC дозволяє створювати інфраструктуру, щоб сесія не була перервана до тих пір, поки працює один з коефіцієнтів кластерів. Там повинно бути щонайменше три коефіцієнт кластери як частина цілого кластера. У цьому випадку досягнуто максимальну ефективність управління працездатністю кожного координатора кластерних технологій (Windows) - **VIPNET Security Network Server** встановлюється на

Windows 10 / Windows 10 Server (32-64) Біти). Залежно від установки координатора VIPNET, можна представити наступні функції:

- ✓ IP-адресний сервер;
- ✓ Проксі-сервери захищених сполук;
- ✓ Тунельний сервер (Cryptoclusa);
- ✓ Брандмауери для відкритих, безпечних та тунельних ресурсів;
- ✓ Безпечний поштовий сервер;
- ✓ Сервер мережевого сервера VIPNET та кластера VIPNET.

Координатор VIPNET HW-VPNM, як розширений модуль для універсальних портів безпеки USG2000, Huawei Symantec, легко встановлюється в існуючу, надійну інфраструктуру захисту від підміни та несанкціонованої заміни RVPN VIPNET.

VIPNET Infoten, Cisco Systems є санкціоновані та випущені програмні забезпечення та апаратні рішення, які поєднують в собі всі переваги систем Cisco. У той же час, як програмне забезпечення виконує функціональність пароля та брандмауера, версія Linux VIPNET координатор використовується. Координатор VIPNET HW1000 - це брандмауер, побудований на апаратній платформі телекомунікаційних серверів BAO BINH та виконує функції криптоперетворювача та брандмауерів. Він може легко інтегруватися в існуючу інфраструктуру, надійно захищаючи інформацію від несанкціонованого доступу та заміни каналів зв'язку. Використання OS Linux налаштовується, а надійна апаратна платформа Aqua Servers дозволяє вам застосувати координатор VIPNET HW1000 як рішення для компанії, до якої висуваються найбільш суворі вимоги функцій ЗІ та зручність роботи, надійність. HW 100 Координатор - це компактний брандмауер, який дозволяє забезпечити доступ для будь-якого мережевого пристрою у віртуальну приватну мережу, побудовану з продуктами VIPNET та передавачем інформації від несанкціонованого доступу та заміни.

Vipnet CryptService (Cryptservice) - це інтерактивний інструмент автоматизації з відкритою інфраструктурою блокування, побудованого на базі CC VIPNET, а також симетричну структуру обраного адміністратором мережі ключового простору, яка використовується в мережах VIPNET. Крім того, VIPNET CRYPTSERVICE дозволяє вставляти зашифровані функції для створення готових

додатків PKI: пост-терміналів та банківських систем, системи електронного документообігу, тощо.

Client - це пакет для Windows 10 / Windows 10 Server (32-64 біт). Виконання даного ПЗ пропонується на робочих місцях або серверах з VPN. Функція клієнта, персональний міжмережевий екран, захищена поштова система, а також криптоперетворювач для програмних застосунків за допомогою ЕЦП та функцій шифрування.

Застосування запропонованих компонентів комплексу VIPNet АРК на рис. 2.8.

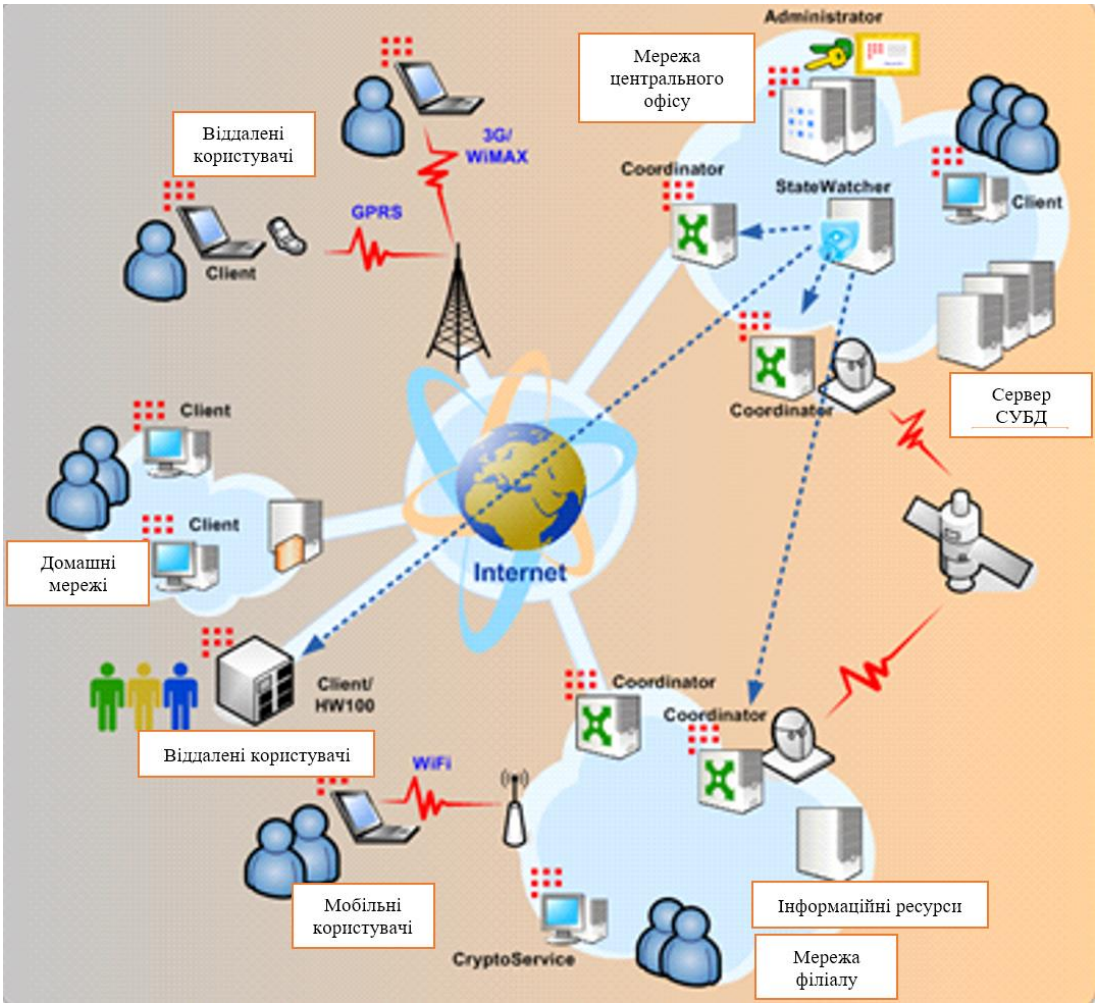

Рис. 2.8. Застосування запропонованого складу комплексу АРК VIPNet

Для структур, запропонованих для організації захищеного каналу в корпоративній мережі підприємства запропонуємо використання компонентів комплексу, описаного вище та показаного на рис. 2.8.

За допомогою запропонованого розгортання компонентів з'являються наступні функції:

- ✓ Захист відеоконференції та IP-телефонів;
- ✓ Доступ до розподілених інформаційних ресурсів комбінованої мережі;
- ✓ Безпечне використання каналів зв'язку для уніфікації віддалених офісів;
- ✓ Безпечне підключення віддаленого користувача до ресурсів локальних мереж;
- ✓ Видалення конфліктів перетину IP-адрес в локальних мережах;
- ✓ Визначення та автентифікування трафіку у безпечній мережі в режимі точки;
- ✓ Авторизація користувачів VPN;
- ✓ Контроль та керування дистриб'юторською мережею;
- ✓ Структура PKI.

Подальші переваги з такої конфігурації введення:

- ✓ Можливість поєднати до 4000000 вузлів з віртуальними мережами, використовуючи VIPNET.
- ✓ Здатність виділяти сегменти, захищені в існуючих мережах.
- ✓ Можливість організувати окремі сегменти в мережі.
- ✓ Збереження існуючої IT-інфраструктури.
- ✓ Легке розширення VPN.
- ✓ Повна підтримка віртуальних адрес у мультимедійних протоколах SIP, SCCP (Cisco Skinny), H.323.
- ✓ Забезпечення прийняття захисту від перешкод за допомогою різних пристроїв NAT або у випадку використання Інтернету.

ВИСНОВОК ДО РОЗДІЛУ 2

Розроблено систему захисту сегмента мережі підприємства, в якій було реалізовано розвиток захищеної структури сегмента мережі підприємства на основі технології VIPNet, і структурований RV захищений у програмі VIPNET для LPUMG Розроблено спосіб застосування технології VIPNet до захищеного сегмента корпоративної мережі. Запропоновано склад індивідуального комплексу VIPNet. Представлено застосування запропонованого компонента комплексу VIPNet APK.

РОЗДІЛ 3
МОДЕЛЮВАННЯ, ПРОДУКТИВНОСТІ І МАСШТАБОВАНОСТІ ЗАХИЩЕНИХ КАНАЛІВ

3.1. Моделювання та оцінка продуктивності роботи захищених каналів

Вибір криптоалгоритму і серверної ОС є одним з найважливіших етапів побудови захищеного каналу корпоративної мережі. У випадку, якби всі алгоритми були ідеальними (тобто не мали ніяких вразливостей), то криптостійкість його була б прямо пропорційна довжині ключа, так як єдиним способом для злому криптограми був метод брутфорсу. Всі вищеописані алгоритми за весь час існування не були скомпрометовані жодного разу, отже, будемо спиратися при оцінці стійкості алгоритму на довжину ключа. Збільшення довжини ключа сильно позначається на продуктивності даного алгоритму через збільшення кількості раундів при шифруванні [7]. Як приклад для тестування було обрано симетричний алгоритм блочного шифрування AES з розмірами ключового простору 128 і 256 біт. Цей вибір пояснюється тим, що з одного боку він є стандартом шифрування в багатьох країнах і, як наслідок, буде використовуватись в складі комплексу VIPNet для реалізації захищеного каналу в корпоративній мережі. Тестування проводилося з двома серверними операційними системами Windows 10 Server і Fedora Core 8.0., З огляду на величезний ринок серверних програм, які потребують цих середовищах.

3.1.1. Оцінка продуктивності захищеного каналу

Для основного тестування в реальних умовах експлуатації були обрані серверні потужності Intel Xeon E5 з частотою 3.6 ГГц і об'ємом оперативної пам'яті в 16 Гб. В якості клієнтів були обрані комп'ютери Intel Core i5 з частотою 2.8 ГГц і оперативною пам'яттю в розмірі 4 Гб. Всі комп'ютери були об'єднані в корпоративну мережу за допомогою комутаційного обладнання. Тестування проводилося з двома серверними ОС Windows 10 Server і Fedora Core 8.0.

