МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп’ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Кваліфікаційна робота бакалавра

на тему: Розробка проекту захищеної комп'ютерної мережі організації

Виконав студент групи _____
122 «Комп’ютерні науки»
Розенталь Аліна Євгенівна

Керівник д.т.н., професор
Казакова Надія Феліксівна

Консультант _____
_____

Рецензент к.т.н., _____
Домаскін О.М.

Одеса 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система

ЕОМ – електронно-обчислювальна машина

ЗІ – захист інформації

ІТС – інформаційно-телекомунікаційна система

КСЗІ – комплексна система захисту інформації

КС – комп’ютерна система

МД – матриця доступу

НСД – несанкціонований доступ

КМ – комп’ютерна мережа

ОС – операційна система

ПЗ – програмне забезпечення

СЗІ – система захисту інформації

DES – Data Encryption Standard

VPN – virtual private network

ВСТУП

У сучасному світі активно розвиваються мережні й інформаційні технології. В даний час неможливо знайти галузь, яка функціонує без впровадженої мережі передач даних. Подібна мережа дозволяє виконувати величезну кількість завдань, максимально спрощуючи різні дії. Застосування сучасних інформаційних технологій стало основною умовою виживання та ефективного керування усіма бізнес-процесами будь-якого підприємства.

У наш час інформація є дуже цінним ресурсом та фактором масового впливу. Як наслідок цих процесів виникає стрімке збільшення зловмисників, які намагаються отримати доступ до системи підприємства. Засоби масової інформації дуже часто повідомляють про кібератаки на різні підприємства. Щоб цього уникнути, потрібно дуже уважно підійти до питання модернізації мережі, особливо з боку безпеки. Все це вказує на високу актуальність даної дипломної роботи.

Сучасні розвинуті комп'ютерні мережі є складними інформаційно-обчислювальними системами з багаторівневими й неоднорідними архітектурами, а також, як правило, взаємодіють з іншими подібними системами. При їх використанні для вирішення задач обробки (в тому числі збирання, зберігання, передачі і т. д.) критичних даних (інформації, що вимагає захисту) виникає потреба у використанні спеціальних додаткових засобів, що виконують функції забезпечення постійного та адекватного технічного захисту інформації. Для забезпечення найбільшої ефективності захисту, а також для відповідності державним нормам з захисту інформації дані засоби мають бути передбачені і реалізовані в самій архітектурі подібної комп'ютерної інформаційно-обчислювальної системи.

На жаль, на сьогоднішньому етапі розвитку технологій не існує універсального і єдиного засобу захисту критичних даних у довільній мережі, а особливо у корпоративній мережі з розвинутою багаторівневою і

неоднорідною архітектурою. Більше того, у зв’язку із значною комерціалізацією даної сфери діяльності, часто пропонуються лише односторонні рішення конкретного розробника, який прагне отримати максимальний прибуток від використання саме його програмного рішення, відкидаючи при цьому елементарні поняття доцільності використання тих чи інших засобів захисту, а також їх корисність та ефективність з практичної точки зору. Для ліквідації такої ситуації в області захисту інформації був розроблений описаний нижче методологічний підхід до визначення потреб корпоративних комп’ютерних мереж щодо захисту інформації.

Основною задачею даної роботи є побудова підходу до визначення потреб у захисті інформаційної взаємодії від несанкціонованого доступу (НСД) у вибраній корпоративній комп’ютерній мережі, на етапі проектування мережі, та побудова на основі цих потреб інформаційної моделі комплексу засобів захисту, який необхідно реалізувати.

1. АНАЛІТИЧНИЙ ОГЛЯД І АНАЛІЗ КЛЮЧОВИХ ПРИНЦИПІВ БУДУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОГО ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1 Аналіз ключових засад інформаційної безпеки комп'ютерної мережі організації

1.1.1 Класифікація порушників інформаційної безпеки комп’ютерних мереж

Для подальшого коректного використання термінології, щодо захисту інформації та інформаційної безпеки, слід розглянути деякі питання нормативного регулювання у цій сфері.

Щоб коректно провести необхідну, відповідно до поставленого завдання, класифікацію порушників розглянемо поняття інформація із точкі зору того, як воно наведено у законодавстві України та у нормативних документах, які регулюють питання необхідного та достатнього рівня захисту в тому числі у комп‘ютерних системах та мережах.

Відповідно до Закону України «Про інформацію» [1]:

- інформація − будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
- захист інформації − сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Основним нормативно-правовим актом України щодо захисту інформації в комп'ютерній системі є Закон «Про захист інформації в інформаційно-комунікаційних системах» [2], який регулює відносини у сфері захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах (далі − система).

У цьому Законі наведені терміни вживаються в такому значенні:

- інформаційна (автоматизована) система − організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;
- телекомунікаційна система − сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;
- інформаційно-телекомунікаційна система − сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;
- захист інформації в системі − діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;
- комплексна система захисту інформації (КСЗІ) − взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

Згідно статті 5 Закону власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом. Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

З метою реалізації положень Закону 29 березня 2006 року Кабінетом Міністрів України постановою № 373 були затверджені «Правила забезпечення захисту інформації в ІТС» [3] (далі − Правила), які визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в ІТС.

У Правилах наведені нижче терміни вживаються у такому значенні:

- автентифікація − процедура встановлення належності користувачу інформації в системі (далі − користувач) пред'явленого ним ідентифікатора (пароль);
- ідентифікація − процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою (логін).

Згідно п.4 Правил захисту в системі підлягає:

- відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі − відкрита інформація);
- конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України «Про доступ до публічної інформації»;
- службова інформація;
- інформація, яка становить державну або іншу передбачену законом таємницю (далі − таємна інформація);
- інформація, вимога щодо захисту якої встановлена законом.

Згідно п.5 Правил відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Отож, питанням нормативного регулювання діяльності та вимог у сфері захисту інформації в тому числі і у комп‘ютерних системах та мережах, як показує проведений аналіз законодавства, присвячена велика кількість

нормативних актів, постанов, законів та нормативних документів Державної служби спеціального зв‘язку та захисту інформації [4]-[9].

Як видно з наведеного аналізу нормативних документів, питання захисту інформації в корпоративних мережах є не стільки питанням внутрішньо-корпоративної етики та забезпечення конфіденційності, цілісності, доступності та спостережуваної, як властивостей інформації що циркулює в системі, але й питанням дотримання вимог законодавства держави. Окремим питанням, яке не розглядалось у роботі, є також відповідальність за порушення законодавства в цій сфері.

Визначившись з основними поняттями, надалі слід перейти до визначення загроз та потенційних порушників, про захист від зловмисних дій яких буде йти мова далі у роботі.

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу комп’ютерної системи засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього [4]:

- **перший рівень** визначає найнижчий рівень можливостей проведення діалогу з КС − можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- **другий рівень** визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- **третій рівень** визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи та на склад і конфігурацію її устаткування;
- **четвертий рівень** визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних

компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник − це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

1.1.2 Класифікація загрозливих операцій з розподілених інформаційних ресурсів

Організація дій для захисту інформації (ЗІ) передбачає певні витрати фінансових та часових ресурсів, отже, необхідно перш за все мати уявлення про порядок цих витрат та адекватність їх до вартості інформації, яка може бути втрачена у разі реалізації атак порушників. Очевидно, що витрати на захист не повинні перевищувати можливих збитків при втраті інформації. Таким чином, необхідно ввести якусь міру цінності інформації, тобто визначити, в якому сенсі слід розуміти її цінність.

Властивостями інформації, що визначають її цінність є конфіденційність, цілісність, доступність і спостереженість [5], [7]. Конфіденційність визначається як властивість інформації, яка полягає в тому, що вона не може бути доступною для ознайомлення користувачам і процесам, які не мають на це відповідних повноважень.

- Цілісність інформації – це властивість, яка полягає в тому, що вона не може бути доступною для модифікації користувачам і процесам, які не мають на це відповідних повноважень. Цілісність інформації може бути фізичною або логічною.

- Доступність інформації – це властивість, що полягає в можливості її використання за вимогами користувача, який має відповідні повноваження.
- Спостереженість – це властивість інформації, яка полягає в тому, що процес її обробки має безперервно знаходитися під контролем органу, що керує захистом.

Під загрозами розуміються шляхи реалізації дій, що вважаються небезпечними. Наприклад, загроза зняття інформації та перехоплення випромінювання з дисплею веде до втрати конфіденційності, загроза пожежі веде до порушення цілісності та доступності інформації, загроза розриву каналу передачі інформації може реалізувати втрату доступності.

Загрози інформації розглядаються з точки зору їх будь-якої небажаної дії на будь-яку з цих властивостей і можливого їх порушення. З цієї точки зору в автоматизованих системах розрізняють наступні класи загроз інформації:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності або відмова в обслуговуванні;
- порушення спостереженості або керованості.

Таким чином, загроза – це потенційно можлива несприятлива дія, що призводить до порушень хоча б одної з наведених властивостей.

Аналіз загроз є одним з найбільш важливих питань при побудові захищених АС. Аналіз загроз має виявити можливі загрози інформації, а також показати, з якого боку і в якій точці АС слід чекати атаки. Загрози можуть реалізуватися внаслідок багатьох причин, серед яких:

- кількісна недостатність – фізична нестача компонентів АС для протидії можливим порушенням безпеки інформації;
- якісна недостатність – недосконаліть конструкції або організації компонентів АС, внаслідок чого не забезпечується протидія можливим порушенням безпеки інформації;

- відмови елементів АС – порушення працездатності елементів, яке призводить до неможливості виконання ними своїх функцій;
- збої елементів АС – тимчасове порушення працездатності елементів, яке призводить до неправильного виконання ними в деякий момент часу своїх функцій;
- помилки елементів АС – неправильне (одноразове або систематичне) виконання елементами своїх функцій внаслідок специфічного (постійного або тимчасового) їх стану;
- стихійні лиха – явища, що виникають випадково, не контролюються і призводять до фізичних зруйнувань;
- зловмисні дії – дії людей, що спеціально спрямовані на порушення безпеки інформації;
- побічні явища – супутні виконанню елементом АС своїх функцій.

Джерелами наведених причин порушення безпеки можуть бути:

- особи, що мають будь-яке відношення до функціонування АС;
- технічні засоби;
- моделі, алгоритми, програмне забезпечення (ПЗ);
- технологія функціонування – сукупність засобів, прийомів, правил, заходів і погоджень, що використовуються в процесі обробки інформації;
- зовнішнє середовище – сукупність елементів, що не входять до складу АС, але можуть впливати на захищеність інформації в АС.

1.1.3 Аналіз загальних положень політики інформаційної безпеки мереж

Політика безпеки інформації в комп'ютерній мережі (КМ) є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації [10].

Принципи політики безпеки. Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися засадами, які наведені далі.

Неможливість минати захисні засоби. Не повинно бути "таємних" модемних чи входів тестових ліній, що йдуть в обхід екрана.

Посилення самої слабкої ланки. Часто самою слабкою ланкою виявляється не комп'ютерна програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Неприпустимість переходу у відкритий стан. При будь-яких обставинах, СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Мінімізація привілеїв. Принцип мінімізації привілеїв радить виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Поділ обов'язків. Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес.

Багаторівневий захист. Принцип багаторівневого захисту радить не покладатися на один захисний рубіж, яким би надійним він ні здавався. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно затрудняє непомітне виконання злочинних дій.

Розмаїтість захисних засобів. Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі.

Простота і керованість інформаційної системи. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Забезпечення загальної підтримки заходів безпеки. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і практичне.

Види політики безпеки. Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи [11].

Для вивчення властивостей способу керування доступом створюється його формальний опис − математична модель. В даний час найкраще вивчені два види політики безпеки: вибіркова і повноважна, засновані, відповідно на вибірковому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Вибіркова політика безпеки. Основою вибіркової політики безпеки є вибіркове керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей вибіркового керування доступом застосовується модель системи на основі матриці доступу (МД), іноді її називають матрицею контролю доступу. Така модель одержала назву матричної.

Повноважна політика безпеки. Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

- усі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
- кожному об'єкту системи привласнена влучна критичності, що визначає цінність інформації, що міститься в ньому;
- кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадаючий потік інформації (наприклад, від рядових виконавців до керівництва). Ніж важливіше об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності [10].

Кожен суб'єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

1.2 Аналіз специфік концепції захисту комп'ютерних мереж на функціональних рівнях стека комунікаційних протоколів

1.2.1 Стек комунікаційних протоколів TCP/IP

Стек TCP/IP був розроблений з ініціативи Міністерства оборони США більше за 20 років для зв'язку експериментальної мережі ARPAnet з іншими мережами як набір загальних протоколів для різнорідної обчислювальної середи. Великий внесок в розвиток стека TCP/IP, який отримав свою назву по популярних протоколах IP і TCP, вніс університет Берклі, реалізовувавши протоколи стека в своєї версії ОС UNIX. Сьогодні цей стек використовується для зв'язку комп'ютерів всесвітньої інформаційної мережі Internet, а також у величезному числі корпоративних мереж.

Стек TCP/IP на нижньому рівні підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, для глобальних протоколи роботи на аналогових комутованих і виділених лініях SLIP, PPP, протоколи територіальних мереж X.25 і ISDN.

Сьогодні стек TCP/IP являє собою один з самих поширених стеків транспортних протоколів обчислювальних мереж. Дійсно, тільки в мережі

Internet об'єднано більше 10 мільйонів комп'ютерів по всьому світу, які взаємодіють один з одним за допомогою стека протоколів TCP/IP.

Хоч протоколи TCP/IP нерозривно пов'язані з Internet і кожний з багатомільйонної армади комп'ютерів Internet працює на основі цього стека, існує велика кількість локальних, корпоративних і територіальних мереж, що безпосередньо не є частинами Internet, в яких також використовують протоколи TCP/IP. Щоб відрізняти їх від Internet, ці мережі називають мережами TCP/IP або просто IP-мережами.

Оскільки стек TCP/IP спочатку створювався для глобальної мережі Internet, він має багато особливостей, що дають йому перевагу перед іншими протоколами, коли мова заходить про побудову мереж, що включають глобальні зв'язки. Зокрема, дуже корисною властивістю, що робить можливим застосування цього протоколу у великих мережах, є його здатність фрагментувати пакети. Дійсно, велика мережа часто складається з мереж, побудованих на абсолютно різних принципах. У кожній з цих мереж може бути встановлена власна величина максимальної довжини одиниці даних, що передаються (кадру). У такому випадку при переході з однієї мережі, що має велику максимальну довжину, в мережу з меншою максимальною довжиною може виникнути необхідність розподілу кадру, що передається на декілька частин. Протокол IP стека TCP/IP ефективно вирішує цю задачу.

Іншою особливістю технології TCP/IP є гнучка система адресації, що дозволяє більш просто в порівнянні з іншими протоколами аналогічного призначення включати в мережу мережі інших технологій. Ця властивість також сприяє застосуванню стека TCP/IP для побудови великих гетерогенних мереж.

У стеку TCP/IP дуже економно використовуються можливості широкомовних розсилок. Ця властивість необхідна при роботі на повільних каналах зв'язку, характерних для територіальних мереж.

Однак, як і завжди, за переваги, що отримуються треба платити, і платою тут виявляються високі вимоги до ресурсів і складність адміністрування IP-мереж. Могутні функціональні можливості протоколів стека TCP/IP вимагають для своєї реалізації високих обчислювальних витрат. Гнучка система адресації і відмова від широкомовних розсилок приводять до наявності в IP-мережі різних централізованих служб типу DNS, DHCP і т. п. Кожна з цих служб направлена на полегшення адміністрування мережі, в тому числі і на полегшення конфігурування обладнання, але в той же час сама вимагає пильної уваги з боку адміністраторів.

Основними протоколами стека, що дали йому назву, є протоколи IP і TCP. Ці протоколи в термінології моделі OSI відносяться до мережевого і транспортного рівнів відповідно. IP забезпечує просування пакету по складовій мережі, а TCP гарантує надійність його доставки. Нижче наведено таблицю, де порівнюються функції протоколів стеку TCP/IP з рівнями моделі взаємодії відкритих систем OSI (табл. 1.1).

Таблиця 1.1 – Відповідність ієрархічних рівнів моделі OSI за стандартом 7498 ISO) та стеку протоколів TCP/IP

Рівні моделі OSI	**Рівні стеку TCP/IP**
Прикладний	Прикладний
Відображення	
Сеансовий	
Транспортний	Транспортний
Мережевий	Міжмережевий
Канальний	Міжмережевого інтерфейсу (канальний)
Фізичний	

У стеку TCP/IP виділяють чотири ієрархічні рівні, які функціонально відповідають семи рівням моделі OSI. Функції трьох верхніх рівнів моделі OSI об’єднані у одному прикладному рівні стеку TCP/IP та функції двох нижніх

рівнів моделі об’єднані у одному рівні мережевого інтерфейсу, який також називають канальним рівнем.