На VIPNet клієнтах використовувалася ОС Windows 10. Для реалізації зашифрованого каналу було обрано програмний комплекс VIPNet CUSTOM.

Як тестуючий засіб узятий програмний продукт з графічною оболонкою JpREF версії 3.7.1, що являє кросплатформене ПЗ клієнт-серверної архітектури - генератор TCP і UDP трафіку для тестування пропускної здатності мережі [9].

Налаштування VIPNet с застосуванням сертифікатів X.509.

Файл конфігурації серверів зображений на рис. 3.1.

```
dev tap
server 192.168.0.0 255.255.255.0
cipher AES-128-CBCauth key.txt 0serverdh1024.pemca.crtswat.crtswat.key
keepalive 10 60
Файл конфігурації клієнтів:
remote 192.160.1.111
dev tapAES-256-CBCauth key.txt 110 60clientdh1024.pem
ca ca.crtclient.crt
key client.key
```

Рис. 3.1. Конфігурація серверного обладнання з ПЗ VIPNet для проведення тестування захищеного каналу обміну корпоративною інформацією

Для обрання мережевої ОС в умовах роботи безлічі віддалених клієнтів з сервером по захищеному каналу необхідно отримати кількісну оцінку залежності пропускної здатності цього каналу від типу мережевої ОС, довжини ключа криптографічного алгоритму, кількості віддалених клієнтів. Під пропускною здатністю захищеного каналу (його продуктивністю) будемо розуміти кількість переданої інформації в одиницю часу **[bits / sec]**.

Для вирішення поставленого завдання зробимо обчислювальний експеримент, використовуючи пакет JpREF, для одного, двох і трьох клієнтів протягом часу 30 сек. для альтернативних варіантів мережевих ОС.

Результати тестування для варіанту використовуваних ОС: сервер - Windows 10 Server, клієнт - Windows 10, представлені в таблиці 3.1

Таблиця 3.1.

Результати тестування захищеного каналу системи VIPNet для варіанта: Windows 10 Server з клієнтами Windows 10

Кількість клієнтів	Тип алгоритму шифрування							
	AES-128-CBC				AES-256-CBC			
	вих.	вхід.	сума	CPU	вих.	вхід.	сума	CPU
1	21	33,3	54,38	22,7	13,2	30,3	43,52	23
2	18,5	28,3	48,89	28,1	10,7	10,5	21,13	27,3
3	16	40,7	57,69	31,5	17,4	35,2	47,6	31,7

У таблиці 3.1 використані такі умовні позначення:

- ✓ **Вих.** - вихідний трафік від сервера до клієнта за одиницю часу [bits / sec];
- ✓ **Вхід.** - вхідний трафік від клієнта до сервера за одиницю часу [bits / sec];
- ✓ **Сума** - підсумований вихідний і вхідний трафік за одиницю часу [bits / sec];
- ✓ **CPU** - завантаження центрального процесора серверної платформи представлена у вигляді % від максимально допустимої.

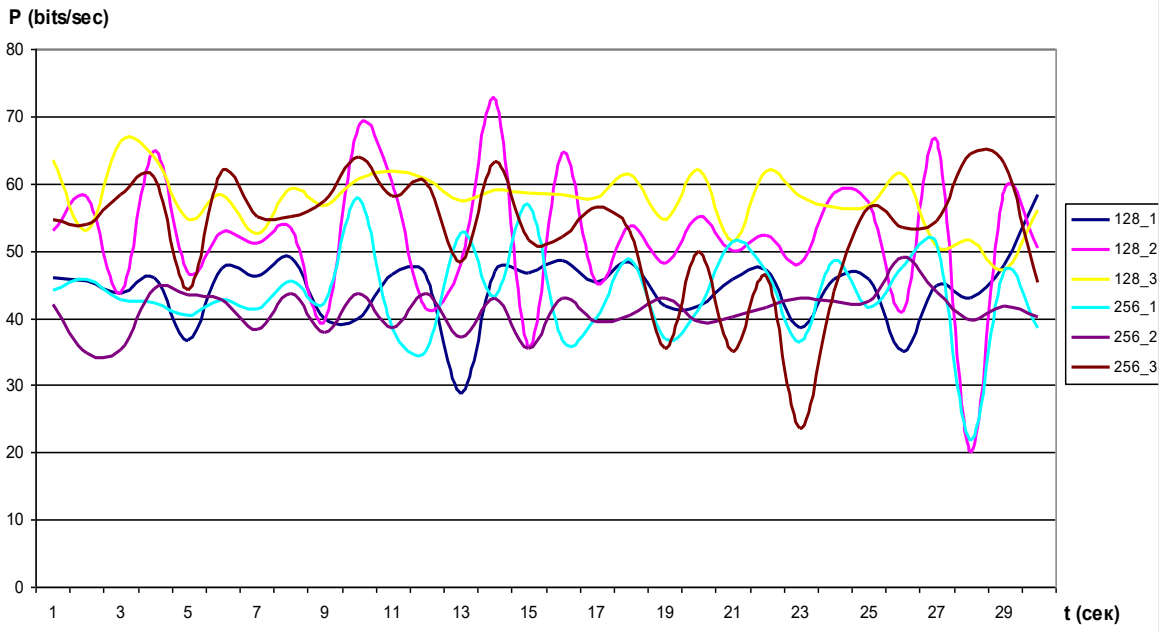

Рис 3.2. Пропускна здатність захищеного каналу корпоративної мережі з серверною ОС Windows 10 Server

На рис. 3.2 використані такі умовні позначення:

*** _ * приклад (128_1);

*** - розмір ключа шифрування в бітах 128, 256;

* - кількість віддалених клієнтів при тестуванні мережі.

P - пропускна здатність захищеного каналу, приймається значення в одиницю часу [bits / sec].

Таблиця 3.2.

Результати тестування захищеного каналу для варіанта:

Fedora Core з клієнтами Windows 10

Кількість клієнтів	Алгоритм шифрування							
	AES-128-CBC				AES-256-CBC			
	вих.	вхід.	сума	CPU	вих.	вхід.	сума	CPU
1	22,5	33,6	55,04	23	22,5	31,7	54,21	22,4
2	20,3	32,2	51,47	27,7	22,3	30,8	53,16	26,6
3	27,9	41,8	68,68	29,6	24,5	39,2	63,78	30,5

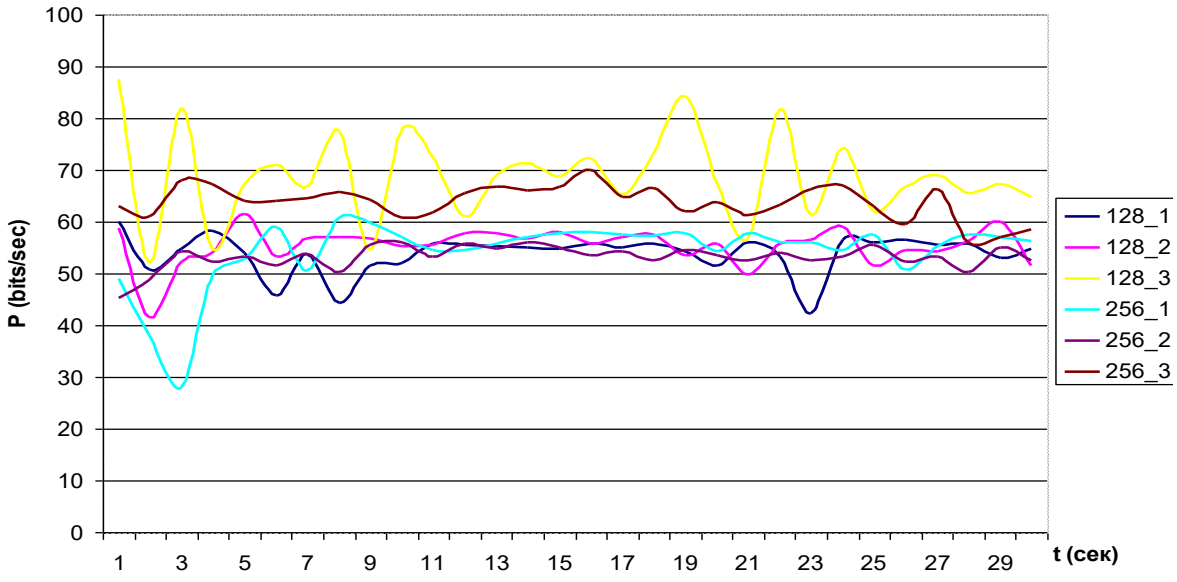

Рис 3.3 Пропускна здатність захищеного каналу корпоративної мережі з серверною ОС Fedora Core

В результаті було проведено 360 тестів, і на їх основі побудований зведений графік, який представляє загальну залежність пропускної здатності захищеного каналу мережі.

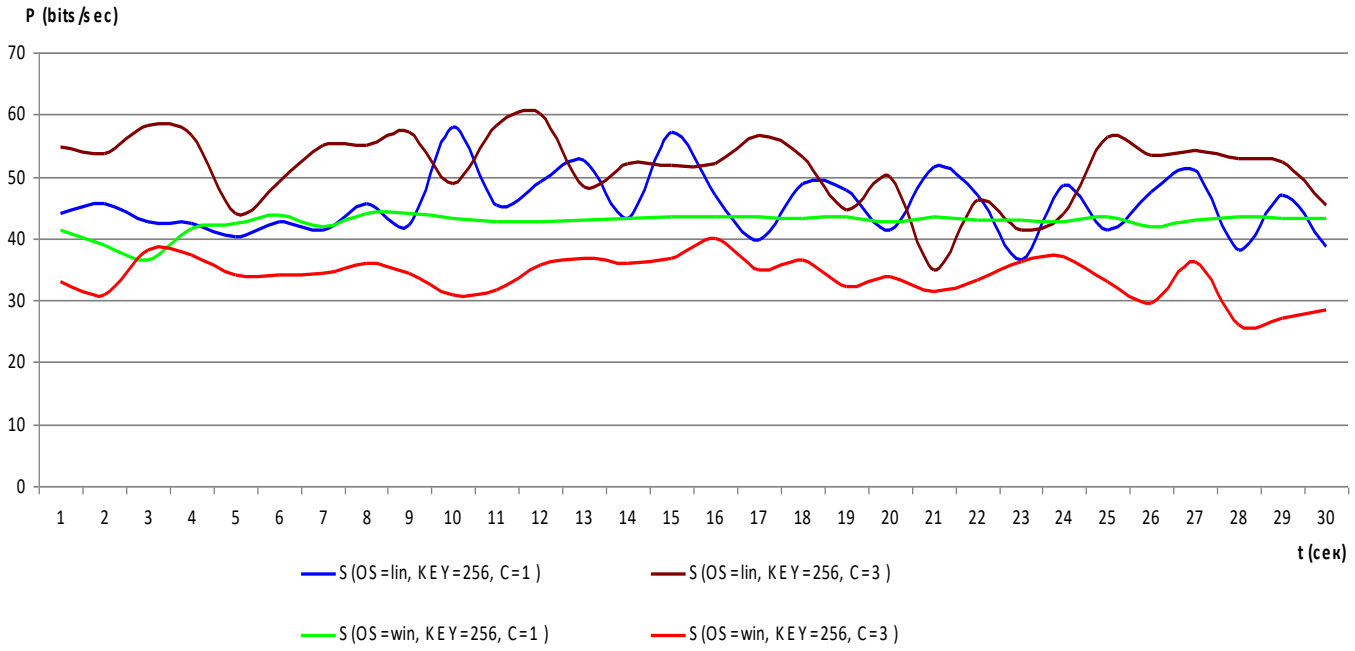

Рис 3.4. Пропускна здатність захищеного каналу корпоративної мережі з використанням альтернативних варіантів серверних ОС

На рис 3.4 використані такі умовні позначення:

- ✓ OS - тип мережевої операційної системи (MS Windows 10 Server, Fedora Core 8 (Linux));
- ✓ KEY - в bit (біт) - довжина ключа, встановленого для використовуваного протоколу шифрування (використана група протоколів AES-xxx-CBC, в назву якої замість xxx - довжини ключа використано значення 256 біт);
- ✓ C - кількість віддалених вузлів, що одночасно здійснюють обмін даними з сервером VIPNet VPN;
- ✓ P - пропускна здатність захищеного каналу, приймається значення за одиницю часу [bits / sec].

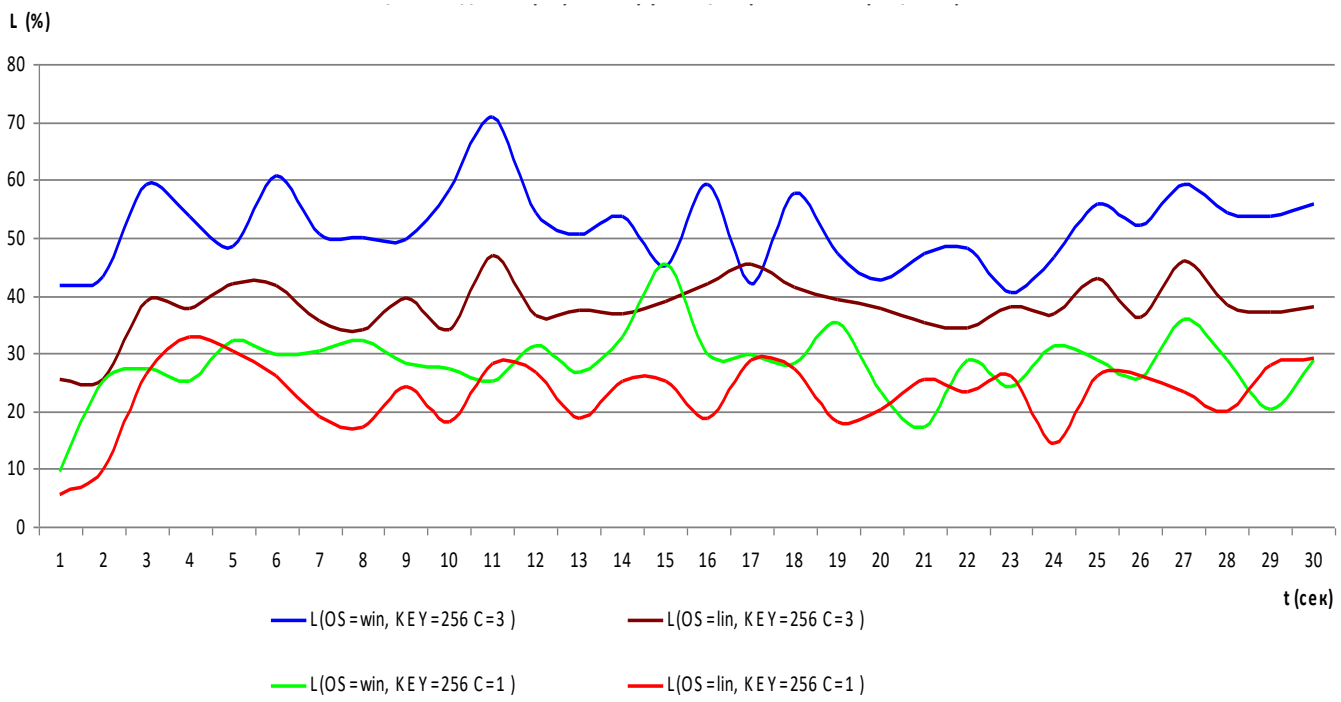

Рис 3.5. Графік завантаження центрального процесора при організації захищеного каналу в корпоративній мережі для альтернативних варіантів серверних ОС

На рис 3.5 використані такі умовні позначення:

- ✓ OS - тип мережевої операційної системи (MS Windows 10 Server, Fedora Core 8 (Linux));
- ✓ KEY - в bit (біт) - довжина ключа, встановленого для використовуваного протоколу шифрування (використана група протоколів AES-xxx-CBC, в назву якої замість xxx - довжини ключа використано значення 256 біт);
- ✓ C - кількість віддалених вузлів, що одночасно здійснюють обмін даними з сервером VIPNet VPN;
- ✓ L - завантаження центрального процесора сервера представлена у вигляді % від максимально допустимої;

Аналіз результатів у вигляді графіків, представлених на рис. 3.4, рис. 3.5, дозволяє зробити наступні висновки:

- ✓ За однакових умов збору статистики, ОС сімейства Fedora Core забезпечують більшу продуктивність у порівнянні з ОС Windows для організації захищеного каналу.

- ✓ В умовах роботи ОС Fedora Core збільшення кількості віддалених клієнтів не значно позначається на пропускній спроможності захищеного каналу, чого не можна сказати при використання ОС сімейства MS Windows 10 Server для неї характерні великі навантаження;
- ✓ Так само виходячи, з проведених тестувань, можна зробити висновок, що для сучасних комп'ютерів серверного класу довжина ключа шифрування захищеного каналу майже не позначається на загальній продуктивності системи.
- ✓ В умовах роботи ОС Fedora Core навантаження на центральний процесор значно менше, особливо при збільшенні кількості вузлів мережі. Для ОС сімейства MS Windows 10 Server існує досить великі навантаження на ЦП.

3.2. Розробка моделі функціонування корпоративної мережі

З метою автоматизації обрання оптимальних параметрів в захищеному каналі корпоративної мережі підприємства, побудованої на базі VPN рішення від VIPNet, необхідно задати функцію зворотного зв’язку, яка буде моніторити та ідентифікувати пропускну здатність КЗ в залежності від чинників, що впливають: ОС, довжини криптографічного ключа, кількості вузлів КМ. У якості математичного апарату, що дозволяє вирішити поставлене завдання виступає GMDH – Group Method of Data Handling. Він застосовується в самих різних областях науки і техніки для аналізу даних і відшукання знань, прогнозування та моделювання систем, оптимізації і розпізнавання образів. Індуктивні алгоритми GMDH дають унікальну можливість автоматично знаходити взаємозалежності в даних, вибрати оптимальну структуру моделі чи мережі та збільшити точність існуючих алгоритмів [6].

Цей підхід самоорганізації моделей принципово відрізняється від класичних дедуктивних методів. Він заснований на індуктивних принципах - знаходження кращого рішення засноване на переборі всіляких варіантів.

За допомогою перебору різних рішень підхід індуктивного моделювання намагається мінімізувати вплив автора на результати моделювання. Комп'ютер сам знаходить структуру моделі і закони, що діють в об'єкті. Він може бути використаний

при створенні штучного інтелекту як помічник для вирішення спорів і при прийнятті рішень.

Іншою перевагою GMDH є те, що він гарантує стійкість одержуваних моделей. Чим більше ступінь неточності даних, яка характеризується відношенням потужності перешкоди до потужності точних даних, тим простіше модель оптимальної складності, тому GMDH при збільшенні перешкод вибирає все більш вузькі межі області моделювання і все більш прості структури моделей [9]. Таким чином, при самоорганізації моделі на ЕОМ вибирається структура, найближча до оптимальної для кожного рівня співвідношення сигнал / завада.

Виходячи з вищевикладеного, GMDH - найбільш зручний засіб для вирішення завдання кількісної ідентифікації системи, яка дозволяє отримати об'єктивну, стійкість перед перешкодами, несуперечливу модель оптимальної структури.

Для підготовки елементів вибірки до використання в GMDH необхідно провести її приведення до відрізка [0,1].

Для нормальної випадкової величини 99,7% значень знаходяться всередині інтервалу $\left[\vec{X}-3\sigma, \vec{X}+3\sigma\right]$, де $\vec{X}$ - середнє значення, σ - дисперсія цієї величини, тому значення, що знаходяться поза цим інтервалом, як правило, породжені різними похибками і є викидами, а, значить, такі спостереження повинні бути виключені з вибірки [8].

Після цензурування вибірки все її значення наводяться до відрізка [0,1] за формулою [8]:

$$X_{ij} = \frac{X_{ij} - X_{jmin}}{X_{jmax} - X_{jmin}}. \qquad (3.1)$$

Необхідність такого приведення викликана великим числом арифметичних операцій на елементах вибірки в GMDH, що при різних порядках чисел веде до накопичення великих похибок методу.

Для відновлення залежності використовується поліноміальний ітераційний алгоритм GMDH, в результаті роботи якого повинна бути отримана залежність:

$$f(x,\alpha)=\sum_{k=1}^{m}\alpha_k\prod_{j=1}^{l}x_j^{\beta_{kj}}\ , \tag{3.2}$$

де l - число елементів у вихідному базисі;

m - число доданків моделі з ненульовими значеннями коефіцієнтів – складність моделі [8].

Перед початком роботи алгоритму вибірка ділиться на дві частини: робочу, по якій модель будується, і екзаменаційну - на ній вона перевіряється.

Розглянемо докладніше процедуру GMDH.

В якості нульового наближення береться безліч моделей складності 1, це самі значення факторів. Таким чином, первісна модель має вигляд $t=\alpha_k x_k$, де коефіцієнт α_k визначається ітераційним методом найменших квадратів (МНК) по робочій частині вибірки, після цього по екзаменаційній частині вибірки визначається F найкращих моделей за допомогою зовнішнього критерію регулярності - мінімуму евклідової норми вектора нев'язки між реальним значенням відгуку і значенням для перевірки [8]:

$$R=\sum_{k=1}^{N_э}\left|t_k-f(x_k,\alpha_k)\right|\ , \tag{3.3}$$

де $N_э$ - число елементів екзаменаційної частини вибірки.