Схема взаємодії прикладних процесів з використанням протокольного стеку TCP/IP (рис. 1.1) практично не відрізняється від схеми взаємодії за стандартом 7498 ISO. Усі вимоги щодо сумісності протоколів, які виконують одні й ті самі функції, однакові у обох схемах. На прикладі обміну інформацією між об’єктами усіх рівнів протокольного стеку TCP/IP, ознайомимось далі зі загальними принципами побудови стеків телекомунікаційних протоколів комп’ютерних мереж.

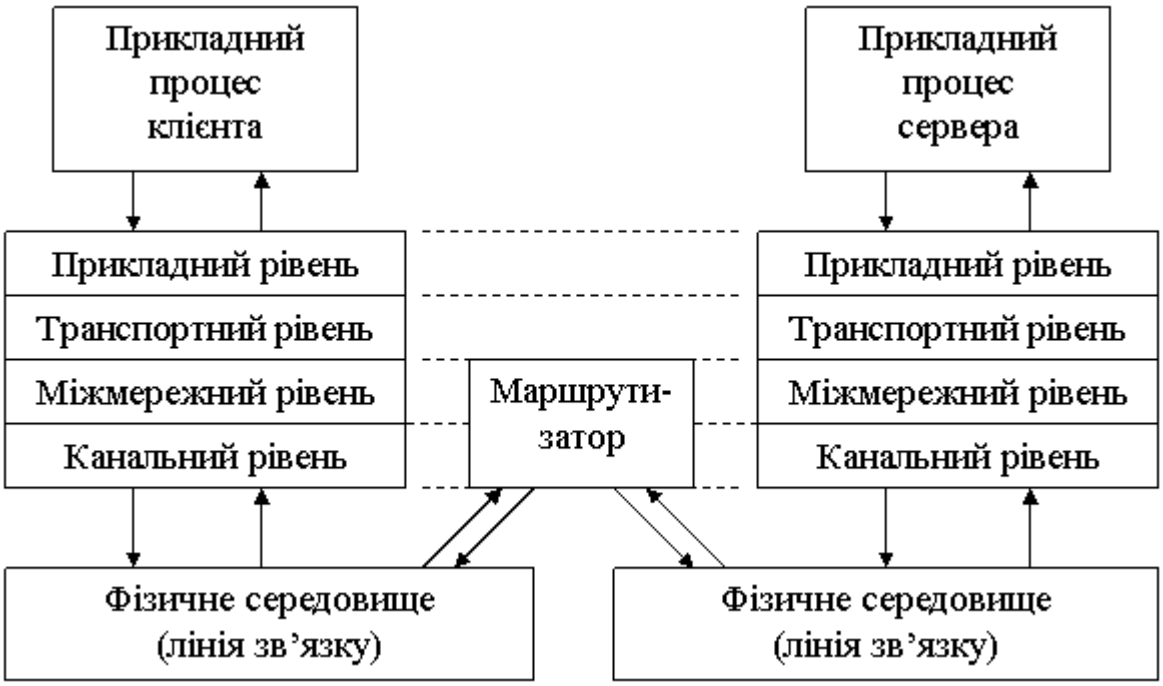

Рисунок 1.1 − Взаємодія прикладних процесів у мережі з використанням стеку протоколів TCP/IP

Розглянемо послідовність дій, що виконуються на кожному рівні протокольного стеку TCP/IP, у реальній остаточній системі під час передачі повідомлення (рис. 1.2). Прикладний процес є відправником інформації. Перед тим як потрапити у лінію зв’язку, повідомлення доповнюється заголовками від кожного ієрархічного рівня, а на канальному рівні доповнюється ще й кінцівкою. До лінії зв’язку повідомлення потрапляє у вигляді пакета або серії

пакетів канального рівня, що звуться кадрами (frame). Усі рівні, крім канального, реалізовані у вигляді програмного забезпечення. Канальний рівень потребує апаратних засобів для з'єднання з фізичною лінією зв'язку.

На прикладному рівні (application layer) існує декілька протоколів, що забезпечують доступ до мережі різноманітним процесам. У кожному з протоколів передбачено декілька варіантів повідомлень. Довжина повідомлень не обмежується. У деяких протоколах передбачена можливість перетворення даних. Після приєднання заголовка на прикладному рівні утворюється потік інформації, який передається на транспортний рівень.

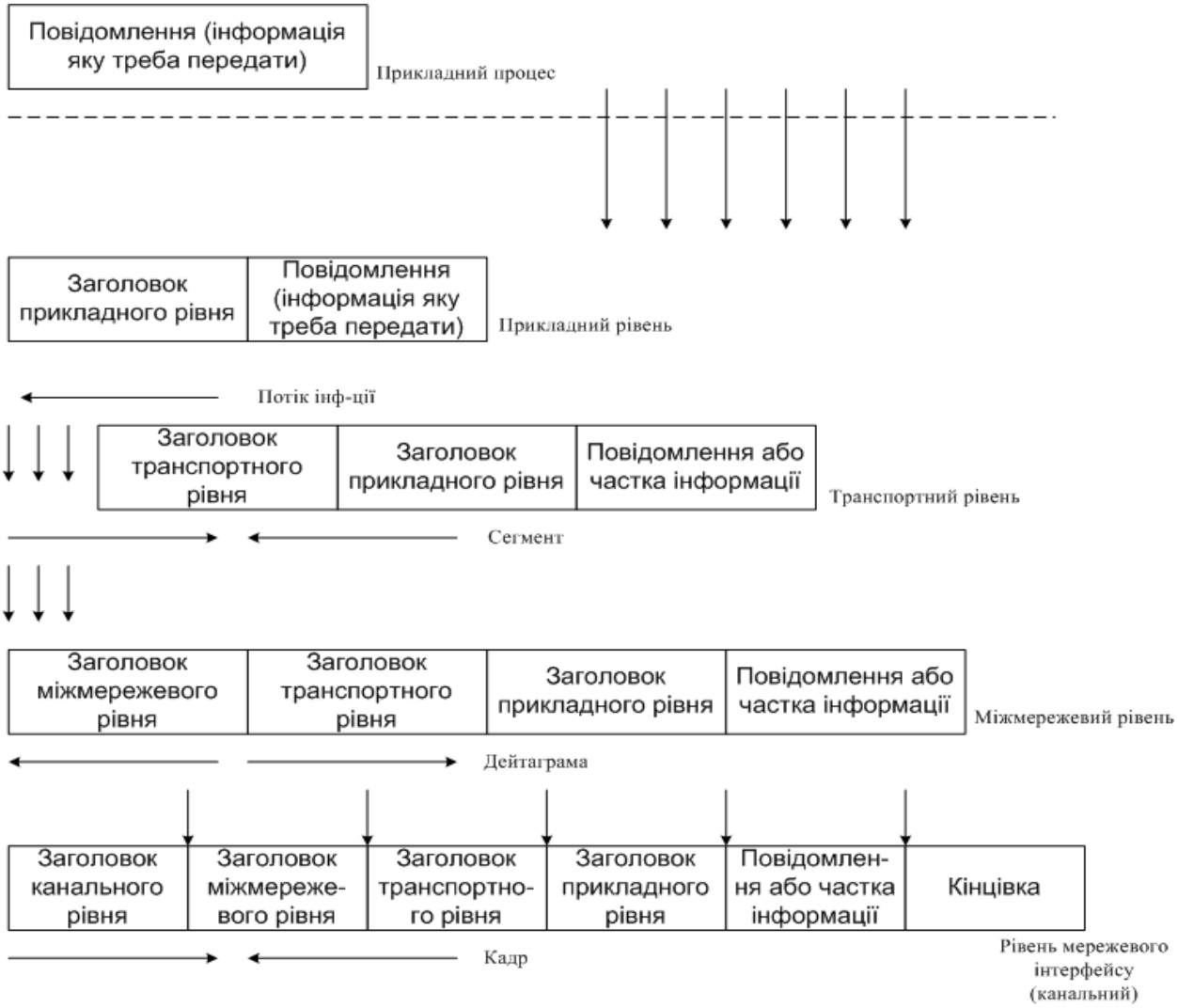

Рисунок 1.2 – Послідовність формування пакетів на ієрархічних рівнях стеку протоколів TCP/IP

На транспортному рівні (transport layer) існує два базових протоколи TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). Головний протокол цього рівня TCP. Він забезпечує керування процесом передавання даних. Спочатку виконується процедура встановлення з'єднання, яка полягає в обміні спеціальними інформаційними пакетами. Цей обмін здійснюється між об'єктами транспортного рівня систем відправника та одержувача інформації. Тільки після успішного обміну цими пакетами розпочинається процес передавання даних.

Далі потік інформації, що надходить з прикладного рівня, формується в інформаційні пакети. Довжина пакетів обмежена. Її максимальне значення задають під час інсталяції програмного забезпечення і вибирають в залежності від типу мережевого обладнання. Так, для мереж сім'ї Ethernet ця довжина становить 1500 байт. Коротенькі повідомлення можуть розміщуватись в одному пакеті, а довгий потік інформації буде поділено на частки максимально допустимої довжини.

Під час сеансу передавання даних між об'єктами транспортного рівня систем відправника та одержувача інформації існує зворотний зв'язок. Після успішного прийняття кожного пакета на транспортному рівні одержувача формується відповідь, яка передається на транспортний рівень відправника. Ця відповідь зветься квитанцією або підтвердженням. У разі затримки підтвердження той самий пакет може відправлятися повторно протягом встановленого інтервалу часу, після якого передавання даних буде припинено.

Після успішного завершення процесу передавання даних виконується процедура роз'єднання, яка нагадує процедуру з'єднання, бо також являє собою обмін спеціальними пакетами між об'єктами транспортного рівня систем відправника та одержувача інформації. Закінчення цієї процедури свідчить про те, що потік інформації безпомилково передано на прикладний рівень системи одержувача.

Протокол UDP призначений для термінової передачі коротких повідомлень без встановлення з'єднання та без підтверджень. При цьому пакет, що складається з повідомлення та заголовка UDP, називають так само, як пакет міжмережевого рівня дейтаграмою, а не сегментом, як пакети з TCP заголовком.

На міжмережевому рівні (internet layer) відбувається доставка пакетів між об'єктами транспортного рівня систем відправника та одержувача інформації. Головна функція, яка виконується на цьому рівні, полягає у виборі найкращого маршруту доставки пакетів. Кожен пакет проходить свій шлях незалежно від інших. При цьому гарантії, що пакет дійде до адресата, немає. Можливі порушення порядку надходження пакетів, а також розмноження їх. Головний протокол міжмережевого рівня зветься IP (Internet Protocol). Пакети, що формуються відповідно до цього протоколу, звуться дейтаграмами або данограмами. Вони складаються з пакетів транспортного рівня (сегментів) та заголовків міжмережевого рівня.

Крім протоколу IP, на міжмережевому рівні є протоколи, які забезпечують виконання операцій пошуку маршруту для доставки пакетів та знаходження адрес сусідніх маршрутизаторів.

На рівні мережевого інтерфейсу (network interface layer) відбувається доставка пакетів між об'єктами міжмережевого рівня, що належать одній мережі на фізичному рівні моделі OSI. Пакети цього рівня складаються з пакетів міжмережевого рівня, заголовків канального рівня та кінцівок у вигляді контрольної суми. У стеку протоколів TCP/IP, якщо перевірка контрольної суми кадру дає негативний результат, кадр відкидають.

Розподіл найбільш відомих протоколів стеку TCP/IP за ієрархічними рівнями показано на рис. 1.3. Призначення цих протоколів полягає у наступному.

HTTP (Hypertext Transfer Protocol) – протокол для передавання Web-сторінок (гіпертексту).

FTP (File Transfer Protocol) – протокол для передавання файлів.

SMTP (Simple Mail Transfer Protocol) – протокол для передавання повідомлень електронною поштою.

Telnet – протокол для емуляції термінала віддаленого комп'ютера.

DNS (Domain Name System) – доменна система імен, яка призначена для перетворення символьних імен мережевих ресурсів у цифрові адреси серверів, де розміщено ці ресурси.

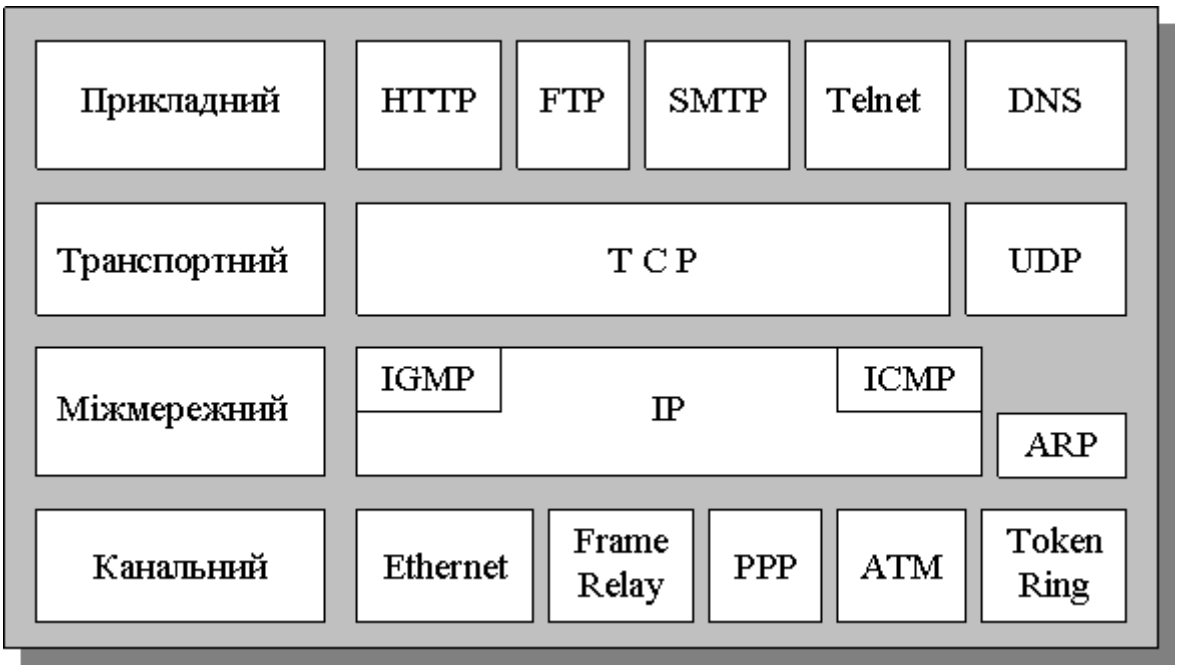

Рисунок 1.3 – Протоколи стеку TCP/IP

TCP (Transmission Control Protocol) – протокол, що забезпечує надійне логічне з'єднання тип "один до одного" та гарантує вірність передавання даних.

UDP (User Datagram Protocol) – протокол, що забезпечує можливість передавання широкомовних повідомлень без гарантії їх отримання споживачами інформації.

IP (Internet Protocol) – протокол, що забезпечує переміщення пакетів між мережами, але не гарантує доставку пакетів за адресою одержувача.

IGMP (Internet Group Management Protocol) – протокол, що забезпечує широкомовність для груп користувачів, які мають єдину групову адресу (multicast). Ця адресація призначена для економічного розповсюдження інформації у великих корпоративних мережах. Зараз такою технологією користуються в межах експерименту.

ICMP (Internet Control Message Protocol) – протокол для обміну службовою інформацією між маршрутизаторами (про виявлення помилок та аварійні ситуації), а також для перевірки працездатності мережі. Пакети IGMP та ICMP протоколів доповнюються IP-заголовком та циркулюють між об'єктами міжмережевого рівня, це пояснює їх особливе місце на рис. 1.6.

ARP (Address Resolution Protocol) – протокол для визначення фізичної адреси інтерфейсу. Ця адреса необхідна для формування заголовка пакета канального рівня (кадру). Пакети ARP протоколу не доповнюються IP-заголовком міжмережевого рівня, а одразу пакуються в кадри (пакети канального рівня), бо вони циркулюють тільки в межах однієї мережі.

Ethernet – найбільш розповсюджена технологія побудови каналів зв'язку у локальних мережах.

Frame Relay – технологія побудови каналів зв'язку для глобальних мереж.

PPP (Point-to-Point Protocol) – протокол, що широко застосовують для побудови каналу зв'язку між двома віддаленими вузлами, що з'єднані між собою фізичною лінією зв'язку.

ATM (Asynchronous Transfer Mode) –універсальна технологія побудови каналів зв'язку для глобальних і локальних мереж, що забезпечує гарантовану якість і терміновість передавання даних.