Для формування базису змінних подальших кроків процедури використовується функція $g=(v_1,v_2,...,v_m)$, яка з F кращих моделей попереднього кроку і l вихідних змінних формує базові змінні наступного кроку, наприклад:

$$g(w_1,w_2,w_3,\eta)=\eta_1 w_1+\eta_2 w_2 w_3\ . \tag{3.4}$$

Число F переданих від кроку до кроку найкращих моделей називається свободою вибору методу.

При формуванні базису r-го кроку враховується той факт, що на r-му кроці складність моделі не повинна перевищувати r. Паралельно з процесом побудови базису йде побудова набору коефіцієнтів для цього базису ітераційним МНК робочої частини вибірки і обчислення критерію регулярності екзаменаційної частини. У пам'яті ЕОМ в кожен момент часу зберігаються тільки F кращих моделей. При вичерпанні безлічі базисів r-го кроку здійснюється перехід до наступного $(r + 1)$.

Процес зупиняється при виконанні нерівності:

$$\min_k R_k^{r-1} \le \min_k R_k^r \le \min_k R_k^{r+1} \ , \tag{3.5}$$

і за результат приймається найкраща модель (r-1) кроку.

Тепер розглянемо докладніше процедуру підбору коефіцієнтів моделі по заданій структурі моделі ітераційним МНК.

Нехай задана структура моделі складності $m : f_1, f_2, \ldots, f_m$, необхідно підібрати коефіцієнти $\alpha_1, \alpha_2, \ldots, \alpha_m$, щоб наблизити значення відгуку з робочої частини вибірки:

$$t = \sum_{k=1}^{N_p} \alpha_k f_k = \varphi(\alpha, f) \tag{3.6}$$

з точністю до заданого e, щоб мінімізувати зважену суму квадратів відхилень:

$$S = \sum_{l=1}^{N_p} \beta_i (t_i - \sum_{k=1}^{m} \alpha_k f_{ki})^2 \to min \ , \tag{3.7}$$

де N_p - число спостережень в робочій частині вибірки [8].

Спочатку вагові коефіцієнти β_i спостережень передбачаються однаковими і рівними 1, з цими вагами будується система коефіцієнтів a_k, $k=1,2,...,m$ моделі у вигляді рішення системи лінійних рівнянь [8]:

$$\begin{aligned}
&\alpha_1 \sum_{l=1}^{N_p} \beta_i f_{1i}^2 + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{1i} f_{2i} + ... + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{1i} f_{ki} = \sum_{i=1}^{N_p} \beta_i t_i f_{1i} \\
&\alpha_1 \sum_{i=1}^{N_p} \beta_i f_{2i} f_{1i} + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{2i}^2 + ... + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{2i} f_{ki} = \sum_{i=1}^{N_p} \beta_i t_i f_{2i} \\
&\alpha_1 \sum_{i=1}^{N_p} \beta_i f_{ki} f_{1i} + \alpha_2 \sum_{i=1}^{N_p} \beta_i f_{ki} f_{2i} + ... + \alpha_k \sum_{i=1}^{N_p} \beta_i f_{ki}^2 = \sum_{i=1}^{N_p} \beta_i t_i f_{ki} .
\end{aligned} \tag{3.8}$$

Потім вибираються ваги β_i , $i = 1,2,...,N_p$ таким чином, щоб вага *i*-го спостереження залежала від *i*-го залишку в попередній ітерації до загальної мірою залишків в цій ітерації:

$$\beta_i = \frac{1}{S} \left| t_i - \sum_{k=1}^{m} \alpha_k f_{ki} \right| \tag{3.9}$$

і за цими вагами будується нова система коефіцієнтів моделі α_i , $i = 1,2,...,m$ і т.д. Процес зупиняється, коли досягається задана ступінь точності *e*, тобто коли виконається нерівність

$$\frac{1}{S_k} |S_k - S_{k-1}| \prec \varepsilon \quad . \tag{3.10}$$

Для використання отриманої залежності в моделі необхідно провести перерахунок коефіцієнтів моделі з урахуванням коефіцієнтів лінійного перетворення, яке здійснювалося при центруванні і нормуванні [6].

Для побудови функції відгуку скористаємося спеціалізованим пакетом для моделювання нейронних мереж NeuroShell 2 (Ward Systems Group, Inc.), в якому

реалізований комбінаторний алгоритм GMDH. Для побудови функції потрібно серія дослідів з різним станом мережі, будемо використовувати дані, отримані при тестування з Додатка А.

В результаті розрахунку з використанням пакета NeuroShell була отримана функція відгуку:

$$Y=-0.42-0.14*X1-8.8E-002*X2+0.4*X3+0.36*X3^2+6.7E-002*X1*X2+ 0.26*X1*X3-2.6E-002*X2*X3, \quad (3.11)$$

де:

X1=2*(win/lin-1)-1 операційна система;

X2=2*(key-128)/128 довжина ключа в бітах;

X3=(Kol-1)/2 кількість клієнтів беруть участь в тестування;

Y=2*S<->C- 6.54/87 (розрахункова продуктивність в тисячах bit/sec).

В результаті роботи пакета NeuroShell побудуємо графіки:

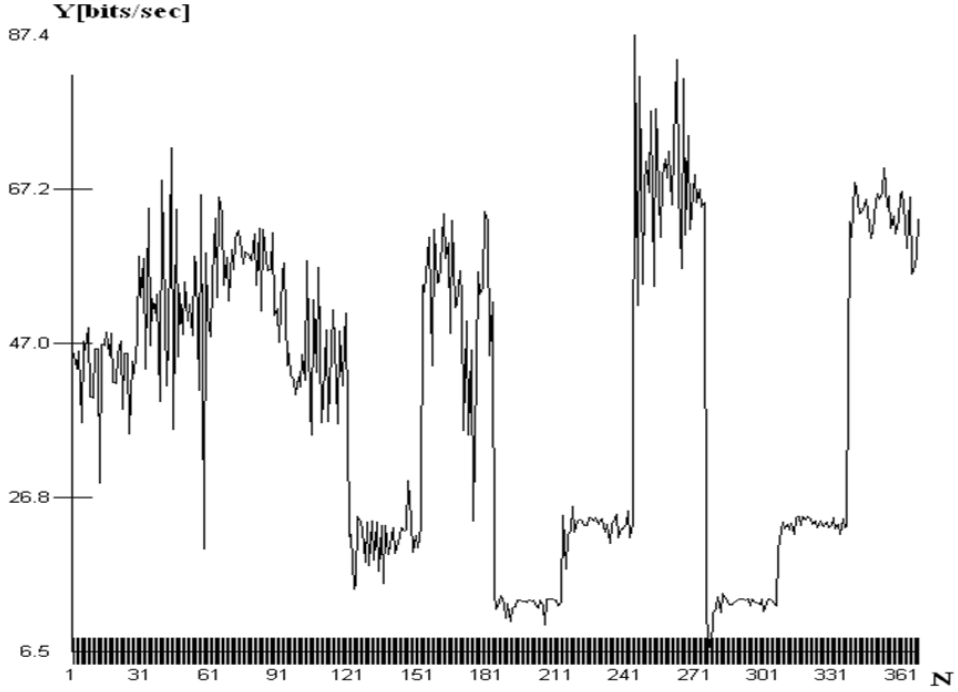

Рис 3.6. Графік продуктивності захищеного каналу побудований на основі даних отриманих дослідним шляхом.

Y- пропускна спроможність каналу [bits / sec]; **N** – порядковий номер досліду

Значення параметра N визначає умови в частині використовуваної мережевої операційної системи сервера, кількості віддалених клієнтів мережі та довжини ключа

шифрування. Вся необхідна інформація для побудови графіка, представлена на рис. 3.6-3.9, наведена в Додатку А.

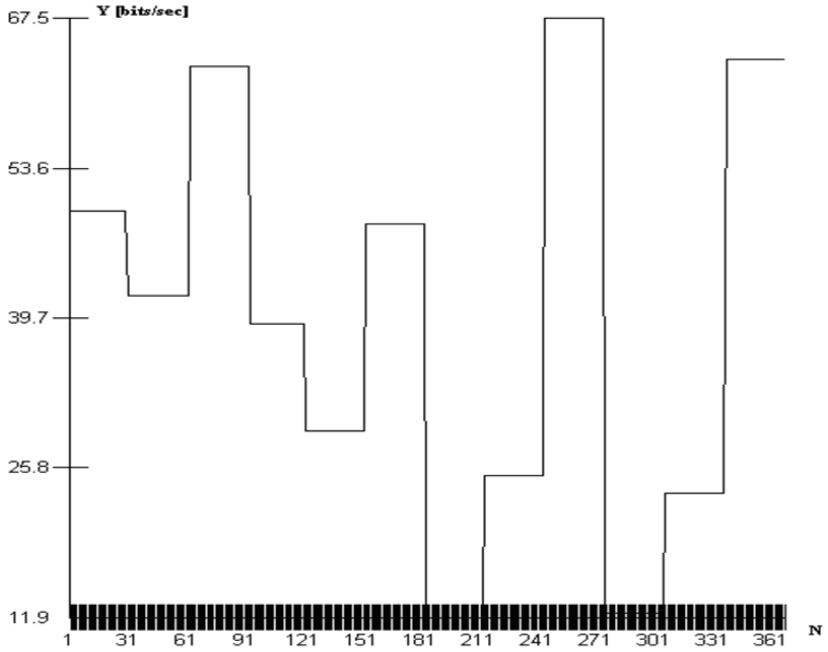

Рис 3.7. Графік функції *Y(N)* продуктивності захищеного каналу корпоративної

Для порівняння з вихідними даними, отриманими при прорахунку програмою, побудуємо разом з ним графік пропускної здатності мережі отриманий дослідним шляхом при тестуванні:

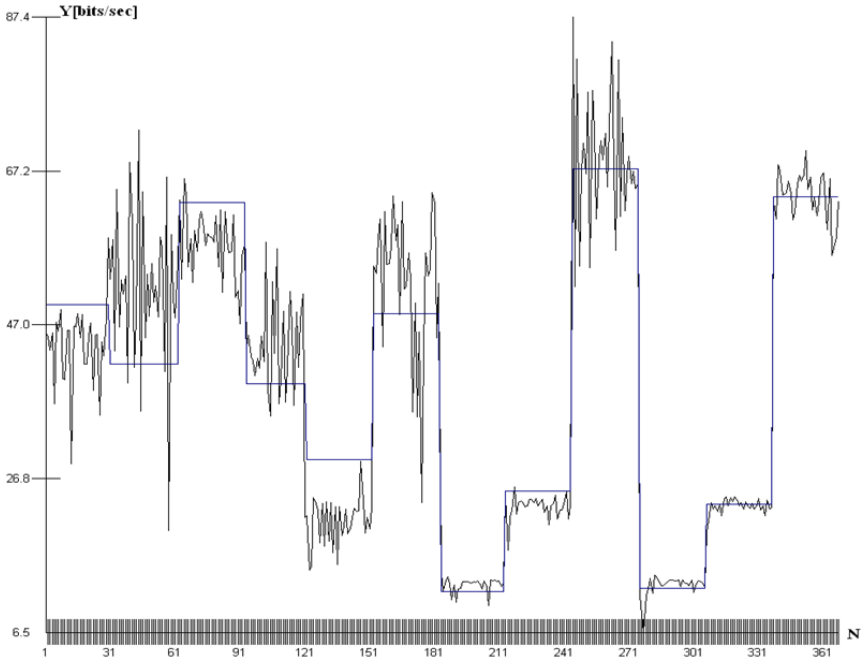

Рис 3.8. Суміщений графік функції відгуку Y (N) і емпіричних даних.

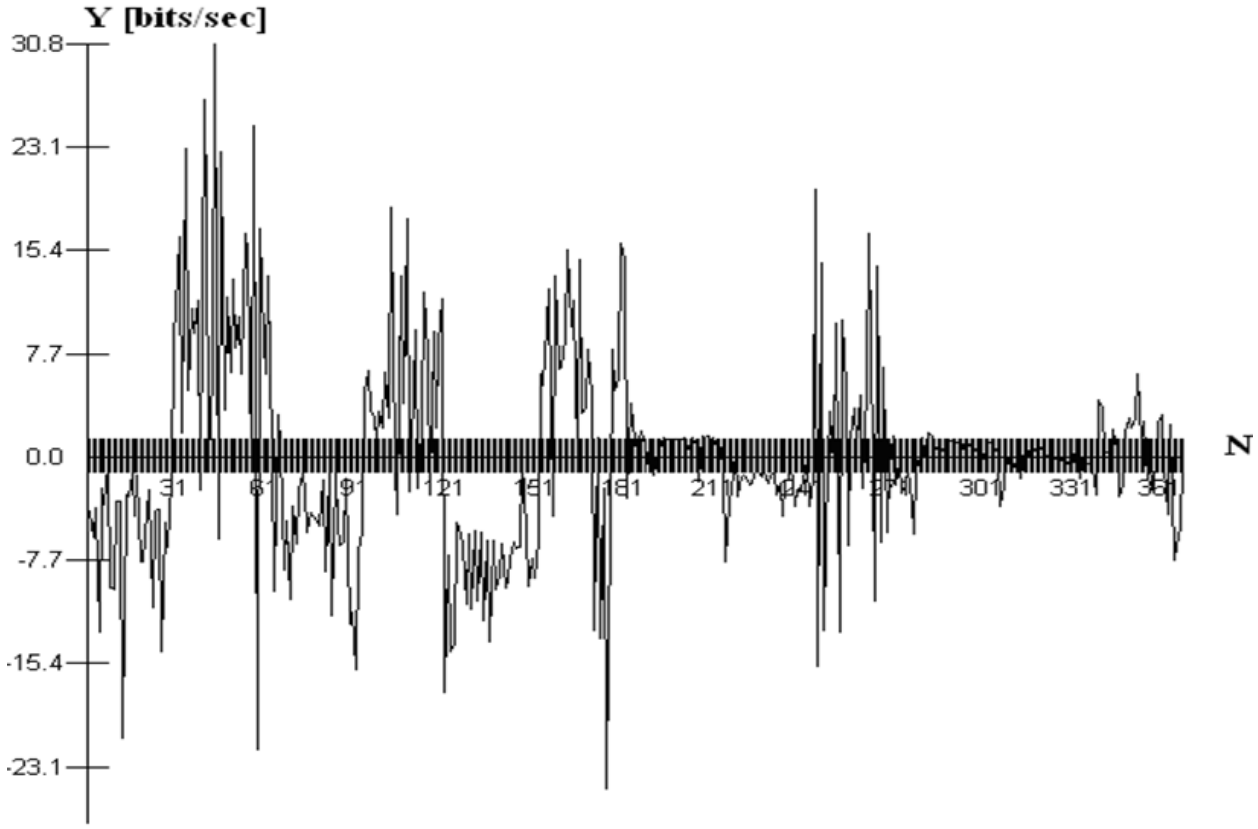

Рис 3.9. Графік середньоквадратичного відхилення помилки і кореляцією *Y(N)* і вихідних даних

З графіка рис 3.8 видно, що функція відгуку, отримана за допомогою пакету GMDH рис 3.7, схожа з графіком рис 3.6 побудованим на основі даних отриманих дослідним шляхом. Виходячи з цього можна судити про адекватність даної моделі в реальних умовах.

Отримана функція відгуку (3.11) дозволяє виробляти періодичну адаптацію моделі до змін в корпоративній мережі в залежності від навантаження. Дозволяє розрахувати продуктивність захищеного каналу при зміні ситуації в корпоративній мережі (зростання трафіку, зміна алгоритмів шифрування зміна кількості віддалених робочих станцій, що входять безпосередньо в корпоративну мережу). Ця функція може бути використана в програмному забезпеченні для керування захищеним каналом. Наприклад, такий додаток може виконувати динамічну зміну алгоритму шифрування на основі передбаченої моделі поведінки системи. Варто відзначити і те, що функцію можна автоматично адаптувати до середовища в міру розширення даних про стан каналу, так як GMDH дозволяє динамічно «навчатися» на нових вибірках.

3.3. Багатомірний регресійний аналіз

Для того щоб визначити значимість залежних змінних на отриману функцію зворотного зв'язку (3.11) проведемо багатовимірний регресійний аналіз.

Необхідно знайти оптимальний варіант моделі, що відображає основні закономірності досліджуваного явища з достатнім ступенем статистичної надійності.

У модель повинні бути включені всі фактори, які впливають на залежну змінну (в нашому випадку - кількість вузлів, операційна система, розмір ключа шифрування). При невиконанні цієї вимоги модель може виявитися неадекватною внаслідок недообліку істотних чинників.

З іншого боку, кількість факторів, що включаються в модель, не повинна бути занадто великою. Невиконання цієї вимоги призводить до необхідності збільшення числа спостережень, до неможливості використання досить складних залежностей, до зниження точності оцінок, до якої складності інтерпретації моделі і до труднощів її практичного використання [6].

Таким чином, виникає необхідність зменшення числа змінних, що включаються в модель, без порушення вихідних передумов, тобто задача зниження розмірності моделі.

Виділяють два істотних підходи до вирішення проблеми скорочення кількості вихідних змінних [9]:

- ✓ відсіювання менш істотних факторів в процесі побудови регресійної моделі;
- ✓ замінити оригінальний набор змінних меншим числом еквівалентних факторів, отриманих в результаті перетворень вихідного набору.

Процедура відсіву несуттєвих факторів в процесі побудови регресійної моделі і отримала назву багатокрокового регресійного аналізу.

Цей метод заснований на обчисленні декількох проміжних рівнянь регресії, в результаті аналізу яких отримують кінцеву модель, що включає тільки фактори, що мають статистично істотний вплив на досліджувану залежну змінну. Різні поєднання одних і тих же факторів надають різний вплив на залежну змінну. Внаслідок цього

з'являється необхідність вибору найкращої моделі, тому що перебирати всі можливі варіанти поєднання чинників і будувати безліч рівнянь регресії (кількість яких може бути дуже велика) просто не має сенсу [6, 8-9].

Таким чином методи покрокового регресійного аналізу дозволяють уникнути настільки громіздких розрахунків і отримати достатньо надійну і повну модель залежності досліджуваної ознаки від ряду пояснюють змінних.

Як було сказано вище, основою багатокрокового регресійного аналізу є побудова рівняння регресії. Розглянемо більш докладно його систему і основні поняття.

У загальному вигляді багатовимірна лінійна регресійна модель залежності у від пояснюють змінних x_1, x_2,…, x_k має вид:

$$\tilde{y} = M(y/x_i) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + ... + \beta_k x_k + \varepsilon . \quad (3.12)$$

Для оцінки невідомих параметрів β_j взята випадкова вибірка обсягу *n* з *(k + 1)* - мірою випадкової величини (у, x_1, x_2,…, x_k).

У формі модель має вигляд [8-9]:

$$Y = X\beta + \varepsilon , \quad (3.13)$$

де $Y = \begin{pmatrix} y_1 \\ y_2 \\ ... \\ ... \\ y_n \end{pmatrix}$, $X = \begin{pmatrix} 1\, x_{11}\, x_{12} ... x_{1k} \\ 1\, x_{21}\, x_{22} ... x_{2k} \\ ..... \\ 1\, x_{n1}\, x_{n2} ... x_{nk} \end{pmatrix}$, $\beta = \begin{pmatrix} \beta_0 \\ \beta_1 \\ ... \\ \beta_k \end{pmatrix}$, $\varepsilon = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ ... \\ \varepsilon_n \end{pmatrix}$ (3.14)

вектор-стовпець фактичних значень залежної змінної розмірності n;

матриця значень пояснюють змінних розмірності *n*(k + 1)*;

вектор-стовпець невідомих параметрів, що підлягають оцінці, розмірності *(k + 1)*;

вектор-стовпець випадкових помилок розмірності n з математичним очікуванням ME = 0 і коваріаційною матрицею

$$V(\varepsilon) = M(\varepsilon\,\varepsilon^T) = \sigma^2 E_n \tag{3.15}$$

відповідно, при цьому

$$E_n = \begin{pmatrix} 1\,0\,0\ldots 0 \\ 0\,1\,0\ldots 0 \\ \ldots\ldots\ldots \\ 0\,0\,0\ldots 1 \end{pmatrix}$$ - одинична матриця розмірності (*nxn*).

Оцінки невідомих параметрів β_j знаходяться методом найменших квадратів, мінімізуючи скалярну суму квадратів $Q = (Y - X\beta)^T (Y - X\beta)$ за компонентами вектору β.