Важливою перевагою стеку TCP/IP є можливість утворення вузлів-маршрутизаторів, які одночасно приєднані до різних мереж. Це дозволяє переносити інформацію між мережами різного типу та створювати альтернативні шляхи доставки інформаційних пакетів. Якщо трапляється

аварія на одному з шляхів, пакет автоматично буде направлений на інший шлях. Отже, робота мережі не припиняється під час аварій на окремих вузлах, а також під час приєднання нових вузлів.

Можна приводити і інші доводи за і проти стека протоколів Internet, однак факт залишається фактом сьогодні це самий популярний стек протоколів, що широко використовується як в глобальних, так і локальних мережах.

1.2.2 Аналіз побудови захисту комп'ютерних мереж на різних рівнях стеку комунікаційних протоколів

Конструкція криптозахисних тунелів на канальному рівні

Віртуальні приватні мережі можуть гарантувати, що направляється через Internet трафік так само захищений, як і передачі усередині локальної мережі, при збереженні усіх фінансових переваг, які можна отримати, використовуючи Internet. [12], [13].

VPN-пристрій розташовується між внутрішньою мережею і Internet на кожному кінці з'єднання. Коли ви передаєте дані через VPN, вони зникають "з поверхні" в точці відправки і знову з'являються тільки в точці призначення. Цей процес прийнято називати " тунелюванням". Як можна здогадатися з назви, це означає створення логічного тунеля в мережі Internet, який сполучає дві крайні точки (рис. 1.4). Завдяки тунелюванню приватна інформація стає невидимою для інших користувачів Web. Перш ніж потрапити в Internet тунель, дані ще і шифруються, що забезпечує їх додатковий захист. Протоколи шифрування бувають різні. Все залежить від того, який протокол тунелювання підтримується тим або іншим VPN-рішенням. IPsec підтримує найширший спектр стандартів шифрування, включаючи DES (Data Encryption Standard) і Triple DES. Ще однією важливою характеристикою VPN-рішень є діапазон підтримуваних протоколів аутентифікації. Більшість популярних продуктів

працюють із стандартами, ґрунтованими на використанні відкритого ключа, такими як X.509. Це означає, що, посиливши свою віртуальну приватну мережу відповідним протоколом аутентифікації, ви зможете гарантувати, що доступ до ваших захищених тунелів отримають тільки відомі вам люди. Віртуальні приватні мережі часто використовуються у поєднанні з міжмережевими екранами. Адже VPN забезпечує захист корпоративних даних тільки під час їх руху по Internet і не може захистити внутрішню мережу від проникнення зловмисників.

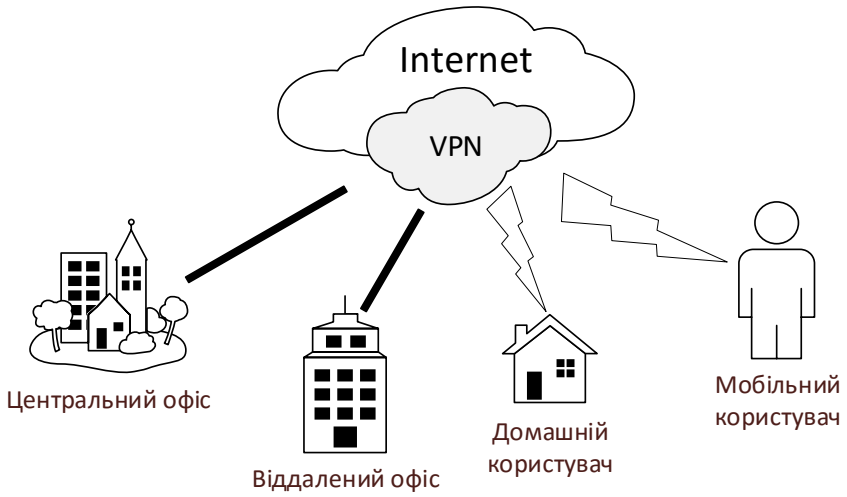

Рисунок 1.4 – Організація обміну даними через VPN

Технологія VPN застосовується там, де потрібно захист корпоративної мережі від дії вірусів, зловмисників, просто цікавих, а також від інших загроз, що є результатом помилок в конфігурації або адмініструванні мережі. Віртуальні приватні мережі (VPN) на базі безпровідної мережі − прекрасна альтернатива ізольованим корпоративним мережам.

Ця технологія має ряд безперечних переваг:

- низька вартість орендованих каналів і комунікаційного устаткування;
- широке географічне охоплення, можливість підключення у будь-якій точці;

- висока надійність;
- легкість в підключенні нових мереж або користувачів;
- легкість зміни конфігурації мережі;
- контроль подій і дій користувачів.

Ключова відмінна риса віртуальних приватних мереж (Virtual Private Networks, VPN) є те, що мережне середовище для них емулюється. В цій емуляції задіяні як мінімум 4 рівні певної мережі (фізичний, канальний, мережний та транспортний), яка виконує роль транспортної мережі.

Результатом емуляції є створення віртуального фізичного рівня певної мережі, зверху якого можна будувати звичну модель – канальний рівень, мережний. Процес емуляції віртуального мережного середовища на базі існуючої комунікаційної мережі має назву тунелювання. Віртуальні з'єднання, що утворюються, абстраговані від властивостей транспортної мережі. Ці з'єднання мають назву тунелів. Технологія, яка використовується для створення тунелів, полягає у транспортуванні пакетів віртуальної мережі у якості даних в складі пакетів, та має назву „інкапсуляція".

В технологіях тунелювання визначають три аспекти:

- пасажирський протокол (Passenger Protocol) – протокол, яким користуються для взаємодії через тунель кінцеві пристрої. Приклад – IP, IPX, NetBEUI.
- протокол інкапсуляції (Encapsulation Protocol) – який регламентує процес інкапсуляції
- протокол носія (Carrier protocol) – протокол, який використовується транспортною мережею.

Віртуальна мережа є суто логічною побудовою і не залежить від географічного розташування пристроїв, що взаємодіють, та конкретних фізичних з'єднань.

У типовому випадку VPN будується зверху публічної мережі, у якості якої часто виступає Інтернет. За цих обставин актуальним є захист інформації,

що передається, від несанкціонованого доступу та модифікації на шляху передачі. Для вирішення цієї задачі VPN як правило будуються з використанням криптування даних, що передаються.

Таким чином технологія VPN базується на тунелюванні та криптуванні.

Оскільки VPN абстраговані від реалізації транспортної мережі, вони можуть бути побудовані, як мережах з виділеними з'єднаннями, так і в мережах з комутацією пакетів або каналів. VPN можуть бути реалізовані як постійні з'єднання, так і використовувати динамічне створення з'єднань за запитом. В останньому випадку існує додаткова можливість для підвищення безпеки – аутентифікація та авторизація ініціатора створення VPN-з'єднання.

У VPN-з'єднанні беруть участь маршрутизатори, які створюють тунель між собою, та спрямовують в нього пакети, якими обмінюються пристрої, що взаємодіють. В частковому випадку маршрутизатор та кінцевий пристрій можуть бути реалізовані у вигляді одного фізичного пристрою.

Тунелювання полягає в передачі пакетів даних в середині інших пакетів. Тунель є логічне з'єднання двох маршрутизаторів, які виконують інкапсуляцію на вході до тунелю та декапсуляцію на його виході. В той час, коли вихідний пакет у своєму заголовку несе адреси пристроїв, що взаємодіють, в заголовку пакета, що мандрує через тунель, присутні адреси маршрутизаторів, які є кінцями тунелю.

Існують два типи тунелювання відповідно до того, якому рівню моделі OSI відповідає мережа, що утворюється:

- тунелювання на рівні 2
- тунелювання на рівні 3

Найбільш часто в VPN використовуються технології, які забезпечують створення канального рівня віртуальної мережі. Прикладами тунелювання на рівні 2 є протоколи PPTP (Point-to-Point Tunneling Protocol), L2F (Layer 2 Forwarding) та L2TP (Layer 2 Tunneling Protocol). Об'єктами передачі є фрейми канального рівня [14].

Конструкція захисту мереж на мереженому рівні

Безпеку на мережевому рівні забезпечує протокол IPsec (IP security − безпечний протокол IP), що по суті є набором протоколів. Протокол Ipsec досить складний, різні його аспекти описують більше десятка документів RFC. Основні документи, що описують протокол IPsec, − це RFC 2401, в якому описується загальна архітектура протоколу IPsec, і RFC 2411, що містить огляд IPsec протоколів і перелік документів, що їх описують.

Конфіденційність на мережевому рівні можна забезпечити, якщо зашифровувати всі дані, що переносяться в IP-дейтаграмах. Тобто кожного разу, перш ніж відправити дейтаграму до мережі, хост повинен зашифровувати її поле даних. В принципі, шифрування може здійснюватися алгоритмом з симетричними ключами, алгоритмом з відкритим ключем або за допомогою ключа сеансу, про який сторони домовляються по алгоритму з відкритим ключем. Поле данних може бути TCP-сегментом, UDP-сегментом, ICMP-повідомленням тощо. Якби подібна мережева служба була реалізована, то всі дані, що пересилаються між хостамі, включаючи електронну пошту, web-сторінки, керуючі повідомлення (такі як ICMP та SNMP) були б приховані від всіх сторонніх. Таким чином, подібна служба забезпечила б певний рівень загального захисту Інтернет-трафіка, істотно підвищивши безпеку мереж [14].

Крім конфіденційності бажано, щоб мережа забезпечувала аутентифікацію джерела. Коли хост-одержувач приймає IP-дейтаграму з визначеною IP-адресою відправника, він повинен бути впевнений, що вказана адреса є істинною. Подібна служба могла б поставити заслін багатьом різновидам мережевих атак.

У набір протоколів IPsec входять два основні протоколи: протокол AH і протокол ESP. Коли хост-відправник посилає дейтаграму хосту-одержувачу, він використовує або протокол AH, або протокол ESP. Протокол AH забезпечує аутентифікацію джерела і цілісність даних, але не забезпечує

конфіденційності. Протокол ESP забезпечує аутентифікацію джерела, цілісність даних і конфіденційність. Цей протокол надає більше можливостей і, зрозуміло, є складнішим і вимагає великих зусиллі при обробці, ніж протокол AH.

У обох протоколах, перш ніж відправити безпечні дейтаграми від хоста-відправника хосту-одержувачу, відправник обмінюється “рукостисканнями” з мережевими хостами і створює логічне з'єднання мережевого рівня. Цей логічний канал називається безпечним з'єднанням (Security Association, SA). Таким чином, протокол IPsec перетворює мережевий рівень Інтернету, що традиційно функціонує без встановлення з'єднань, в рівень з логічними з'єднаннями. Логічне SA-з’єднання є сімплексним, тобто однонаправленим. Якщо обидва хоста хочуть пересилати один одному безпечні дейтаграми, то необхідно встановити два SA-з’єднання по одному в кожному напрямі. SA-з’єднання визначається трьома параметрами:

- ідентифікатором протоколу безпеки (AH або ESP);
- IP-адресою джерела сімплексного з'єднання;
- 32-розрядним ідентифікатором з'єднання, що називається індексом параметра безпеки (Security Parameter Index, SPI).

Отже, протокол AH забезпечує аутентифікацію хоста-джерела і цілісність даних, але не конфіденційність. Коли один хост-джерело хоче відправити одну або декілька дейтаграм певному одержувачу, він спочатку встановлює з одержувачем безпечне з'єднання (SA-з’єднання). Встановивши SA-з’єднання, джерело може посилати хосту-одержувачу безпечні дейтаграми. Кожна безпечна дейтаграма містить AH-заголовок, що включається між початковими даними IP-дейтаграми і IP-заголовком, як показано на рис. 1.5. Таким чином, поле AH розширює оригінальне поле даних, після чого розширене поле даних поміщається в стандартну IP-дейтаграму. При цьому в полі протоколу IP-заголовка поміщається значення 51. Одержавши цю IP-дейтаграму, хост-одержувач виявляє значення 51 в полі

протоколу IP-заголовка і тому обробляє дейтаграмму за протоколом AH. Проміжні маршрутизатори обробляють дейтаграми так само, як і завжди − вони переправляють їх далі відповідно до IP-адрес одержувачів.

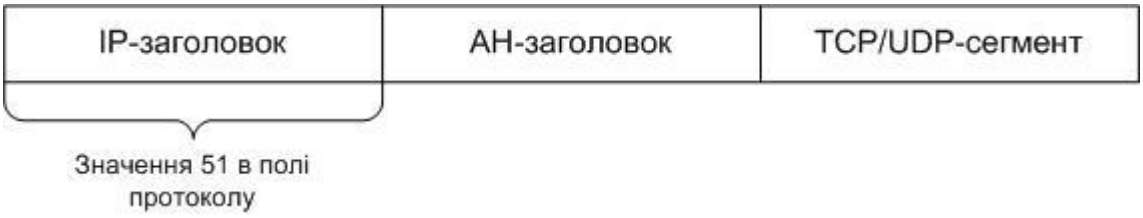

Рисунок 1.5 – Положення AH-заголовка в IP-дейтаграмі

AH-заголовок містить декілька полів.

Наступний заголовок. Це поле грає роль поля протоколу в звичайній дейтаграмі. Воно вказує, чи є наступне за AH-заголовком поле даних TCP-сегментом, UDP-сегментом, ICMP-сегментом тощо.

Індекс параметра безпеки (SPI). Це поле містить довільне значення, яке в комбінації з IP-адресою одержувача ідентифікує SA-з'єднання для даної дейтаграми.

Порядковий номер. 32-розрядне поле, що містить порядковий номер кожної дейтаграми. Спочатку (під час установки SA-з'єднання) це поле встановлюється рівним 0. Поле порядкового номера використовується протоколом AH для віддзеркалення атак повторного відтворення і атак з людиною посередині

Дані аутентифікації. Це поле змінної довжини містить підписаний дайджест повідомлення (тобто цифровий підпис) для даної дейтаграми. Дайджест повідомлення обчислюється по оригінальній IP-дейтаграмі. Таким чином забезпечується аутентифікація хоста-відправника і цілісність IP-дейтаграми. Цифровий підпис обчислюється за допомогою алгоритму, визначеного при установці SA-з'єднання (наприклад, MD5 або SHA).

Одержавши IP-дейтаграмму з AH-заголовком, хост-одержувач визначає для даної дейтаграми SA-з'єднання, а потім, обробивши поле даних аутентіфікації, переконується в цілісності дейтаграми. У процедурі аутентифікації протоколу IPsec (як для протоколу AH, так і для протоколу ESP) використовується схема обчислення зашифрованого дайджеста повідомлення, звана HMAC (RFC 2104). У схемі HMAC для аутентифікації повідомлення застосовується загальний секретний ключ, а не шифрування з відкритим ключем.

Протокол ESP забезпечує конфіденційність на мережевому рівні, а також аутентифікацію хоста-відправника і цілісність даних. Робота протоколу також починається з установки SA-з'єднання з хостом-одержувачем. Потім хост-відправник може посилати хосту-одержувачу безпечні дейтаграми. Як видно безпечна дейтаграма створюється з оригінальної IP-дейтаграми додаванням до її поля даних заголовка і кінцівки. Для поля протоколу в IP-заголовку використовується значення 50. Одержавши IP-дейтаграму, хост-одержувач помічає, що в полі протоколу IP-заголовка міститься значення 50, тому він обробляє дейтаграму за допомогою протоколу ESP. Як показано на рис. 1.6, оригінальні дані IP-дейтаграммы зашифровуються разом з полем ESP-кінцівки. Конфіденційність забезпечується за допомогою алгоритму шифрування DES-CBC (RFC 2405). ESP-заголовок складається з 32-розрядного поля для індексу SPI і 32-розрядного поля для порядкового номера, роль яких аналогічна відповідним полям протоколу AH. Кінцівка включає поле наступного заголовка, що вирішує те ж саме завдання, що і відповідне поле протоколу AH. Оскільки поле наступного заголовка зашифровується разом з початковими даними, зловмисник не зможе визначити, який транспортний протокол використовується. Наступним за кінцівкою розташовується поле даних аутентифікації, що виконує ту саму функцію, що і аналогічне поле протоколу AH.