Далі підставивши вираз [9]:

$$(Y - X\beta) = \begin{pmatrix} y_1 \\ y_2 \\ \ldots \\ y_n \end{pmatrix} - \begin{pmatrix} \beta_0 + \sum_{j=1}^{k} x_{1j}\beta_j \\ \beta_0 + \sum_{j=1}^{k} x_{2j}\beta_j \\ \ldots\ldots\ldots\ldots \\ \beta_0 + \sum_{j=1}^{k} x_{nj}\beta_j \end{pmatrix} = \begin{pmatrix} y_1 - \beta_0 - \sum_{j=1}^{k} x_{1j}\beta_j \\ y_2 - \beta_0 - \sum_{j=1}^{k} x_{2j}\beta_j \\ \ldots\ldots\ldots\ldots \\ y_n - \beta_0 - \sum_{j=1}^{k} x_{2j}\beta_j \end{pmatrix} \tag{3.16}$$

в $Q = (Y - X\beta)^T (Y - X\beta)$,

отримуємо скалярну суму квадратів

$$Q = \sum_{i=1}^{n} (y_i - \beta_0 - \sum_{j=1}^{k} x_{ij}\beta_j)^2$$

Умовою звернення отриманої суми в мінімум є система нормальних рівнянь:

$$\frac{\partial Q}{\partial \beta_j} = 0$$, (j=0,1,2,…,k).

В результаті диференціювання виходить:

$$2X^T (Y - X\beta) = 0$$.

При заміні вектору невідомих параметрів β на оцінки, отримані методом найменших квадратів, отримуємо такий вираз:

$$X^T Y = X^T Xb. \tag{3.17}$$

Далі помноживши обидві частини рівняння зліва на матрицю $(X^T X)^{-1}$, отримаємо:

$$(X^T X)^{-1} \cdot (X^T Y) = (X^T X)^{-1} \cdot (X^T X)b \tag{3.18}$$

Так як $(X^T X)^{-1}(X^T X) = E$, тоді $b = (X^T X)^{-1}(X^T Y)$.

Отримані оцінки вектора b не є зміщеними і ефективними.

Коваріаційна матриця вектора b має вигляд:

$$V(b) = \sigma^2 (X^T X)^{-1},$$

де σ^2 - залишкова дисперсія.

Елементи головної діагоналі цієї матриці представляють собою дисперсії вектора оцінок b. Інші елементи є значеннями коефіцієнтів коваріації:

$$\text{cov}(b_i b_j) = M(b_i - \beta_i)(b_j - \beta_j), \tag{3.19}$$

де $i = 1 \div n$, $j = 0 \div k$.

Таким чином, оцінка b_j - це лінійна функція від залежної змінної. Вона має нормальний розподіл з математичним очікуванням β_j і дисперсією:

$$D_{b_j} = \sigma^2 \,\&\, *[(X^T X)^{-1}]_{jj}. \tag{3.20}$$

Незмінна оцінка залишкової дисперсії визначається за формулою:

$$\hat{S}^2_{ост} = \frac{1}{n-k-1}(Y - Xb)^T (Y - Xb), \tag{3.21}$$

де *n* - обсяг вибіркової сукупності; k - число пояснюють змінних.

Для перевірки значимості рівняння регресії використовують *F*-критерій дисперсійного аналізу, заснованого на розкладанні загальної суми квадратів відхилень на складові частини:

$$Q_{общ} = Q_R + Q_{ост}, \text{ де } Q_R = (Xb)^T (Xb) = \sum_{i=1}^{n} \hat{y}_i^2 \tag{3.22}$$

сума квадратів відхилень (від нуля), обумовлена регресією:

$$Q_{ост} = (Y - Xb)^T (Y - Xb) = \sum_{i=1}^{n} e_i^2 \tag{3.23}$$

сума квадратів відхилень фактичних значень залежної змінної від розрахункових $\hat{y} = Xb$, тобто сума квадратів відхилень відносно площини регресії, обумовлене впливом випадкових і неврахованих в моделі факторів.

Для перевірки гіпотези $H_0 : \beta = 0$ використовується величина [8-9]:

$$F_H = \frac{\frac{1}{k+1} Q_R}{\frac{1}{n-k-1} Q_{ост}}, \tag{3.24},$$

яка має F-розподіл Фішера-Снедекора з числом ступенів свободи $\nu_1 = k+1$ и $\nu_2 = n-k-1$. якщо $F_H > F_{кр}$, то рівняння регресії значимо, тобто в рівнянні є хоча б один коефіцієнт регресії, відмінний від нуля.

У разі значущості рівняння регресії перевіряється значимість окремих коефіцієнтів регресії. Для перевірки нульової гіпотези $H_0 : \beta_j = 0$ використовується величина

$$F_H = \frac{b_j^2}{\hat{S}^2 [(X^T X)^{-1}]_{jj}} \tag{3.25},$$

яка має F-розподіл Фішера-Снедекора з числом ступенів свободи $\nu_1 = 1$ и $\nu_2 = n - k - 1$; $[(X^T X)^{-1}]_{jj}$ - відповідний елемент головної діагоналі ковариационной матриці.

Коефіцієнт регресії β_j вважається значущим, якщо $F_H > F_{кр}$. Для значущих коефіцієнтів регресії можна побудувати довірчі інтервали, використовуючи формулу

$$\beta_j \in \{b_j \pm t_\gamma \hat{S}[(X^T X)^{-1}]_{jj}\} \quad (3.26),$$

де t_γ знаходиться по таблиці розподілу Стьюдента для рівня значущості $\alpha = 1 - \gamma$ і числа ступенів свободи $\nu = n - k - 1$.

Проводити регресійний аналіз будемо за допомогою програми **Statistica 6.0** - система NeuroShell для статистичного аналізу даних, що включає широкий набір аналітичних процедур і методів: більше 10 000 різних типів графіків, описові і внутрішньогрупові статистики, розвідувальний аналіз даних, кореляції, швидкі основні статистики і блокові статистики, інтерактивний імовірнісний калькулятор, Т-критерії (та інші критерії групових відмінностей), таблиці частот, спряженості, прапорів і заголовків, аналіз багатовимірних відгуків, множинна регресія, непараметричні статистики, загальна модель дисперсійного, підгонка розподілів.

Результати, отримані з програми Statistica 6.0 в результаті розрахунку за вихідними даними з додатка 1:

Таблиця 3.3

Матриця парних коефіцієнтів кореляції

	X1	X2	X3	Y
X1	1,00000	0,01094	-0,01016	-0,268308
X2	0,01094	1,00000	0,00355	-0,180454
X3	-0,01016	0,00355	1,00000	0,663083
Y	-0,26831	-0,18045	0,66308	1,00000

У таблиці 3.3 переставлені такі умовні позначення:

- ✓ X1 -тип мережевої операційної системи (MS Windows 10 Server, Fedora Core 8 – (Linux));
- ✓ X2 - в bit (біт) - довжина ключа, встановленого для використовуваного протоколу шифрування (використана група протоколів AES-xxx-CBC, в назву якої замість xxx - довжини ключа використано значення 128, 256);
- ✓ X3 - кількість віддалених вузлів, що одночасно здійснюють обмін даними з сервером VIPNet VPN;
- ✓ Y - отримана функція відгуку.

Аналіз матриці (таблиця 3.3) парних коефіцієнтів кореляції показує, що результативний показник найбільш тісно пов'язаний з показником X3 - кількістю клієнтів, так як цей показник має найбільше значення.

Звідси можна зробити висновок, що найбільш значущим параметром в функції відгуку (3.11), отриманої раніше, є параметр X3, тобто саме кількість клієнтів більшою мірою вплинуло на функцію при її прорахунку пакетом NeuroShell.

ВИСНОВОК ДО РОЗДІЛУ 3

На підставі отриманих тестових результатів можна з упевненістю сказати, що для використання платформи VIPNET і для реалізації клієнт-серверної технології, пропонується використовувати її в зв'язці з сервером Windows 10 Server і СУБД MS SQLserver. Так як за результатами двох тестів ця ОС показала найкращу продуктивність і масштабованість, в умовах даної корпоративної мережі. Для використання сервера Fedora Core 8 і СУБД PostgreSQL для клієнт-серверної технологій VIPNET сервер потребує професійної налаштування, як самої операційної системи, так і СУБД PostgreSQL.

ВИСНОВКИ

В даній дипломній роботі проведено детальний діагностичний аналіз предметної області, завдяки розробці захищеного каналу сегмента корпоративної мережі підприємства.

Операційний процес був описаний з точки зору обміну корпоративною інформацією, що потребує використання захищених каналів. Відображено структуру захищеної АС.

Завдяки результатам дослідження функція зворотного зв'язку була створена для моделі та оцінки роботи мережі компанії з використанням захищеного каналу.

- ✓ Різні стандарти та дві різні операційні системи перевіряються для оцінки одного з найпопулярніших алгоритмів шифрування та їх продуктивності.
- ✓ Набір оптимальних конфігурацій було отримано для створення мережевого каналу компанії.

В результаті тесту можна зробити висновок, що більшість серверних операційних систем є ефективними для моделювання та використання.

В результаті дослідження було отримано найбільш економічне рішення для створення захищених каналів інформаційного обміну в корпоративній мережі підприємства.

Відповідно до результатів випробувань, можна зробити висновок, що більшість операційних систем серверного призначення підходять для розгортання клієнт-серверної архітектури на основі запропонованої технічної платформи VIPNET VPN.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. А.В. Соколов, В.Ф.Шаньгин. Защита информации в распределенных корпоративных сетях и системах. - М.: ДМК Пресс, 2012. - 656с.
2. W. Stallings Cryptography and Network Security: Principles and Practice (Second Edition). - Prentice Hall Upper Saddle River, New Jersey 07458 - 569 с.
3. Л.К. Бабенко, Е.А. Ищукова. Современные алгоритмы блочного шифрования и методы их анализа: учеб. пособие для студентов вузов, обучающихся по группе специальностей в обл. информ. безопасности - М.: Гелиос АРВ,2016. - 376с.
4. Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. Handbook of Applied Cryptography. - CRC Press, October 2019. ISBN 0-8493-8523-7
5. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. - М.: «Диалектика», 2014. - С. 432. - ISBN 0-471-22357-3
6. Бутов А.С., Гаскаров Д.В., Егоров А.Н., Крупенина Н.В. Транспортные системы: моделирование и управление. - СПб.: Судостроение, 2011, - 552 с.
7. Ананий В. Левитин Глава 3. Метод грубой силы: Задача о рюкзаке // Алгоритмы: введение в разработку и анализ = Introduction to The Design and Analysis of Aigorithms. - М.: «Вильямс», 2016. - С. 160-163. - ISBN 0-201-74395-7
8. Гаскаров Д.В., Шаповалов В.И. Малая выборка. - М.: Статистика, 1978. - 248 с.
9. А. Г. Ивахненко, Ю. П. Юрачковский Моделирование сложных систем по экспериментальным данным. - М.: «Радио и связь», 2017. -120с.
10. Барсуков В.С. Безопасность: технологии, средства, услуги. «КУДИЦ-ОБРАЗ», -М., 2017.
11. Волчинская Е.К. Защита персональных данных. Опыт правового регулирования. - М.: Галерея, 2015.
12. Петраков А.В. основы практической защиты информации. «Радио и связь», -М., 2015.
13. Петраков А.В., Лагутин В.С. Телеохрана. Уч. Пособие, 3-е изд., -М., 2014.

14. Торокин А.А. основы инженерно- технической информации. - М.: Издательство «Ось-89», 2018.

15. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический проект; Фонд «Мир», 2013.

16. Михеева. Проблема правовой защиты персональных данных. //http://www.kiev-security.org.ua.

17. Молчанов С. Необходимость защиты персональных данных в электронных источниках информации. //http://www.podolsk.biz.ru.

18. Приватность и права человека - 2012. Япония. http://www.hro.org/docs.

ДОДАТОК А

Таблиця А.1

Зведена таблиця значень параметрів, реальних і модельованих значень продуктивності захищеного каналу

N	win/lin	Key	кол	S<>C	модель	отклонение
1	1	128	1	45,9	49,6439	-3,7439
2	1	128	1	45,5	49,6439	-4,1439
3	1	128	1	43,61	49,6439	-6,0339
4	1	128	1	45,9	49,6439	-3,7439
5	1	128	1	36,6	49,6439	-13,0439
6	1	128	1	47,3	49,6439	-2,3439
7	1	128	1	46,1	49,6439	-3,5439
8	1	128	1	49	49,6439	-0,6439
9	1	128	1	39,9	49,6439	-9,7439
10	1	128	1	39,8	49,6439	-9,8439
11	1	128	1	46,3	49,6439	-3,3439
12	1	128	1	46,3	49,6439	-3,3439
13	1	128	1	28,65	49,6439	-20,9939
14	1	128	1	46,8	49,6439	-2,8439
15	1	128	1	46,7	49,6439	-2,9439
16	1	128	1	48,4	49,6439	-1,2439
17	1	128	1	45,3	49,6439	-4,3439
18	1	128	1	48,3	49,6439	-1,3439
19	1	128	1	41,8	49,6439	-7,8439
20	1	128	1	41,78	49,6439	-7,8639
21	1	128	1	45,6	49,6439	-4,0439
22	1	128	1	47,2	49,6439	-2,4439
23	1	128	1	38,4	49,6439	-11,2439
24	1	128	1	45,6	49,6439	-4,0439
25	1	128	1	45,7	49,6439	-3,9439
26	1	128	1	35,1	49,6439	-14,5439
27	1	128	1	44,7	49,6439	-4,9439
28	1	128	1	42,96	49,6439	-6,6839
29	1	128	1	47,9	49,6439	-1,7439
30	1	128	1	58,4	49,6439	8,756096
31	1	128	2	52,97	41,7632	11,20678
32	1	128	2	58,16	41,7632	16,39678
33	1	128	2	43,56	41,7632	1,796777
34	1	128	2	64,76	41,7632	22,99678
35	1	128	2	46,7	41,7632	4,936777
36	1	128	2	52,82	41,7632	11,05678
37	1	128	2	51	41,7632	9,236777
38	1	128	2	53,38	41,7632	11,61678
39	1	128	2	39,31	41,7632	-2,45322
40	1	128	2	68,37	41,7632	26,60678
41	1	128	2	60,22	41,7632	18,45678

42	1	128	2	41,37	41,7632	-0,39322
43	1	128	2	47,99	41,7632	6,226777
44	1	128	2	72,55	41,7632	30,78678
45	1	128	2	35,64	41,7632	-6,12322
46	1	128	2	64,5	41,7632	22,73678
47	1	128	2	45,27	41,7632	3,506777
48	1	128	2	53,62	41,7632	11,85678
49	1	128	2	48,11	41,7632	6,346777
50	1	128	2	55,01	41,7632	13,24678
51	1	128	2	49,91	41,7632	8,146777
52	1	128	2	52,16	41,7632	10,39678
53	1	128	2	47,96	41,7632	6,196777
54	1	128	2	58,45	41,7632	16,68678
55	1	128	2	57,04	41,7632	15,27678
56	1	128	2	40,86	41,7632	-0,90322
57	1	128	2	66,4	41,7632	24,63678
58	1	128	2	19,95	41,7632	-21,8132
59	1	128	2	58,79	41,7632	17,02678
60	1	128	2	50,44	41,7632	8,676777
61	1	128	2	47,91	41,7632	6,146777
62	1	128	2	55,3	41,7632	13,53678
63	1	128	3	63,35	63,0616	0,288395
64	1	128	3	53,02	63,0616	-10,0416
65	1	128	3	66,2	63,0616	3,138395
66	1	128	3	63,94	63,0616	0,878395
67	1	128	3	54,64	63,0616	-8,4216
68	1	128	3	58,3	63,0616	-4,7616
69	1	128	3	52,49	63,0616	-10,5716
70	1	128	3	59,34	63,0616	-3,7216
71	1	128	3	56,64	63,0616	-6,4216
72	1	128	3	60,56	63,0616	-2,5016
73	1	128	3	61,83	63,0616	-1,2316
74	1	128	3	60,64	63,0616	-2,4216
75	1	128	3	57,38	63,0616	-5,6816
76	1	128	3	58,93	63,0616	-4,1316
77	1	128	3	58,64	63,0616	-4,4216
78	1	128	3	58,34	63,0616	-4,7216
79	1	128	3	57,88	63,0616	-5,1816
80	1	128	3	61,35	63,0616	-1,7116
81	1	128	3	54,54	63,0616	-8,5216
82	1	128	3	62,11	63,0616	-0,9516
83	1	128	3	51,21	63,0616	-11,8516
84	1	128	3	61,91	63,0616	-1,1516
85	1	128	3	58,08	63,0616	-4,9816
86	1	128	3	56,44	63,0616	-6,6216
87	1	128	3	56,71	63,0616	-6,3516
88	1	128	3	61,43	63,0616	-1,6316

89	1	128	3	50,61	63,0616	-12,4516
90	1	128	3	51,49	63,0616	-11,5716
91	1	128	3	47,16	63,0616	-15,9016
92	1	128	3	56,01	63,0616	-7,0516
93	1	128	3	57,5	63,0616	-5,5616
94	1	256	1	44,1	39,2016	4,89837
95	1	256	1	45,6	39,2016	6,39837
96	1	256	1	42,74	39,2016	3,53837
97	1	256	1	42,25	39,2016	3,04837
98	1	256	1	40,26	39,2016	1,05837
99	1	256	1	42,59	39,2016	3,38837
100	1	256	1	41,33	39,2016	2,12837
101	1	256	1	45,5	39,2016	6,29837
102	1	256	1	42,15	39,2016	2,94837
103	1	256	1	57,8	39,2016	18,59837
104	1	256	1	38,5	39,2016	-0,70163
105	1	256	1	34,95	39,2016	-4,25163
106	1	256	1	52,7	39,2016	13,49837
107	1	256	1	43,2	39,2016	3,99837
108	1	256	1	57	39,2016	17,79837
109	1	256	1	36,6	39,2016	-2,60163
110	1	256	1	39,8	39,2016	0,59837
111	1	256	1	48,7	39,2016	9,49837
112	1	256	1	36,8	39,2016	-2,40163
113	1	256	1	41,28	39,2016	2,07837
114	1	256	1	51,4	39,2016	12,19837
115	1	256	1	46,9	39,2016	7,69837
116	1	256	1	36,4	39,2016	-2,80163
117	1	256	1	48,6	39,2016	9,39837
118	1	256	1	41,4	39,2016	2,19837
119	1	256	1	47,6	39,2016	8,39837
120	1	256	1	51	39,2016	11,79837
121	1	256	1	21,67	39,2016	-17,5316
122	1	256	2	21,93	29,2213	-7,29133
123	1	256	2	14,69	29,2213	-14,5313
124	1	256	2	15,26	29,2213	-13,9613
125	1	256	2	24,32	29,2213	-4,90133
126	1	256	2	23,47	29,2213	-5,75133
127	1	256	2	22,57	29,2213	-6,65133
128	1	256	2	18,3	29,2213	-10,9213
129	1	256	2	23,53	29,2213	-5,69133
130	1	256	2	17,89	29,2213	-11,3313
131	1	256	2	23,73	29,2213	-5,49133
132	1	256	2	18,48	29,2213	-10,7413
133	1	256	2	23,59	29,2213	-5,63133
134	1	256	2	17,04	29,2213	-12,1813
135	1	256	2	23,03	29,2213	-6,19133

136	1	256	2	15,51	29,2213	-13,7113
137	1	256	2	23,03	29,2213	-6,19133
138	1	256	2	19,32	29,2213	-9,90133
139	1	256	2	20,44	29,2213	-8,78133
140	1	256	2	22,8	29,2213	-6,42133
141	1	256	2	19,47	29,2213	-9,75133
142	1	256	2	20,12	29,2213	-9,10133
143	1	256	2	21,63	29,2213	-7,59133
144	1	256	2	22,81	29,2213	-6,41133
145	1	256	2	22,39	29,2213	-6,83133
146	1	256	2	22,54	29,2213	-6,68133
147	1	256	2	29	29,2213	-0,22133
148	1	256	2	23,78	29,2213	-5,44133
149	1	256	2	19,6	29,2213	-9,62133
150	1	256	2	21,7	29,2213	-7,52133
151	1	256	2	20,17	29,2213	-9,05133
152	1	256	2	22,95	29,2213	-6,27133
153	1	256	3	54,65	48,4201	6,229902
154	1	256	3	53,77	48,4201	5,349902
155	1	256	3	58,27	48,4201	9,849902
156	1	256	3	60,9	48,4201	12,4799
157	1	256	3	44,08	48,4201	-4,3401
158	1	256	3	61,9	48,4201	13,4799
159	1	256	3	54,95	48,4201	6,529902
160	1	256	3	55,09	48,4201	6,669902
161	1	256	3	57,26	48,4201	8,839902
162	1	256	3	63,91	48,4201	15,4899
163	1	256	3	58,1	48,4201	9,679902
164	1	256	3	60,1	48,4201	11,6799
165	1	256	3	48,3	48,4201	-0,1201
166	1	256	3	63,13	48,4201	14,7099
167	1	256	3	51,64	48,4201	3,219902
168	1	256	3	52,01	48,4201	3,589902
169	1	256	3	56,47	48,4201	8,049902
170	1	256	3	52,97	48,4201	4,549902
171	1	256	3	35,49	48,4201	-12,9301
172	1	256	3	49,86	48,4201	1,439902
173	1	256	3	34,91	48,4201	-13,5101
174	1	256	3	46,08	48,4201	-2,3401
175	1	256	3	23,66	48,4201	-24,7601
176	1	256	3	43,94	48,4201	-4,4801
177	1	256	3	56,39	48,4201	7,969902
178	1	256	3	53,41	48,4201	4,989902
179	1	256	3	54,28	48,4201	5,859902
180	1	256	3	64,32	48,4201	15,8999
181	1	256	3	63,09	48,4201	14,6699
182	1	256	3	45,31	48,4201	-3,1101