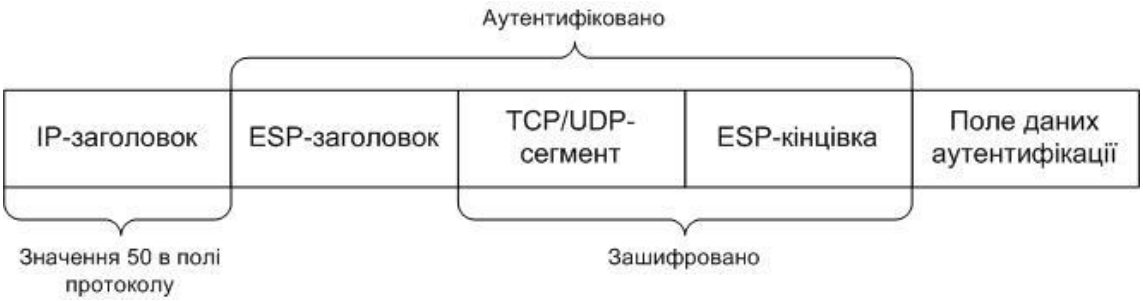

Рисунок 1.6 – Поля протоколу ESP в IP-дейтаграмі

Для успішного розгортання протоколу IPsec необхідні масштабовані і автоматизовані схеми управління ключем і встановлення SA-з'єднання. Для цього було визначено декілька протоколів:

- протокол IKE (Internet Key Exchange − обмін ключів по Інтернету) є протоколом управління ключами для IPsec за замовчанням;
- протокол ISKMP (Internet Security Association and Key Management − безпечне Інтернет-з'єднання та керування ключами) визначає процедури встановлення і розриву SA-з'єднань. Процедури встановлення і розриву SA-з'єднань протоколу ISKMP повністю відокремлені від процедур обміну ключами (IKE).

Конструкція захисту мереж на прикладному рівні

Питання забезпечення безпеки на прикладному рівні доцільно розглядати на прикладі електронної пошти. На початку необхідно визначити, які функції безпеки необхідні в першу чергу. Перш за все, потрібна конфіденційність. Адже ані відправник, ані одержувач, не хочуть, щоб зловмисник прочитав лист. Крім того, відправнику і одержувачу потрібна аутентифікація відправника. Зокрема, одержавши від відправника повідомлення одержувач, зрозуміло, хотів би упевнитися в тому, що це повідомлення прийшло від відправника, а не від зловмисника. Також потрібно забезпечити цілісність повідомлення, тобто потрібна упевненість в тому, що відправлене повідомлення не змінене по дорозі. Нарешті, електронна пошта

повинна забезпечувати аутентифікацію одержувача, тобто відправник хоче бути упевнений в тому, що він дійсно посилає лист одержувачу, а не кому-небудь ще, хто видає себе за нього.

Найбільш простий спосіб забезпечення конфіденційності полягає в шифруванні відправником повідомлень за допомогою алгоритму з симетричними ключами (наприклад, DES або AES). Отримавши лист, одержувач повинен спочатку розшифрувати його. Якщо довжина симетричного ключа достатньо велика і ключ відомий тільки відправнику і одержувачу, то кому-небудь ще прочитати зашифроване повідомлення буде вельми скрутно. Хоча такий метод досить простий, у нього є істотний недолік − важко передати ключ так, щоб його копії були тільки у відправника і одержувача. Але є альтернативний підхід, а саме алгоритм шифрування з відкритим ключем (наприклад, RSA). При шифруванні з відкритим ключем одержувач публікує свій відкритий ключ (наприклад, на сервері відкритих ключів або на своїй особистій web-сторінці), відправник зашифровує своє повідомлення відкритим ключем одержувача і посилає зашифроване повідомлення за адресою електронної пошти одержувача. Отримавши повідомлення, одержувач розшифровує його своїм особистим ключем. За умови упевненості відправника в тому, що використовуваний ним відкритий ключ дійсно належить одержувачу, а довжина цього ключа достатньо велика, подібний метод чудово забезпечує необхідну конфіденційність. Проте один з його недоліків полягає в тому, що шифрування з відкритим ключем відносно неефективне, особливо для довгих повідомлень.

Щоб вирішити проблему неефективності, використовується ключ сеансу. Зокрема, відправник, по-перше, випадковим чином вибирає симетричний ключ сеансу K_S, по-друге, зашифровує цим ключем сеансу K_S своє повідомлення m, по-третє, зашифровує ключ сеансу K_S відкритим ключем Одержувача K_B^+, по-четверте, формує зі всіх зашифрованих даних один пакет і, по-п'яте, посилає цей пакет за адресою електронної пошти одержувача. Ці

дії ілюструє рис. 1.7. (На цьому і на подальших малюнках плюс позначає операцію конкатенації, а мінус − протилежну операцію − тобто роз'єднання.) Одержавши повідомлення, одержувач, по-перше, за допомогою свого особистого ключа K_B^- отримує ключ сеансу K_S ,по-друге, за допомогою ключа сеансу K_S розшифровує повідомлення m.

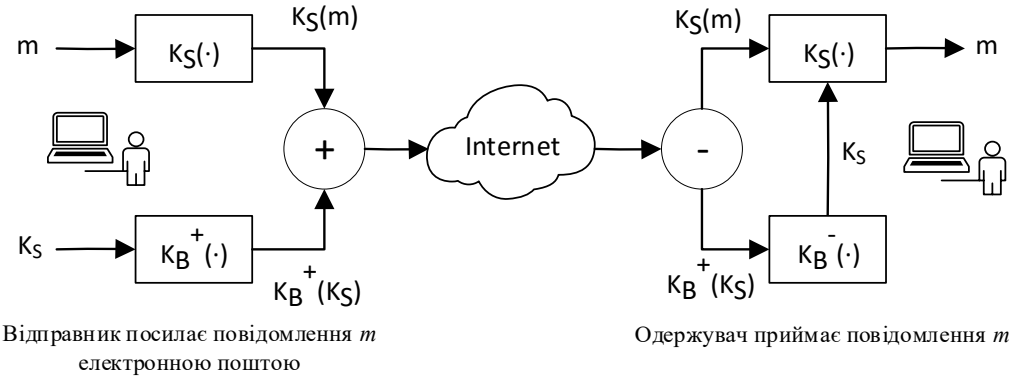

Рисунок 1.7 – Використання шифрування з ключем сеансу для забезпечення конфіденційності

Для вирішення питання аутентифікації та цілісності повідомлення доцільно користуватися цифровими підписами і дайджестами повідомлень. Отже, відправник, по-перше, застосовує до повідомлення т хеш-функцію Н (наприклад, MD5) і отримує дайджест повідомлення, по-друге, підписує результат хеш-функції своїм особистим ключем КА-, по-третє, об'єднує початкове (незашифроване) повідомлення з підписом, формуючи пакет, і, по-четверте, відправляє цей пакет за адресою електронної пошти одержувача. Отримавши повідомлення, одержувач, по-перше, застосовує відкритий ключ КА+ відправника до підпису дайджеста повідомлення і, по-друге, порівнює результат цієї операції з хешем повідомлення, який він обчислює сам. Ці дії ілюструє рис. 1.8.

Якщо результати цих двох обчислень співпадають, одержувач може бути впевнений, що повідомлення прийшло від відправника і воно не модифіковане.

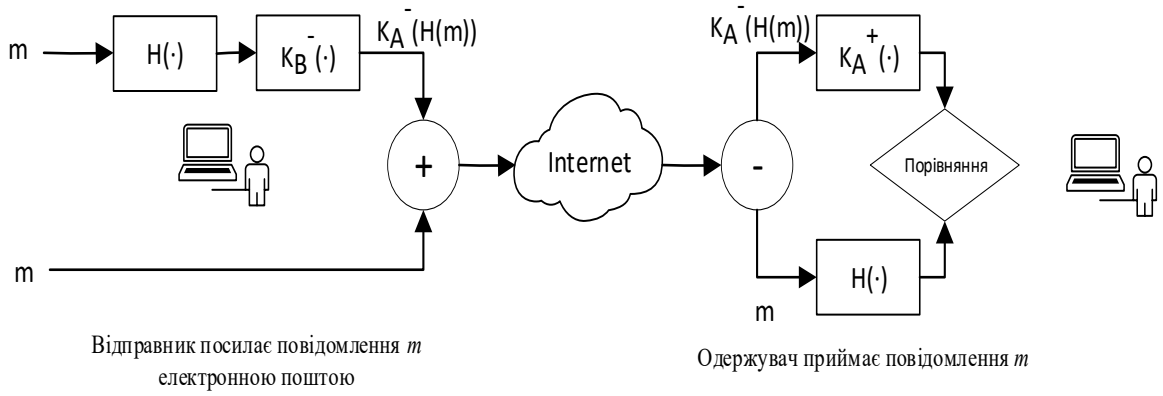

Рисунок 1.8 – Використання хеш-функції і цифрового підпису для аутентифікації і забезпечення цілісності повідомлення

Можна об'єднати в одній системі служби забезпечення конфіденційності, аутентифікації відправника і цілісності повідомлення. Спочатку відправник створює попередній пакет (рис. 1.7), що складається з початкового повідомлення і підписаного цифровим підписом хеша цього повідомлення. Потім весь попередній пакет зашифровується як єдине повідомлення (рис. 1.7), формується новий пакет, який і відправляється одержувачу. Отримавши пакет, одержувач спочатку застосовує до нього дії, показані на рис. 1.7, а потім дії, показані на рис. 1.8. Очевидно, що така схема забезпечує конфіденційність, аутентифікацію відправника і цілісність повідомлення. Потрібно звернути увагу, що відправник двічі використовує шифрування з відкритим ключем: один раз зі своїм особистим ключем і другий раз з відкритим ключем одержувача. Відповідно, одержувач також використовує шифрування з відкритим ключем двічі: один раз з своїм особистим ключем і другий раз з відкритим ключем відправника.

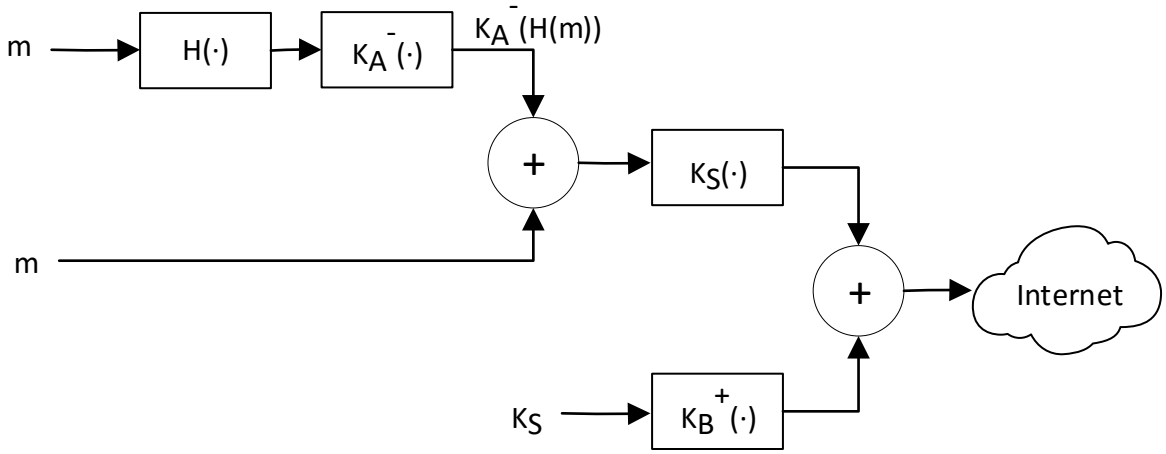

Рисунок 1.9 – Схема, що забезпечує конфіденційність, аутентифікацію і цілісність повідомлення

Показана на рис. 1.8 схема безпечної електронної пошти забезпечить достатній рівень безпеки для більшості користувачів.

2. ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Структура та корпоративна мережа організації

Відповідно до завдання на дипломне проектування базовим підприємством для дослідження і підвищення захищеності комп'ютерної мережі було визначено Одеський національний економічний університет.

Одеський національний економічний університет − один із провідних та найстаріших економічних вищих навчальних закладів України, який засновано у 1921 році з метою підготовки висококваліфікованих фахівців з економіки, проведення досліджень усього спектру економічних проблем [15].

Структурні підрозділи Одеського Національного Економічного Університету

Ректорат; Факультет Економіки і управління підприємництвом; Факультет Фінансів та банківської справи; Факультет Менеджменту, обліку та інформаційних технологій; Факультет Міжнародної економіки; Інформаційно-обчислювальний центр; Центр заочної та вечірньої форми навчання; Центр професійної освіти; Центр забезпечення якості освіти; Центр підвищення кваліфікації та сучасних освітніх технологій; Центр надання додаткових освітніх послуг; Кафедра Банківської справи; Кафедра Бухгалтерського обліку і аудиту; Кафедра Економіки, права та управління бізнесом; Кафедра Економіки підприємства та організації підприємницької діяльності; Кафедра Економічного аналізу; Кафедра Економічної кібернетики та інформаційних технологій; Кафедра Загальної економічної теорії та економічної політики; Кафедра Іноземних мов; Кафедра Маркетинга; Кафедра Математичних методів аналізу економіки; Кафедра Менеджменту; Кафедра Міжнародних економічних відносин; Кафедра Мовної та психолого-педагогічної підготовки; Кафедра Статистики; Кафедра Туристичного та

готельно-ресторанного бізнесу; Кафедра Управління персоналом і економіки праці; Кафедра Філософії, історії та політології; Кафедра Фізичного виховання та безпеки життєдіяльності; Кафедра Фінансів; Кафедра Фінансового менеджменту та фондового ринку; Приймальна комісія; Відділ міжнародних зв'язків; Науково-дослідна частина; Аспірантура; Рада молодих вчених; Науково-редакційний відділ; Бібліотека; Навчально-методичний відділ; Планово-фінансовий відділ; Бухгалтерія; Відділ кадрів; Відділ документального забезпечення (Канцелярія); Профспілкова організація співробітників; Профспілкова організація студентів; Навчально-методична лабораторія дистанційного навчання; Відділ маркетингу і зв'язків з роботодавцями; Відділ оперативної поліграфії; Відділ охорони праці; Архів; Гуртожиток 1; Гуртожиток 2; Гуртожиток 3; Спортивно-оздоровчий комплекс "ЕКОНОМІСТ" [15].

Структура та штатний розпис ЦІТ визначаються і затверджуються ректором за поданням начальника ЦІТ з урахуванням завдань, що поставлені перед ЦІТ.

Структура ЦІТ:

1. Апарат управління ЦІТ

- начальник ЦІТ - загальне керівництво у відповідності до посадової інструкиії;
- заступник начальника з експлуатаційних питань;
- заступник начальника з ТЗІ і ВЕБ питань.

2. Сектор експлуатації ЦІТ

- група експлуатації завдань;
- диспетчерська ЦІТ.

3. Сектор технічного обслуговування ЦІТ.
4. Лабораторія комунікаційних технологій ЦІТ.
5. Лабораторя АСУ ВНЗ.

2.2 Ключові завдання та обов'язки Інформаційно-обчислювального центру

ЦІТ є структурним підрозділом ОНЕУ, який забезпечує:

- Розвиток та функціонування технічної бази, інформаційної інфраструктури в навчальних аудиторіях і приміщеннях служб та структурних підрозділах ОНЕУ;
- Впровадження програмно-технічних засобів інформатизації навчального процесу та адміністративної діяльності ОНЕУ;
- Зв'язок ОНЕУ з регіональним та світовим інформаційними просторами;
- Телекомунікаційний та комп'ютерний зв'язок між структурними підрозділами ОНЕУ;
- Проведення науково-дослідних, та інших робот наукового спрямування в галузі нових інформаційних технологій;
- Режим збереження комп'ютерної техніки, техніки безпеки користувачів, протипожежної безпеки та ТЗІ ресурсів ОНЕУ.

Робота ЦІТ здійснюється відповідно до перспективного та річного планів концепції його розвитку. ЦІТ розробляє перспективні та річні плани, а також веде документацію, що відображає стан їх виконання та накопичує статичні данні про кількість і структуру звернень підрозділів [16].

До складу ЦІТ входять такі структурні підрозділи:

- Сектор експлуатації;
- Сектор технічного обслуговування;
- Лабораторія комунікаційних технологій;
- Лабораторія АСУ ВУЗ.

Метою ЦІТ є реалізація стратегії інформатизації ОНЕУ в частині забезпечення стійкого функціонування та розвитку його інформаційної

інфраструктури, а також розв’язання проблем інформатизації навчального процесу, наукових досліджень, адміністративного управління, формування та розвиток єдиного інформаційного простору та інтеграції його до світового інформаційного суспільства.

Завдання ЦІТ:

- Організація чіткого і безперервного забезпечення навчального процесу комп’ютерними ресурсами та прикладними програмами, мережними ресурсами, доступом до мережі Інтернету;
- Організація динамічної системи масового обслуговування для забезпечення обробки потоків вхідної, вихідної, внутрішньої інформації;
- Впровадження в експлуатацію програмного забезпечення навчального процесу;
- Підтримання у працездатному стані технічної бази;
- Виконання заяв усіх користувачів з питань технічних та системних розладів комп’ютерної техніки;
- Розробка перспективних планів в галузі засобів нових інформаційних технологій навчання;
- Підтримка проектів, в яких приймає участь ОНЕУ, що фінансуються різними благодійними та науковими фондами, виконання яких передбачує використання нових інформаційних технологій та мережі Інтернет;
- Консультація з виробу комп’ютерної, мультимедійної та іншої електронної техніки та програмного забезпечення для потреб структурних підрозділів ОНЕУ;
- Внесення пропозиції та розробка повнів технічного переобладнання або переоснащення, придбання та пристосування, а також визначення переліку необхідної техніки, її установка та програмно-технічний супровід, діагностування неіспрввностей та ремонт комп’ютерної та

іншої електронної техніки, програмного забезпечення для потреб структурних підрозділів ОНЕУ на підставі інших замовлень;

– Забезпечення режиму зберігання комп’ютерної техніки, електробезпеки, протипожежних заходів та ТЗІ ресусів.

Під час проведення дипломного проектування, в межах наданих повноважень, було розглянуто та досліджено архітектуру розподіленої комп‘ютерної мережі, а також, як окремий приклад для проектування було взято за основу мережу головний корпус вищого навчального закладу ОНЕУ, а саме – Факультет економіки і управління підприємництвом за адресою: вул. Преображенська, 8.

Однак, у зв‘язку з необхідністю нерозголошення конфіденційної інформації, надалі всі розрахунки, схеми та структури мереж будуть надані в «умовному вигляді», який в повній мірі відповідає структурі мережі що існує, але не наводить реальні характеристики обладнання та ін. Загалом мережа об’єднує 84 комп’ютери (50 в центральному офісі і 34 у філіях). Зв’язок з центральним офісом відбувається по виділеним каналам через SHDSL-модеми. Доступ до Інтернет через ADSL-модеми.

В свою чергу, мережа центрального офісу поділяється на декілька підмереж. У відділі зв’язку і телекомунікацій знаходиться сервер. Підмережа складається з 19-ти комп’ютерів (PC20-PC38) та має 3 світча (S1, S2 та S3). Також свої під мережі мають управління фінансового забезпечення та бухгалтерського обліку (PC39-PC44; S7), управління організаційно-аналітичного забезпечення та оперативного реагування (PC1-PC19; S4-S6) та відділ документального забезпечення (PC45-PC50; S8).

Інформаційні бази даних окремих підрозділів не мають спільних сегментів із базою даних центральної локальної мережі та функціонують в ізольованому режимі. В умовах, коли зростає число та об’єм бази даних, така адміністративна структура гальмує взаємний оперативний обмін інформацією між окремими філіями та центральною дирекцією. Тому було запропоновано

об’єднати локальні мережі окремих підрозділів організації в єдину корпоративну мережу, структура якої приведена на рис. 2.2. та рис. 2.3.

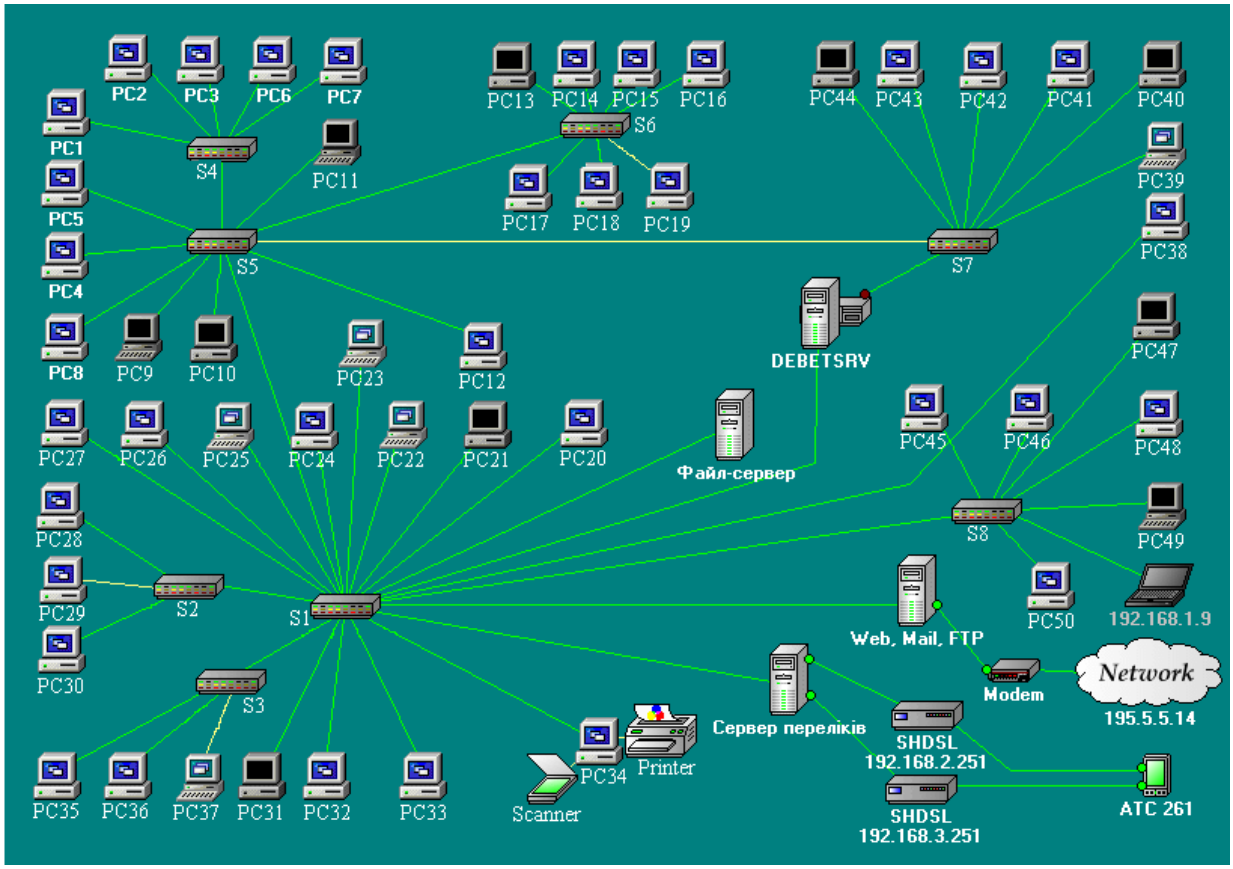

Рисунок 2.2 − Структура мережі центрального корпусу

Як видно з приведених рисунків, в даній корпоративній мережі для забезпечення зв’язку між окремими локальними мережами використовується об’єднана мережа INTERNET. Створення єдиного web-сайту та структури електронної пошти забезпечує віддалений доступ до обчислювальних ресурсів і бази даних та підвищити ефективність роботи. У зв’язку з тим, що в базах даних окремих підрозділів крім відкритої знаходиться службова та конфіденційна інформація, необхідно було розробити систему захисту цієї інформації від несанкціонованого доступу.

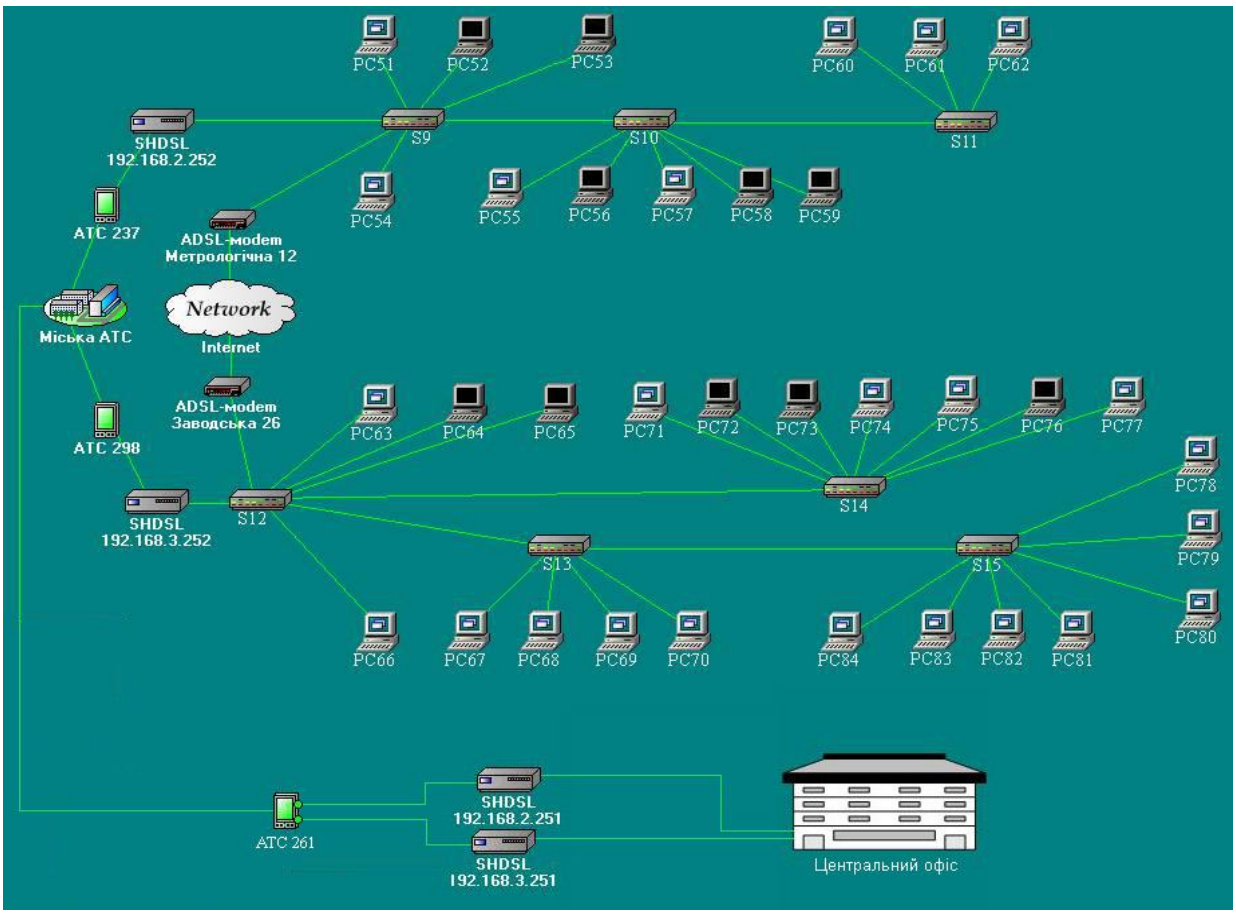

Рисунок 2.3 − Структура мережі іншого корпусу

Система захисту інформаційної взаємодії приведеної структури побудована на базі встановлення віртуальної приватної мережі. Технологія VPN ефективно використовує канальні ресурси і значно зменшує ризик зовнішнього втручання.

Захист віртуальних мереж найефективніше проводити на прикладному рівні стеку комунікаційних протоколів TCP/IP за допомогою протоколу SSL. Побудова VPN на основі протоколу SSL має такі переваги:

- підключення до мережі Internet через стандартний браузер відкриває доступ до ресурсів корпоративної мережі через Web-сторінку;
- забезпечується доступ до будь-якого пристрою, що підтримує роботу зі стандартним браузером.

- багато операційних систем, що підтримують роботу зі стандартним Web-браузером, можуть використовувати цей спосіб доступу у будь-яких операційних системах – Windows, Mac OS, UNIX і Linux;
- користувачі можуть одержати доступ до файлів на мережевих дисках;
- користувачі, що підключаються до корпоративної мережі через Web-браузер, не є робочими станціями корпоративної мережі, на відміну від VPN-клієнтів. Вони одержують доступ до ресурсів компанії через proxy-сервер. Отже, даний підхід більш безпечний, особливо стосовно віддалених користувачів.

Створення єдиного web-сайту та структури електронної пошти забезпечує віддалений доступ до обчислювальних ресурсів і бази даних та підвищити ефективність роботи. У зв'язку з тим, що в базах даних окремих підрозділів крім відкритої знаходиться службова та конфіденційна інформація, необхідно розробити систему захисту цієї інформації від несанкціонованого доступу.

На даний час технологія VPN використовує канальні ресурси й найбільше перспективна для захисту взаємодії між віддаленими локальними системами корпоративної мережі, зменшує ризик втручання [11]-[13].

2.3 Розробка VPN мережі

До складу спроектованої віртуальної мережі входять шлюзи кодування, програма контролю цілісності та модулі генерації й розподілу ключів, реєстрації та підготовки електронних ключів для мобільних клієнтів.

Шлюз є основним модулем VPN, що виконує функції маршрутизації, фільтрації й кодування пакетів. Кожен шлюз, призначений для захисту визначеної групи локальних мереж. На комп'ютері-шлюзі встановлюється модуль з функціями кодування й декодування та програма аутентифікації.

Функціями шлюзу є:

- фільтрація трафіка ;
- кодування трафіка;
- взаємодія з іншими шлюзами;
- реєстрація подій у центрі моніторингу;
- забезпечення власного захисту.

Модуль розподілу ключів здійснює керування периметром безпеки, а також виконує наступні функції:

- одержання зі змінного носія відкритих ключів шлюзів;
- розсилання шлюзам повідомлень про зміни структури мережі, що захищається;
- виготовлення й виконання процедури зміни сеансових ключів;
- збереження інформації про структуру мережі.

Модуль реалізований у вигляді програмного комплексу, що виконує функції збереження й видачі відкритих ключів кодування на мережевий запит від модулів кодування.

У функції модуля генерації ключів входить:

- генерація пар відкритого і секретного ключів, кодуючих модулів;
- генерація пари ключів для сертифікації відкритих ключів кодуючих модулів;
- генерація сертифікатів відкритих ключів, підписаних секретним ключем сертифікації;
- розміщення підписаних сертифікатів відкритих ключів на змінні носії;
- збереження еталонних копій сертифікованих відкритих ключів в архіві.

VPN містить у собі засоби формування й перевірки контрольних сум файлів. Ці засоби реалізовані у вигляді програми контролю цілісності, що

призначена для визначення і повідомлення адміністратора безпеки про зміну, додавання й видалення файлів.

Функції кодування міжмережевих інформаційних потоків виконуються відповідними протоколами VPN. Кожна мережа в складі VPN захищена своїм кодуючим модулем, встановленим у точці її з'єднання із зовнішніми мережами. Інформація, що захищається, кодується на передавальному модулі і декодується на приймальному, тобто передається у відкритому вигляді в межах локальних мереж і в кодованому за їхніми межами.

VPN дозволяє сформувати периметр безпеки, що поєднує IP-адреси всіх абонентів, що мають доступ у віртуальну захищену мережу. Абонентами VPN можуть бути цілі мережі, підмережі й окремі робочі станції.

Периметр безпеки формується для поділу трафіка на трафік, який кодується та який не кодується. Кодуючий модуль VPN робить виділення пакетів, які необхідно кодувати, на підставі IP-адрес відправника й одержувача пакета і, крім того, перевірку інтерфейсу, через який проходить пакет.

Кодування даних здійснюється на основі сеансових ключів, автоматично сформованих за допомогою довгострокових ключів, що мають обмежений час існування. VPN здійснює необхідні дії по керуванню ключами: генерацію й розподіл довгострокових ключів, вироблення сеансових ключів, сертифікацію відкритих ключів, планову й позаштатну зміну ключів кодування.

Протоколи VPN здійснюють збір і збереження статистичної й службової інформації про всі події, що виникають при аутентифікації вузлів, передачі кодованої інформації, обмеження доступу абонентів локальної обчислювальної мережі. Засоби моніторингу проводять збір і аналіз протоколів реєстрації від усіх модулів комплексу по кодованому каналу.

2.4 Локальна мережа головного корпусу

Локальна комп’ютерна мережа побудована на базі технології Fast Ethernet, яка забезпечує швидкість передачі даних 100 Мбіт/с. На фізичному рівні використовується специфікація 100 Base-TX, в якій використовується кабель UTP 5-ї категорії.

Локальна мережа працює під управлінням операційної системи Windows NT 2000 із використанням стеку телекомунікаційних протоколів TCP/IP і нараховує 50 комп’ютерів.

З прикладного програмного забезпечення в мережі використовується текстовий редактор Word, редактор електронних таблиць Excel, поштова програма Outlook та система управління базами даних Oracle.

У мережі входять відповідальні за доступ в Інтернет маршрутизатор, сервер VPN, сервер DNS, сервер SMTP, сервер FTP/http та міжмережевий екран.