183	1	256	3	52,38	48,4201	3,959902
184	2	128	1	14,28	11,8886	2,391388
185	2	128	1	12,07	11,8886	0,181388
186	2	128	1	13,03	11,8886	1,141388
187	2	128	1	13,86	11,8886	1,971388
188	2	128	1	12,88	11,8886	0,991388
189	2	128	1	10,89	11,8886	-0,99861
190	2	128	1	12,78	11,8886	0,891388
191	2	128	1	10,55	11,8886	-1,33861
192	2	128	1	12,29	11,8886	0,401388
193	2	128	1	12,36	11,8886	0,471388
194	2	128	1	13,28	11,8886	1,391388
195	2	128	1	13,21	11,8886	1,321388
196	2	128	1	13,18	11,8886	1,291388
197	2	128	1	13,1	11,8886	1,211388
198	2	128	1	13,04	11,8886	1,151388
199	2	128	1	13,25	11,8886	1,361388
200	2	128	1	13,08	11,8886	1,191388
201	2	128	1	13,3	11,8886	1,411388
202	2	128	1	12,91	11,8886	1,021388
203	2	128	1	12,26	11,8886	0,371388
204	2	128	1	13,31	11,8886	1,421388
205	2	128	1	12,67	11,8886	0,781388
206	2	128	1	10,06	11,8886	-1,82861
207	2	128	1	13,47	11,8886	1,581388
208	2	128	1	13,35	11,8886	1,461388
209	2	128	1	13,43	11,8886	1,541388
210	2	128	1	13,2	11,8886	1,311388
211	2	128	1	13,3	11,8886	1,411388
212	2	128	1	12,59	11,8886	0,701388
213	2	128	1	13,03	11,8886	1,141388
214	2	128	2	24,44	25,1202	-0,68019
215	2	128	2	17,34	25,1202	-7,78019
216	2	128	2	21,8	25,1202	-3,32019
217	2	128	2	22,54	25,1202	-2,58019
218	2	128	2	25,64	25,1202	0,51981
219	2	128	2	22,15	25,1202	-2,97019
220	2	128	2	23,63	25,1202	-1,49019
221	2	128	2	23,8	25,1202	-1,32019
222	2	128	2	23,62	25,1202	-1,50019
223	2	128	2	23,05	25,1202	-2,07019
224	2	128	2	23,15	25,1202	-1,97019
225	2	128	2	24,09	25,1202	-1,03019
226	2	128	2	24,09	25,1202	-1,03019
227	2	128	2	23,61	25,1202	-1,51019
228	2	128	2	24,14	25,1202	-0,98019
229	2	128	2	23,18	25,1202	-1,94019

230	2	128	2	23,75	25,1202	-1,37019
231	2	128	2	24	25,1202	-1,12019
232	2	128	2	22,28	25,1202	-2,84019
233	2	128	2	23,2	25,1202	-1,92019
234	2	128	2	20,69	25,1202	-4,43019
235	2	128	2	23,23	25,1202	-1,89019
236	2	128	2	23,49	25,1202	-1,63019
237	2	128	2	24,62	25,1202	-0,50019
238	2	128	2	21,5	25,1202	-3,62019
239	2	128	2	22,69	25,1202	-2,43019
240	2	128	2	22,65	25,1202	-2,47019
241	2	128	2	23,42	25,1202	-1,70019
242	2	128	2	24,97	25,1202	-0,15019
243	2	128	2	21,5	25,1202	-3,62019
244	2	128	2	23,34	25,1202	-1,78019
245	2	128	3	87,41	67,5308	19,87917
246	2	128	3	51,96	67,5308	-15,5708
247	2	128	3	81,94	67,5308	14,40917
248	2	128	3	54,67	67,5308	-12,8608
249	2	128	3	67,29	67,5308	-0,24083
250	2	128	3	70,88	67,5308	3,34917
251	2	128	3	66,82	67,5308	-0,71083
252	2	128	3	77,51	67,5308	9,97917
253	2	128	3	54,45	67,5308	-13,0808
254	2	128	3	77,75	67,5308	10,21917
255	2	128	3	72,57	67,5308	5,03917
256	2	128	3	60,88	67,5308	-6,65083
257	2	128	3	68,96	67,5308	1,42917
258	2	128	3	71,15	67,5308	3,61917
259	2	128	3	68,63	67,5308	1,09917
260	2	128	3	72,16	67,5308	4,62917
261	2	128	3	65,13	67,5308	-2,40083
262	2	128	3	72,89	67,5308	5,35917
263	2	128	3	84,21	67,5308	16,67917
264	2	128	3	67,28	67,5308	-0,25083
265	2	128	3	56,79	67,5308	-10,7408
266	2	128	3	81,74	67,5308	14,20917
267	2	128	3	61,22	67,5308	-6,31083
268	2	128	3	74,17	67,5308	6,63917
269	2	128	3	61,93	67,5308	-5,60083
270	2	128	3	66,75	67,5308	-0,78083
271	2	128	3	69,12	67,5308	1,58917
272	2	128	3	65,49	67,5308	-2,04083
273	2	128	3	67,15	67,5308	-0,38083
274	2	128	3	64,86	67,5308	-2,67083
275	2	128	3	65,47	67,5308	-2,06083
276	2	256	1	11,41	12,309	-0,899

277	2	256	1	8,84	12,309	-3,469
278	2	256	1	6,54	12,309	-5,769
279	2	256	1	11,5	12,309	-0,809
280	2	256	1	12,29	12,309	-0,019
281	2	256	1	13,7	12,309	1,391004
282	2	256	1	11,72	12,309	-0,589
283	2	256	1	14,1	12,309	1,791004
284	2	256	1	13,89	12,309	1,581004
285	2	256	1	13,26	12,309	0,951004
286	2	256	1	12,68	12,309	0,371004
287	2	256	1	12,66	12,309	0,351004
288	2	256	1	12,96	12,309	0,651004
289	2	256	1	13,25	12,309	0,941004
290	2	256	1	13,45	12,309	1,141004
291	2	256	1	13,46	12,309	1,151004
292	2	256	1	13,35	12,309	1,041004
293	2	256	1	13,31	12,309	1,001004
294	2	256	1	13,45	12,309	1,141004
295	2	256	1	12,61	12,309	0,301004
296	2	256	1	13,43	12,309	1,121004
297	2	256	1	13,01	12,309	0,701004
298	2	256	1	13,01	12,309	0,701004
299	2	256	1	12,7	12,309	0,391004
300	2	256	1	13,38	12,309	1,071004
301	2	256	1	11,8	12,309	-0,509
302	2	256	1	12,83	12,309	0,521004
303	2	256	1	13,37	12,309	1,061004
304	2	256	1	13,24	12,309	0,931004
305	2	256	1	13,11	12,309	0,801004
306	2	256	1	12,56	12,309	0,251004
307	2	256	2	19,72	23,441	-3,72096
308	2	256	2	21,24	23,441	-2,20096
309	2	256	2	23,57	23,441	0,129042
310	2	256	2	22,7	23,441	-0,74096
311	2	256	2	23,19	23,441	-0,25096
312	2	256	2	22,44	23,441	-1,00096
313	2	256	2	23,39	23,441	-0,05096
314	2	256	2	21,88	23,441	-1,56096
315	2	256	2	24,12	23,441	0,679042
316	2	256	2	24,33	23,441	0,889042
317	2	256	2	23,17	23,441	-0,27096
318	2	256	2	24,26	23,441	0,819042
319	2	256	2	23,77	23,441	0,329042
320	2	256	2	24,34	23,441	0,899042
321	2	256	2	23,9	23,441	0,459042
322	2	256	2	23,23	23,441	-0,21096
323	2	256	2	23,61	23,441	0,169042

324	2	256	2	22,79	23,441	-0,65096
325	2	256	2	23,68	23,441	0,239042
326	2	256	2	23,22	23,441	-0,22096
327	2	256	2	22,88	23,441	-0,56096
328	2	256	2	23,49	23,441	0,049042
329	2	256	2	22,79	23,441	-0,65096
330	2	256	2	23,17	23,441	-0,27096
331	2	256	2	24,17	23,441	0,729042
332	2	256	2	22,68	23,441	-0,76096
333	2	256	2	23,2	23,441	-0,24096
334	2	256	2	21,85	23,441	-1,59096
335	2	256	2	23,93	23,441	0,489042
336	2	256	2	22,79	23,441	-0,65096
337	2	256	2	23,01	23,441	-0,43096
338	2	256	3	62,99	63,752	-0,76198
339	2	256	3	60,88	63,752	-2,87198
340	2	256	3	68,03	63,752	4,278017
341	2	256	3	67,32	63,752	3,568017
342	2	256	3	64	63,752	0,248017
343	2	256	3	64,11	63,752	0,358017
344	2	256	3	64,38	63,752	0,628017
345	2	256	3	65,83	63,752	2,078017
346	2	256	3	64,3	63,752	0,548017
347	2	256	3	60,76	63,752	-2,99198
348	2	256	3	61,63	63,752	-2,12198
349	2	256	3	65,58	63,752	1,828017
350	2	256	3	66,63	63,752	2,878017
351	2	256	3	65,9	63,752	2,148017
352	2	256	3	66,7	63,752	2,948017
353	2	256	3	69,92	63,752	6,168017
354	2	256	3	64,79	63,752	1,038017
355	2	256	3	66,38	63,752	2,628017
356	2	256	3	62,09	63,752	-1,66198
357	2	256	3	63,66	63,752	-0,09198
358	2	256	3	61,29	63,752	-2,46198
359	2	256	3	63,13	63,752	-0,62198
360	2	256	3	66,26	63,752	2,508017
361	2	256	3	66,92	63,752	3,168017
362	2	256	3	62,97	63,752	-0,78198
363	2	256	3	59,47	63,752	-4,28198
364	2	256	3	66,19	63,752	2,438017
365	2	256	3	56,1	63,752	-7,65198
366	2	256	3	57,12	63,752	-6,63198
367	2	256	3	58,53	63,752	-5,22198
368	2	256	3	63,32	63,752	-0,43198

У додатку використані такі позначення:

- ✓ N - номер досвіду;
- ✓ Win / lin - серверна ОС (Windows 10 / Fedora core 8);
- ✓ Key - довжина ключа шифрування;
- ✓ К - кількість віддалених клієнтів;
- ✓ S <> C - сумарна пропускна здатність;
- ✓ Модель - прорахована пропускна здатність;
- ✓ Відхилення - різниця між S <> C і моделлю.