Обов'язки вхідного маршрутизатора полягають у тому, щоб відокремити мережу Інтернет провайдера від мережі корпорації. Основна фільтрація трафіка відбувається саме на вході цього маршрутизатора. Він пропускає в мережу тільки дозволений TCP або UDP трафік від вузлів із допустимими IP-адресами. Це дозволяє виключити обробку трафіка з небажаних напрямків або від неавторизованих сервісів.

Основною функцією міжмережевого екрана (брандмауера) є фільтрація та аналіз установлених через нього TCP-сесій зв'язку. Міжмережевий екран може мати від одного до декількох сегментів – так званих "демілітаризованих зон" (DMZ), наприклад, для серверів, що відкриті для публічного доступу (Web, ftp), для підключення серверів VPN. У демілітаризованій зоні відбувається не тільки обмеження трафіку по IP-адресах і TCP-портах, але і по його напрямку. Так, web-сервер не генерує TCP запити самостійно, а тільки відповідає на запити клієнтів. Це запобігає можливості завантажити на зламаний web-сервер додаткові засоби атак і не дозволяє хакеру переключати в ході первинної атаки деякі сесії.

У загальній системі безпеки важливу роль відіграє сервер DNS, що повинен закрити хакеру доступ до вивчення мережі, що містить у собі заборону міжзональних пересилань (zone transfers) для будь-яких вузлів, крім авторизованих вторинних серверів DNS. Сервер SMTP повинен виконувати перевірку електронних повідомлень, що пересилаються користувачами, і відтинати віруси, що можуть надходити у внутрішню мережу. Міжмережевий екран повинен також фільтрувати SMTP-повідомлення, пропускаючи тільки необхідні команди для поштового сервера.

На внутрішній маршрутизатор покладаються функції поділу IP-адрес і маршрутизації між Інтернет-сегментом і корпоративною мережею. Даний пристрій працює винятково як маршрутизатор, не проводячи фільтрації вхідного трафіка. Цей маршрутизатор по суті є границею між внутрішньою мережею і зовнішнім середовищем.

Концентратор VPN забезпечує захищене підключення до корпоративної мережі віддалених користувачів. Перед тим як дозволити користувачеві підключення до мережі, концентратор VPN здійснює сесію зв'язку із сервером контролю доступу у внутрішній мережі, який за допомогою системи одноразових паролів проводить аутентифікацію користувача.

Після концентратора VPN доступу трафік надходить на міжмережевий екран.

Використовуються різні конфігурації включення міжмережевого екрану та VPN шлюзу, серед яких розглянемо наступні:

1. Шлюз VPN на брандмауері.

Перевага:

- є тільки одна точка, яка контролює процес інформаційної безпеки, це означає, що треба налаштовувати меншу кількість машин.

Недолік:

- неправильне налаштування брандмауера може дозволити Інтернет-потоку попасти в середину мережі, використовуючи адреси VPN.

2. Шлюз VPN попереду брандмауера.

Переваги:

- VPN трафік узагалі не проходить через брандмауер, тому не треба змінювати його конфігурацію для підтримки пакетів VPN;
- легка масштабованість мережі.

Недолік:

- VPN-сервер безпосередньо зв’язаний з Інтернетом.

3. Шлюз VPN позаду брандмауера.

Перевага:

- VPN повністю захищена від Інтернету брандмауером.

Недоліки:

- весь потік інформаційного обміну мережі VPN повинен проходити також і через брандмауер, що збільшує час затримки;
- брандмауер не може перевірити зашифрований потік.

У спроектованій мережі використаємо схему включення міжмережевого екрана попереду брандмауера, що здійснює блокування атак на брандмауері системою виявлення вторгнень.

Вибираємо для підмережі адресу з діапазону Intranet 192.168.16.0/24. Отже ми маємо IP-адреси починаючивід 192.168.16.0/24 і закінчуючи 192.168.16.138/24. Найперша серед них, яка закінчується на 0, є адресою мережі її не можна використовувати для ідентифікації мережевих вузлів. Остання адреса діапазону, яка закінчується на 138, є широкомовною адресою. Ця адреса також не може використовуватися для ідентифікації мережевих вузлів. Для ідентифікації інтерфейсу маршрутизатора, який пов'язує нашу мережу з Інтернетом, використовуємо адресу (192.168.16.1/24). Решту IP-адрес розділяємо між VPN комутатором (192.168.16.2/24), WWW і FTP сервером, які знаходяться на одному комп’ютері (192.168.16.3/24), E-mail сервером (192.168.16.5/24) та зовнішнім інтерфейсом брандмауера

(192.168.16.4/24). Інші IP-адреси присвоюємо робочим станціям мережі рис. 2.4.

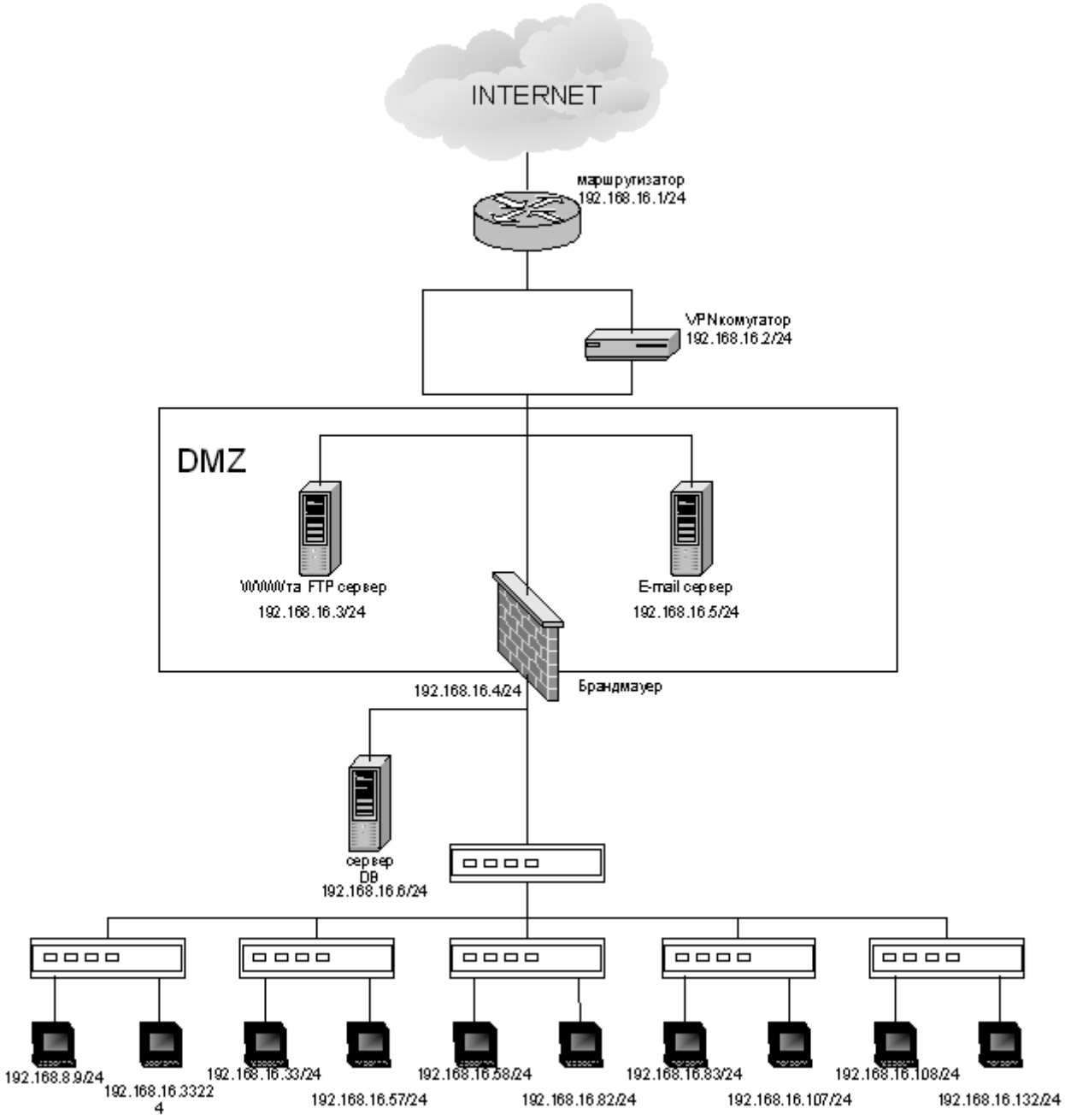

Рисунок 2.4 – Структура локальної мережі Головного корпусу

Мережу можна умовно розділити на три частини Інтернет – починається на дальньому від нас інтерфейсі маршрутизатора провайдера. На ближній до нас стороні маршрутизатора починається зона DMZ (Demilitarized Zone). Зона DMZ включає підконтрольні ресурси і є буфером, що відокремлює нашу

внутрішню мережу від Інтернету. Вона включає в себе: WWW сервер, FTP сервер та E-mail сервер. Зона DMZ закінчується зовнішнього інтерфейсу брандмауера. За внутрішнім інтерфейсом брандмауера починається внутрішня мережа.

2.5 Вибір політики безпеки корпоративної мережі

Будь-яке з'єднання між брандмауерами та відкритими мережами повинне використовувати механізм шифрованих віртуальних приватних мереж для забезпечення конфіденційності й цілісності даних, переданих по глобальних мережах. Також повинні бути створені відповідні засоби розподілу й адміністрування ключів шифрування перед початком експлуатації VPN.

VPN містить у собі засоби формування й перевірки контрольних сум файлів, призначених для визначення і повідомлення адміністратора безпеки про зміну, додавання й видалення файлів.

Кожна підмережа в складі VPN захищена своїм кодуючим модулем, встановленим у точці її з'єднання із зовнішніми мережами. Інформація, що захищається, кодується на передавальному модулі і декодується на приймальному, тобто передається у відкритому вигляді в межах локальних мереж і в кодованому за їхніми межами.

Необхідно сформувати периметр безпеки, що поєднує IP-адреси всіх абонентів, що мають доступ у віртуальну захищену мережу.

Протоколи VPN здійснюють збір і збереження статистичної й службової інформації про всі штатні й позаштатні події, що виникають при аутентифікації вузлів, передачі кодованої інформації, обмеження доступу абонентів локальної обчислювальної мережі. Засоби моніторингу проводять збір і аналіз протоколів реєстрації від усіх модулів комплексу по кодованому каналу.

Кожен відокремлений структурний підрозділ повинен мати по одній адресі електронної пошти, щоб не розкривати комерційної інформації.

Електронна пошта може бути отримана тільки через VPN-Інтранет.

POP-сервер розміщений у кожній локальній мережі філії, дає можливість мережам працювати незалежно, що зменшує кількість служб доступних ззовні.

Пошта, яка отримана SMTP-сервером, перевіряється на правомірність і направляється за допомогою VPN-шлюзу на відповідний POP-сервер.

Весь адміністративний доступ здійснюється через управляючі функції VPN.

2.6 Захист інформаційної взаємодії

Протокол SSL призначений для вирішення традиційних задач забезпечення захисту інформаційної взаємодії, що у середовищі клієнт/сервер інтерпретуються в такий спосіб:

- користувач, підключаючись до сервера, повинен бути впевнений, що він обмінюється інформацією не з підставним сервером, а саме з тим, який йому потрібний;
- після встановлення з'єднання між сервером і клієнтом весь інформаційний потік між ними повинен бути захищеним від несанкціонованого доступу;
- при обміні інформацією сторони повинні бути впевнені у відсутності випадкових або навмисних спотворень при її передачі.

Протокол SSL дозволяє серверу й клієнту перед початком інформаційної взаємодії автентифікувати один одного, погодити алгоритм шифрування і сформувати загальні криптографічні ключі. З цією метою протокол використовує криптосистеми з двома ключами, зокрема, RSA. Один ключ

використовується відправником для шифрування інформації, що повинна захищатись, іншим ключем одержувач розшифровує отриманий шифротекст.

Конфіденційність інформації, переданої по встановленому захищеному з'єднанню, забезпечується шляхом шифрування потоку даних на сформованому загальному ключі з використанням симетричних криптографічних алгоритмів, зокрема RC4, а контроль цілісності переданих блоків даних за рахунок використання так званих кодів автентифікації повідомлень, що обчислюються за допомогою хеш-функцій, зокрема, MD5.

Шифрування за алгоритмом RC4 виконується в режимі CFB (потоковий режим шифрування). Для генерації послідовності восьмирозрядних символів $\{k_i\}$ використовується таблиця станів шифратора S, що складається з 256 восьмирозрядних слів $\{S_1, S_2 \ldots S_{255}\}$. Початкове формування таблиці S виконується заданим ключем К в такий спосіб: елементи S ініціалізуються лінійно зростаючою послідовністю чисел S[0]=0, S[1]=1, S[2]=2, … . Ключ К розбивається на групи по 8 розрядів у кожній і розміщується в таблиці К довжиною 255 байт. При довжині ключа менш 255 байт виробляється циклічне заповнення таблиці К вихідною послідовністю символів ключа. Алгоритм володіє високої криптостійкістю. Число станів таблиці S складає приблизно 10^{1700}.

Протокол SSL містить у собі два етапи взаємодії сторін з'єднання:

- установлення SSL-сесії;
- захист потоку даних.

На етапі встановлення SSL-сесії здійснюється аутентифікація сервера й клієнта, сторони домовляються про криптографічні алгоритми, які будуть використовуватись, і формують загальний "секрет", на основі якого створюються загальні сеансові ключі для наступного захисту з'єднання. Цей етап називають також процедурою "рукостискання".

На другому етапі (захист потоку даних) інформаційні повідомлення прикладного рівня поділяються на блоки, для кожного з яких обчислюється

код аутентифікації повідомлень, потім дані шифруються й відправляються приймальній стороні. Приймальна сторона виконує зворотні дії: дешифрування, перевірку коду аутентифікації повідомлення, складання повідомлень, передачу на прикладний рівень.

Перевагою SSL є те, що він незалежний від прикладного протоколу. Протоколи, такі як HTTP, FTP, TELNET тощо можуть працювати поверх протоколу SSL зовсім прозоро. Протокол SSL може погоджувати алгоритм шифрування й ключ сесії, а також аутентифікувати сервер до того, як програма прийме або передасть перший байт даних. Усі протокольні прикладні дані передаються зашифрованими з гарантією конфіденційності.

Протокол SSL надає "безпечний канал", що має три основні властивості:

- канал є приватним (шифрування використовується для всіх повідомлень після простого діалогу, що служить для визначення секретного ключа);
- канал аутентифікований;
- канал надійний (транспортування повідомлень, містить у собі перевірку цілісності).

У SSL усі дані пересилаються у виді рекордів (записів), об’єктів, що складаються із заголовка й поля даних. Кожен заголовок рекорду містить два або три байти коду довжини. Якщо старший біт у першому байті коду довжини рекорду дорівнює 1, то рекорд не має заповнювача і повна довжина заголовка дорівнює 2 байтам, у протилежному випадку рекорд містить заповнювач і повна довжина заголовка дорівнює 3 байтам. Передача завжди починається із заголовка.

Довжина рекорда обчислюється наступним чином:

```
RECORD-LENGTH = ((byte[0] & 0x3F) << 8)) | byte[1];
IS-ESCAPE = (byte[0] & 0x40) != 0;
PADDING = byte[2];
```

Заголовок рекорда визначається значенням PADDING, що специфікує число байтів, доданих відправником до вихідного рекорда. Відправник

"заповненого" рекорду додає заповнювач після наявних даних, а потім шифрує все повідомлення. Уміст заповнювача немає значення, тому що обсяг переданих даних відомий, заголовок повідомлення може бути коректно сформований з урахуванням обсягу субполя PADDING. Одержувач цього рекорду дешифрує усі поля даних і одержує вихідну інформацію. Після цього виробляється обчислення дійсного значення RECORD-LENGTH, при цьому заповнювач із поля "дані" видаляється.

Частина даних рекорду SSL складається з трьох компонентів:

```
MAC-DATA[MAC-SIZE]
ACTUAL-DATA[N]
PADDING-DATA[PADDING]
```

ACTUAL-DATA – являє собою реальні передані дані

PADDING-DATA – це дані заповнювача, що посилаються коли використовується блоковий код шифрування.

MAC-DATA – є кодом аутентифікації повідомлення (Message Authentication Code).

Коли рекорди SSL посилаються відкритим текстом, не використовуються ніякі шифри. Отже, довжина PADDING-DATA буде дорівнювати нулеві й обсяг MAC-DATA також буде нульовим. При шифруванні, PADDING-DATA є функцією розміру блоку шифру. MAC-DATA залежить від CIPHER-CHOICE.

MAC-DATA обчислюється в такий спосіб:

```
MAC-DATA = HASH[ SECRET, ACTUAL-DATA, PADDING-DATA, SEQUENCE-
NUMBER ] ,
```

де SECRET передається хеш-функції першим, далі йде ACTUAL-DATA і PADDING-DATA , за якими передається SEQUENCE-NUMBER. Порядковий номер (SEQUENCE-NUMBER) являє собою 32-бітний код, що передається хеш-функції у вигляді 4 байт. Першим передається старший байт (тобто, використовується мережний порядок передачі − "big endian").

MAC-SIZE є функцією алгоритму, що використовується для обчислення дайджесту.

Значення SECRET залежить від того, хто з партнерів посилає повідомлення. Якщо повідомлення посилається клієнтом, тоді SECRET дорівнює CLIENT-WRITE-KEY (сервер буде використовувати SERVER-READ-KEY для верифікації MAC). Якщо клієнт одержує повідомлення, SECRET дорівнює CLIENT-READ-KEY (сервер буде використовувати SERVER-WRITE-KEY для генерації MAC).

SEQUENCE-NUMBER є лічильником, що інкрементується як відправником, так і одержувачем. Для кожного напрямку передачі, використовується пара лічильників (один для відправника, інший для одержувача). При відправленні повідомлення лічильник інкрементується**.** Порядковими номерами є беззнакові 32-бітні цілі числа, що при переповненні анулюються.

Одержувач повідомлення використовує очікуване значення порядкового номера для передачі хеш-функції MAC (тип хеш-функції визначається параметром CIPHER-CHOICE). Обчислена MAC-DATA повинна збігатися з переданою MAC-DATA. Якщо порівняння не пройшло, рекорд вважається пошкодженим, така ситуація розглядається як випадок "I/O Error".

Остаточна перевірка відповідності виконується, коли використовується блоковий шифр і відповідний протокол шифрування. Обсяг даних у рекорді (RECORD-LENGTH) повинен бути кратним розмірові блоку шифру. Якщо отриманий рекорд не кратний розмірові шифру, рекорд вважається пошкодженим, при цьому вважається, що мала місце помилка "I/O Error" (що викликала розрив з’єднання).

Рівень рекордів SSL використовується для всіх комунікацій SSL, включаючи повідомлення діалогу та інформаційний обмін. Рівень рекордів SSL застосовується як клієнтом, так і сервером.

Для двобайтового заголовка максимальна довжина рекорду дорівнює 32767 байтів. Для трибайтового заголовка максимальна довжина рекорду дорівнює 16383 байтів. Повідомлення протоколу діалогу SSL повинні відповідати одиночним рекордам протоколу SSL (Record Protocol). Повідомлення прикладного протоколу можуть займати кілька рекордів SSL.

Перш ніж послати перший рекорд SSL усі порядкові номери стають рівними нулеві. При передачі повідомлення порядковий номер інкрементується**,** починаючи з повідомлень CLIENT-HELLO і SERVER-HELLO.

Протокол діалогу SSL має дві основні фази. Перша фаза використовується для встановлення конфіденційного каналу комунікацій, друга – для аутентифікації клієнта.

Фаза 1

Перша фаза є фазою ініціалізації з'єднання, коли обидва партнери посилають повідомлення "HELLO". Клієнт ініціює діалог посилкою повідомлення CLIENT-HELLO. Сервер одержує це повідомлення, обробляє його і відгукується повідомленням SERVER-HELLO.

До цього моменту, як клієнт, так і сервер мають досить інформації, щоб знати, чи потрібний новий головний ключ. Якщо він не потрібний, клієнт і сервер негайно переходять у фазу 2.

Якщо потрібний новий головний ключ, повідомлення SERVER-HELLO буде містити досить даних, щоб клієнт міг сформувати такий ключ. Сюди входить підписаний сертифікат сервера, список базових шифрів і ідентифікатор з'єднання (останній являє собою випадкове число, сформоване сервером і використовуване протягом сесії). Клієнт генерує головний ключ і посилає повідомлення CLIENT-MASTER-KEY (або повідомлення ERROR, якщо інформація сервера вказує, що клієнт і сервер не можуть погодити базовий шифр).

Кожна закінчена точка SSL використовує пари шифрів для кожного з'єднання (тобто всього 4 шифри). На кожній кінцевій точці один шифр використовується для вихідних комунікацій і один − для вхідних. Коли клієнт або сервер генерує ключ сесії, вони в дійсності формують два ключі:

- SERVER-READ-KEY (відомий також як CLIENT-WRITE-KEY);
- SERVER-WRITE-KEY (відомий також як CLIENT-READ-KEY).

Головний ключ використовується клієнтом і сервером для генерації різних ключів сесій.

Після того як головний ключ визначений, сервер посилає клієнтові повідомлення SERVER-VERIFY. Цей заключний крок аутентифікує сервер, тому що тільки сервер, якій має відповідний загальнодоступний ключ, може знати головний ключ.

Фаза 2

Друга фаза є фазою аутентифікації. Сервер уже аутентифікований клієнтом на першій фазі, тому здійснюється аутентифікація клієнта. При типовому сценарії, серверові необхідно одержати щось від клієнта, і він надсилає запит. Клієнт надішле позитивний відгук, якщо має необхідну інформацію, або надішле повідомлення про помилку, якщо немає. Коли один партнер виконав аутентифікацію іншого партнера, він посилає повідомлення finished. У випадку клієнта повідомлення CLIENT-FINISHED містить зашифровану форму ідентифікатора CONNECTION-ID, що повинен верифікувати сервер. Якщо верифікація зазнає невдачі, сервер посилає повідомлення ERROR.

Якщо партнер послав повідомлення finished, він повинен продовжити сприймати повідомлення доти, доки не одержить повідомлення finished від партнера. Як тільки обидва партнери послали та одержали повідомлення finished, протокол діалогу SSL закінчив свою роботу. З цього моменту починає працювати прикладний протокол.

2.7 Налаштування VPN мережі

Оскільки VPN шлюзи працюють під управлінням операційної системи Linux, то налаштування будемо проводити за допомогою команд Linux:

1. Створення користувача, який буде запускати команди VPN на обох кінцях з'єднання.

Нехай ім'я користувача буде sslvpn.

```
root # groupadd sslvpn
root # useradd –m –d /opt ssl –vpn –c “SSL VPN User” –g sslvpn
sslvpn
```

Робочу станцію, яка починає процес з'єднання з віддаленим абонентом, назвемо VPN клієнтом, а віддаленого абонента – VPN сервером.

2. Створення ключів і сертифікатів.

Нам потрібно аутентифікація обох кінців SSL з'єднання, що гарантує легітимність цих кінцевих точок. Для цього потрібно створити ключі й сертифікати і для клієнта, і для сервера. VPN-сервер повинен вимагати сертифікат на обох кінцях. Будемо використовувати самопідписні сертифікати. Для генерації ключів використовується конфігураційний файл OpenSSL, який називається sslvpn.conf. Створені ключі й сертифікати потрібно розмістити в спеціальних каталогах Stunel. Щоб мати можливість створити декілька VPN із різними сертифікатами та ключами, для зберігання цих файлів створимо каталог з ім'ям /opt/ssl-vpn/etc/ім'я VPN/. Так як нам потрібно встановити декілька VPN з'єднань, то замість ім'я VPN буде vpn1,vpn2,vpn3 і т.д.

Створюємо й підписуємо ключ

На серверній машині:

```
vpn-server$ cd/opt/ssl-vpn/etc/vpn1
 vpn-server$ openssl reg -new -x509 -days 365 \
-config/opt/ssl-vpn/etc/sslvpn.cnf\
-out server.pem -keyout server.pem
```

На клієнтській машині:

```
client$ cd /opt/ssl-vpn/etc/vpn1
client$ openssl reg -new -x509 -days 365\
-config/opt/ssl-vpn/etc/sslvpn.cnf\
-out server.pem -keyout server.pem
```

Аргументи команди означають

reg -new -x509 – сертифікат діє напротязі 365 днів;

config – шлях до конфігураційного файлу OpenSSL;

out – файл для запису сертифіката;

keyout – файл для запису приватного ключа;

Таким чином наш ключ і сертифікат створені і мають відповідно вид server.pem і client.pem.

Тепер копіюємо сертифікат сервера на клієнтську машину (і навпаки) для використання в перевірці.

3. Налаштування таблиці маршрутизації.

```
sslvpn@client$ sudo route add -net 192.168.1.0/24 gw
123.45.67.82
sslvpn@server$ sudo route add -net 192.168.2.0/24 gw
125.51.67.82
```

4. Установлення скриптів vpn-server та vpn-client.

5. Створення конфігураційних файлів.

Програми vpn-server та vpn-client потрібні для встановлення будь-якого числа VPN з'єднань. Визначивши ім'я, VPN скрипт отримує з файлу /opt/ssl-vpn/etc/ім'я_vpn/config її конфігураційні змінні. Таким чином для нашої VPN з ім'ям vpn1 ми повинні створити файл /opt/ssl-vpn/etc/ vpn1/config. Кожна змінна в конфігураційному файлі починається з server_ або client_, що означає можливість створити один файл із усіма необхідними значеннями і використовувати його в обох системах.

Конфігураційний файл:

```
# /opt/ssl-vpn/etc/vpn1
client_network=192.168.2.0/24
server_network=192.168.1.0/24
client_debug="yes"
server_debug="yes"
```

Вибираємо IP-адреси для обох VPN

```
server_ppp_ip=125.51.67.82
client_ppp_ip=123.45.67.82
```

PPP аутентифікація

```
client_require_pap="no"
server_require_pap="no"
client_require_chap="yes"
server_require_chap="yes"
```

#Нестандартні аргументи pppd

```
#client_pppd_args="usepeerdns"
#server_pppd_args="proxyarp"
```

Опис змінних, які використовуються в конфігураційному файлі:

- client_network – мережа на VPN-клієнті. Використовується VPN-сервером для встановлення маршруту до віддаленої мережі за допомогою команди route add. Якщо значення не встановлено, клієнт вважається хостом, а не шлюзом і маршрути не встановлюються;
- server_network мережа на VPN-сервері. Використовується VPN-клієнтом для встановлення маршруту до віддаленої мережі за допомогою команди route add;
- server_ppp_ip – IP-адреса кінця PPP-з’єднання, на якому знаходиться VPN-сервер;
- client_ppp_ip – IP-адреса кінця PPP-з'єднання, на якому знаходиться VPN-клієнт;
- client_debug – додає опцію debug до аргументів pppd; додає опцію D7 до аргументів Stunnel і запускає set -x для покрокового виводу крипта vpn-client;
- server_debug – аналогічно попередньому, тільки для сервера;
- client_stunnel_args – додаткові аргументи Stunnel для клієнта;
- server_stunel_args – додаткові аргументи Stunnel для сервера;
- client_pppd_args – додаткові аргументи командної стрічки pppd, які специфічні для даної VPN;
- server_pppd_args – додаткові аргументи командної стрічки pppd, які специфічні для даної VPN;

- client_require_pap – VPN-клієнт буде вимагати PAP-аутентифікацію сервера. Усі значення, крім yes, еквівалентні no;
- server_require_pap – VPN-сервер буде вимагати PAP-аутентифікацію клієнта. Усі значення, крім yes, еквівалентні no.

6. Запуск і зупинка VPN.

Для запуску VPN виконуємо наступну команду на клієнтській машині:

```
server# /etc/init.d/vpn1 start
client# /etc/init.d/vpn1 start
```

Для зупинки VPN потрібно виконати команду

```
root# /etc/init.d/vpn1 stop
```

2.8 Вибір обладнання для VPN мережі

Використання пристроїв SSL VPN дозволяє знизити вартість розгортання й обслуговування віртуальних приватних мереж у порівнянні з традиційними рішеннями на основі IPSec.

При встановленні обладнання значну роль відіграє вибір фірми виробника.

Провідні позиції на ринку VPN займає фірма NetScreen, яка пропонує рішення на базі протоколу SSL.

В якості обладнання для Головного корпусу використовуємо продукт цієї фірми NetScreen-SA 1000, який буде головним VPN-концентратором, а для територіальних підрозділів − NetScreen-50.

Спеціалізовані мікросхеми GigaScreen прискорюють виконання задач програм політик безпеки, шифрування та аутентифікації на апаратному рівні. Такий підхід забезпечує найвищу швидкодію в порівнянні з підходом, заснованим на програмній реалізації даних задач на базі процесора загального

призначення. Пристрої NetScreen надають рішення по безпеці, що охоплюють широке коло користувачів – від високошвидкісних віддалених користувачів, до великих корпорацій, компаній електронного бізнесу й операторів зв'язку. Усі пристрої NetScreen засновані на технологіях stateful inspection, захисту від вторгнень і захисту від відмови в обслуговуванні.

Пристрої забезпечують:

- інтегровані рішення, що включають апаратне забезпечення, що оптимізоване для задач безпеки;
- стійке запобігання атакам, включаючи атаки типу SYN, UDP Floods, ICMP Floods, Ping-of-Death, а також розпізнавання спроб сканування портів, некоректного використання властивостей стандартних протоколів, перевірку компонентів, що завантажуються, Java/Active/ZIP/EXE;
- трансляцію адрес (NAT), трансляцію портів (PAT), маршрутизацію або режим transparent mode;
- підтримка як повнозв'язних (full mesh), так і ієрархічних (hub and spoke) VPN мереж, дає користувачам великі можливості на вибір архітектури мережі того або іншого типу, чи їхньої комбінації;
- підтримка доступу за протоколами SSL, IPSec та SSH.

Усі пристрої NetScreen мають розвинені засоби аутентифікації користувачів для контролю доступу до ресурсів мережі, включаючи аутентифікацію користувачів із використанням як локальних ресурсів, так і зовнішніх серверів RADIUS, SecurID, або LDAP.

Характеристики пристроїв.

NetScreen-SA 1000:

- забезпечення захищеного доступу до web і ftp ресурсів, клієнт-серверним програмам. Можлива також організація доступу до ресурсів будь-якого типу;

- можливість заборони завантаження прикріплених до поштових повідомлень документів (у режимі Web-mail);
- оперативний аудит клієнтського ПК для задоволення вимог з безпеки перед наданням доступу до захищених ресурсів (Host Checker);
- примусове очищення кеш-пам'яті браузера після завершення користувацької сесії або через певний проміжок часу (Cache Cleaner);
- динамічна авторизація (призначення ролей користувачам у залежності від їхньої приналежності до тієї або іншої категорії);
- режим Single Sign-On (при роботі з додатками сторонніх виробників, що потребують аутентифікації);
- можливість створення безлічі віртуальних web-сайтів на одному пристрої;
- кластеризація (режими Active /Passive і Active/Active);
- організація захищених web-конференцій.

NetScreen-SA 1000 забезпечує 25-100 SSL/VPN тунелів. Продуктивність 550 Mbps при виконанні функцій міжмережевого екрана.

NetScreen-50:

Забезпечує інтегроване рішення для віддалених офісів. Мають 4 порти Ethernet 10/100. Пристрої забезпечують гнучке рішення для задач, де потрібні декілька демілітаризованих зон, безпровідна локальна мережа, або декілька незалежних сегментів мережі. NetScreen-50- це високопродуктивний пристрій забезпечує 170 Mbps при виконанні функцій міжмережевого екрана. Може підтримувати до 100 VPN тунелів.

3. ДОСЛІДЖЕННЯ СПРОЕКТОВАНОЇ VPN МЕРЕЖІ

3.1 Тестування продуктивності VPN мережі

Для тестування VPN шлюзів ми використали програму SmartFlow, яка генерує TCP та UDP-пакети. В ході тестування пропускна спроможність використовуємих шлюзів склала 152Мбіт/с. При передачі пакетів розміром 128, 512 і 1400 байт ми не виявили ніякої залежності втрати пакетів від їх розмірів. Втрати пакетів склали 1%.

Оцінимо продуктивність VPN мережі, за допомогою програми NetIQ Chariot. Порівняємо продуктивність VPN при створенні різної кількості тунелів.

Створимо криптозахисний тунель (1-2) та заміримо його продуктивність. В результаті ми отримаємо показники, на основі яких можна побудувати наступний графік (рис. 3.1).

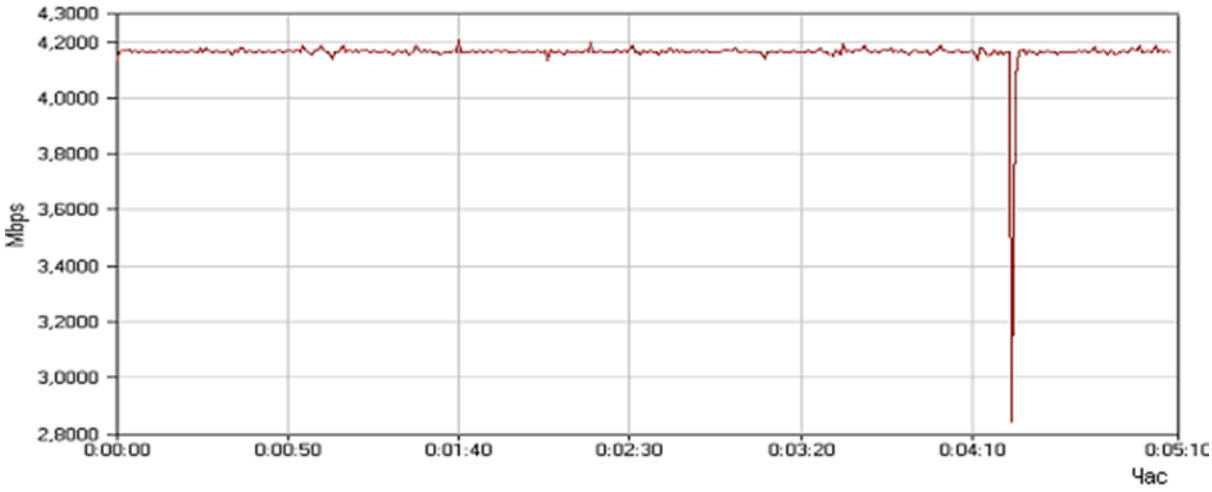

Рисунок 3.1 – Графік продуктивності криптотунелю

Середня швидкість передачі даних − 4.159 Mbps

Середня продуктивність першого VPN-тунелю (1-2) складає 2.907 Mbps, другого − 2.604 Mbps

Створимо два криптозахисних тунелів (1-2 та 1-3) та одночасно заміримо їх продуктивність (рис. 3.2).

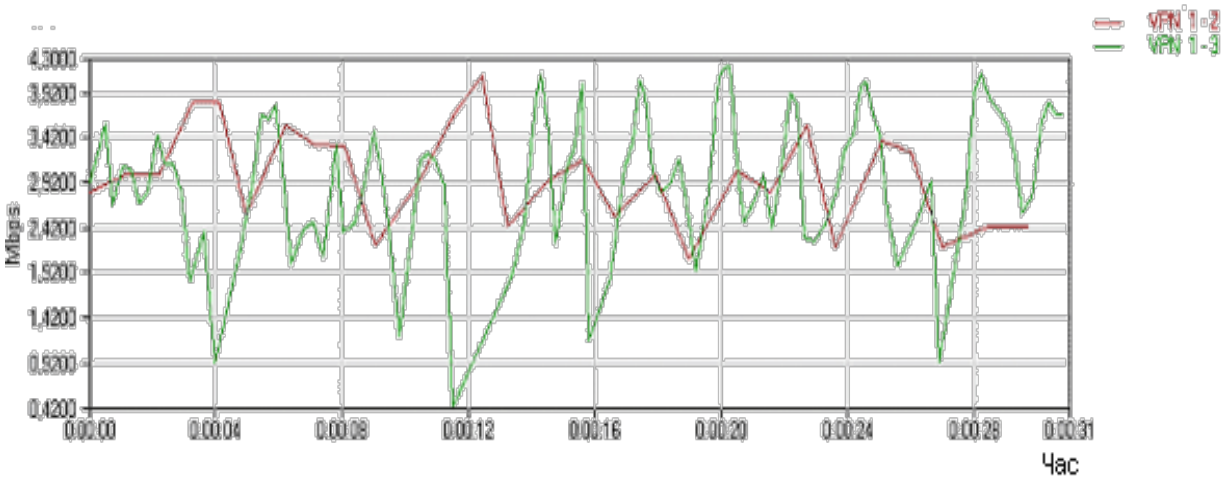

Рисунок 3.2 – Порівняння продуктивності VPN тунелів (1-2)

Сумарну продуктивність між двома VPN тунелями на діаграмі (рис. 3.3).

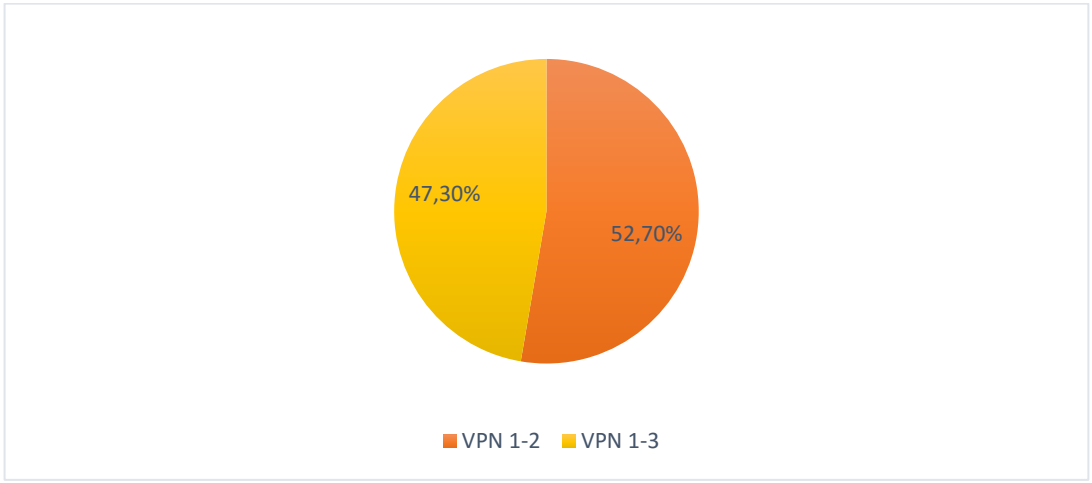

Рисунок 3.3 – Сумарна продуктивність між двома VPN тунелями

Додаємо ще один тунель (1-4). Результати у вигляді графіка (рис. 3.4).

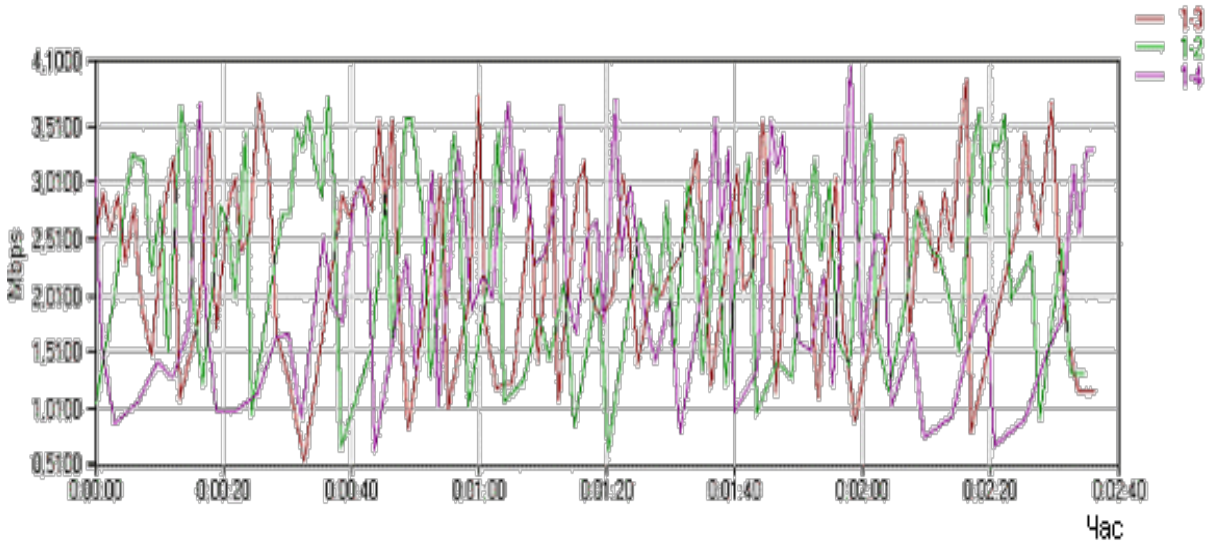

Рисунок 3.4 – Порівняння продуктивності VPN тунелів (1-4)

Середня продуктивність тунелю 1-2 склала 1.963 Mbps, туннеля 1-3 – 2.048 Mbps, тунелю 1-4 – 1.743 Mbps. Сумарна середня продуктивність складає 5.754 Mbps. Сумарну продуктивність між трьома VPN тунелями представимо на діаграмі (рис 3.5).

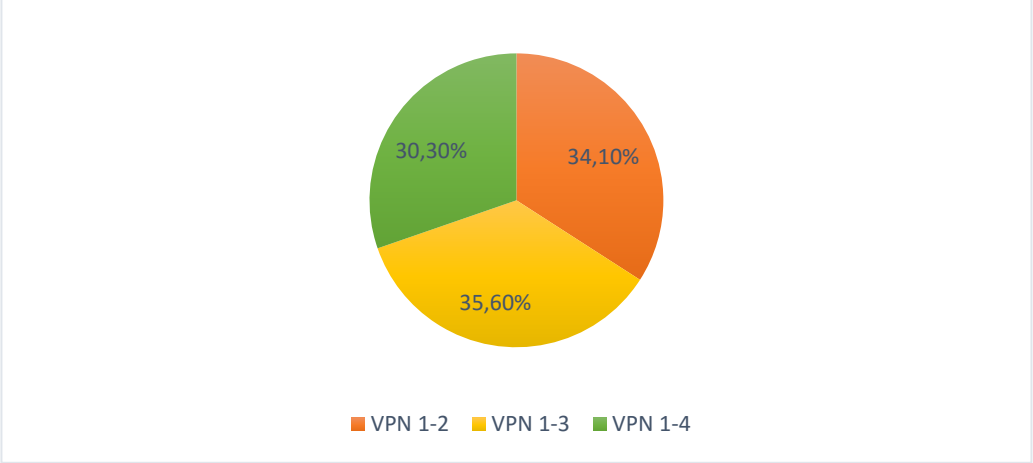

Рисунок 3.5 – Сумарна продуктивність між трьома VPN тунелями

Ми можемо зробити висновок, що VPN мережа добре справляється з навантаженням і показує добрі швидкісні показники, які дозволяють використовувати її на каналах Інтернет.

3.2 Перевірка алгоритму асиметричного шифрування

За допомогою утиліти openssl rand [-out file] [-rand file] num перевіряємо алгоритм асиметричного шифрування.

- опція out виводить результат в file;
- опція rand вказує на файли, з яких будуть зчитуватись данні для seed (зерна) генератора випадкових чисел.

Результати перевірки заносимо в таблицю 3.1.

Таблиця 3.1 – Результати перевірки

Підпис	Перевірка	За секунду підписано	За секунду перевірено
rsa 512 bits	0.0036s	281.4	3221.7
rsa 1024 bits	0.0184s	54.3	1072.9
rsa 2048 bits	0.1105s	9.0	315.6
rsa 4096 bits	0.7414s	1.3	89.4

3.3 Аналіз стійкості до атак

В цьому розділі розглядаються деякі атаки, які можна провести на VPN мережу, побудовану на основі протоколу SSL.

Розкриття шифрів

Атаки проти комунікаційних сесій можуть здійснюватися шляхом запису сесії, і потім, витративши велику кількість комп'ютерного часу, починається спроба підібрати ключ сесії або ключ RSA. У випадку успіху відкривається можливість прочитати передану інформацію. SSL робить ціну таких атак вище, ніж вигоди від успішної атаки, таким чином, роблячи її марною витратою часу і грошей.

Атака відкритого тексту

Атака відкритого тексту відбувається таким чином, що атакуючий має поняття про те, якого типу повідомлення посилаються зашифрованими. Атакуючий може формувати базу даних, де ключами є зашифровані рядки

відомого тексту і за допомогою апаратних або програмних засобів ідентифікувати ключ сесії

SSL намагається протистояти цим атакам, використовуючи великі ключі сесії. Спочатку клієнт генерує ключ, що довше ніж допускається експортними обмеженнями, і посилає частину його відкритим текстом серверові (це дозволено експортними правилами). Відкрита частина ключа поєднується із секретною частиною, щоб одержати досить довгий ключ.

Атака відгуку

Зловмисник записує комунікаційну сесію між клієнтом і сервером. Пізніше, він встановлює з'єднання із сервером і відтворює записані повідомлення клієнта.

SSL відбиває цю атаку, за допомогою спеціального коду "nonce" (ідентифікатор з'єднання), що є унікальним.

Теоретично зловмисник не може вгадати цей код заздалегідь, тому що він ґрунтується на наборі випадкових подій, непідвласних зловмисникові і, отже, він не може реагувати адекватно на запити сервера.

Зловмисник з великими ресурсами може записати велике число сесій між клієнтом і сервером і спробувати підібрати “правильну” сесію, ґрунтуючись на коді nonce, посланому сервером посилає в повідомленні SERVER-HELLO. Однак коди nonce SSL мають, принаймні, довжину 128 біт, таким чином, зловмисник буде змушений записати приблизно 264 кодів nonce, при цьому він одержить імовірність вгадування лише 50%. Це число достатнє велике, щоб зробити такого роду атаку неефективною.

Людина посередині

Атака посередника (людина посередині) припускає участь у комунікаційній сесії трьох суб'єктів: клієнта, сервера і посередника-зловмисника, що знаходиться між ними. Таке розташування дозволяє зловмисникові перехоплювати всі повідомлення, які прямують в обох напрямках, і підмінювати їх.

“Посередник” виступає в ролі сервера для клієнта і клієнтом для сервера. У випадку SSL така атака неможлива через використання сервером сертифікатів. Під час діалогу про встановлення безпечного з'єднання із сервером необхідно надати сертифікат, що підписаний сертифікаційним центром. У цьому сертифікаті розміщається загальнодоступний ключ сервера, його ім'я й ім'я емітента сертифіката. Клієнт перевіряє підпис сертифіката, а потім перевіряє ім'я емітента.

Якщо посередник надає підроблений сертифікат, то він не пройде перевірку підпису, тому що зловмисник не може знати секретного ключа сервера.

ВИСНОВКИ

У дипломній роботі було проведено аналітичний огляд та аналіз основних принципів побудови систем інформаційного захисту корпоративних мереж. З’ясовано, що на даний час технологія VPN ефективно використовує канальні ресурси й найбільш перспективна для захисту взаємодії між віддаленими локальними системами корпоративної мережі та значно зменшує ризик зовнішнього втручання.

Були всебічно вивчені і проаналізовані теоретичні відомості, які стосуються комп'ютерних мереж в загальному та способів захисту мережі. Розроблена та налаштована VPN мережа, що використовує протокол SSL, який дозволяє серверу й клієнту перед початком інформаційної взаємодії аутентифікувати один одного, погодити алгоритм шифрування і сформувати загальні криптографічні ключі.

Проведено тестування продуктивності спроектованої віртуальної корпоративної мережі, в результаті яких можна зробити висновок, що VPN мережа добре справляється з навантаженням і показує гарні швидкісні показники, які дозволяють використовувати її на каналах Інтернет.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. (Електронний ресурс) Режим доступу: www/ URL: https://zakon.rada.gov.ua/laws/show/2657-12

2. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 81/94-ВР//ВВР. 1994. № 31. С. 286.

3. Постанова Кабінету міністрів України від 29 березня 2006 р. N 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»

4. Загальні положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

5. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

6. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації: НД ТЗІ 1.1-005-07. [Чинний від 2007.12.12]. К. : ДСТСЗІ СБУ, 2007. № 232. (Нормативний документ системи технічного захисту інформації).

7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

8. Класифікація автоматизованих систем і стандартні функціо-нальні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. [Чинний від 1999.04.28]. К. : ДСТСЗІ СБУ, 1999. № 22. (Нормативний документ системи технічного захисту інформації).

9. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: НД ТЗІ 3.6-001-2000. [Чинний від 2000.12.30]. К. : ДСТСЗІ СБУ, 2000. № 60. (Нормативний документ системи технічного захисту інформації).

10. Комплексні системи захисту інформації [Текст] : навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.] ; Вінницький національний технічний університет. Вінниця : ВНТУ, 2018. 118 с

11. Політика безпеки для Internet. [Електронний ресурс]. Режим доступу: https://lektsii.org/8-12435.html Загол. з екрана. Дата звернення 12.11.2019.

12. Лапоніна О.Р. Основи мережевої безпеки: криптографічні алгоритми та протоколи взаємодії: підручник. Київ: Іздательство Інтуїт, 2010. 608 с.

13. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". Харків : НТУ "ХПІ", 2014. 251 с.

14. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. К.: КУБГ, 2019. 218 с

15. Офіційний сайт університету ОНЕУ (Електронний ресурс) Режим доступу: www/ URL: http://oneu.edu.ua/pages/about-university/

16. Інформаційно-обчислювальний центр ОНЕУ (Електронний ресурс) Режим доступу: www/ URL: http://oneu.edu.ua/pages/tsentri/cit/