Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

на тему: **" Передавання інформації захищеними мережами. "**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки»)

ПЛАН ЛЕКЦІЇ

1. Захист інформації у відкритих канал зв'язку.
2. Віртуальні захищені мережі.
3. Рівні реалізації віртуальних захищених мереж.
4. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні.

ЛІТЕРАТУРА

1. **Богуш В.М., Кудін А.М.** Інформаційна безпека від А до Я. - К.: МОУ, 1999. – 456 с.
2. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.
3. **Тимошенко А.О.** Методи аналізу та проектування систем захисту інформації: Курс лекцій. - К.: Політехніка, 2007. – 174 с.
4. **Ken Thompson.** Reflections on Trusting Trust. // Communication of the ACM. - Vol. 27, No. 8, August 1984. - P. 761-763.

1. Захист інформації у відкритих канал зв‘язку.

Розвиток мережних технологій змінює типові виробничі процеси в сучасному світі. Можливість індивідуального та колективного доступу до корпоративної мережі майже в будь-який час є незмінною вимогою. Дедалі більше організацій звертає увагу на технології, що дають змогу добре організувати територіально розподілену робочу силу. Співробітники, які перебувають у відрядженнях, тепер мають можливість входити в корпоративну мережу безпосередньо зі своїх номерів у готелях, а ті, хто працює вдома, можуть підтримувати зв'язок із головними офісами своїх компаній у режимі реального часу. Прагнучи зміцнити співробітництво з партнерами та постачальниками, організації відкривають для них окремі області своїх мереж, скорочуючи таким чином час, витрачений на впровадження нової продукції, та підвищуючи якість обслуговування клієнтів.

Слід чітко усвідомлювати, що *будь-які заходи, яких вживають для забезпечення захисту інформації, не повинні коштувати більше, ніж сама інформація.* Облаштування фізично ізольованих захищених каналів зв'язку для безпечного інформаційного обміну між віддаленими вузлами є надзвичайно дорогим і не завжди економічно обґрунтованим заходом. Тому дуже привабливо виглядає можливість забезпечити захист інформації, що передається відкритими каналами зв'язку, зокрема мережею Інтернет.

Захист інформації у процесі її передавання відкритими каналами зв'язку базується на виконанні таких функцій:

1. *автентифікація взаємодіючих сторін;*
2. *шифрування інформації;*
3. *підтвердження достовірності та цілісності доставленої інформації;*
4. *захист від повтору, затримки та видалення повідомлень;*
5. *унеможливлення відмови від фактів відправлення й отримання повідомлень.*

Зазначені функції тісно пов'язані між собою. В основу їх реалізації покладено криптографічний захист даних.

2. Віртуальні захищені мережі.

Об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передавання інформації в єдину віртуальну мережу, яка забезпечує захист інформації, що в ній циркулює, називають захищеною, або приватною віртуальною мережею (Virtual Private Network, VPN). Назва походить від протиставлення приватних (Private) мереж (корпоративних мереж, не доступних для сторонніх користувачів) публічним (Public) мережам (відкритим мережам, мережам загального доступу). Слід зауважити, що слово «private» в англійській мові є синонімом слова «secret» — «таємний». Хоча термін «віртуальні приватні мережі» — дуже поширений, інколи надають перевагу терміну «віртуальні захищені мережі» , оскільки ця технологія стосується не приватної власності, а захисту інформації.

Віртуальна мережа — це така мережа, яка формується як деяка підмножина реальної мережі. Особливою ознакою віртуальної захищеної мережі є її відокремленість від реальної мережі, що робить її достатньо надійною і такою, що в змозі гарантувати конфіденційність і цілісність даних, які нею передаються, а також забезпечувати автентифікацію сторін і унеможливлювати відмову від авторства.

Види віртуальних захищених мереж

Є багато різновидів віртуальних захищених мереж. Починаючи з мереж провайдерів, що дають змогу обслуговувати клієнтів безпосередньо на їхній території, та закінчуючи корпоративними мережами VPN, які розгортають і якими керують організації-власники. Як правило, *віртуальні захищені мережі поділяють на три основні групи: VPN віддаленого доступу (Remote Access VPN), внутрішньо- корпоративні VPN (Intranet VPN) і міжкорпоративні VPN (Extranet VPN).*

VPN віддаленого доступу

Віртуальні захищені мережі віддаленого доступу набули загального визнання завдяки тому, що їх використання значно скорочує витрати на застосування комутованих і виділених ліній. Принцип їх роботи простий: користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі (точкою присутності інтернет-провайдера), після чого дані, які вони передають, тунелюються через Інтернет, що дає змогу уникнути плати за міжміський чи міжнародний зв'язок. Потім дані від усіх користувачів концентруються на спеціальних пристроях — шлюзах віртуальної захищеної мережі — і передаються у корпоративну мережу. Суттєва економія від застосування VPN цього типу є потужним стимулом, але використання відкритого Інтернету для транспортування чутливого (конфіденційного) корпоративного трафіку робить механізми захисту інформації життєво важливими елементами цієї технології.

Внутрішньо-корпоративна мережа VPN

Організації, які бажають організувати для своїх філій та відділень доступ до централізованих сховищ інформації, зазвичай підключають віддалені вузли через виділені лінії або із застосуванням технології Frame Relay. Але використання виділених ліній означає зростання поточних витрат у разі потреби збільшити смугу пропускання та відстань між об'єктами. Через це витрати на зв'язок виділеними лініями перетворюються в одну з основних витратних статей на експлуатацію корпоративної інформаційної системи. Щоб зменшити їх, організація може поєднати вузли за допомогою віртуальної захищеної мережі. Дорогі виділені лінії слід замінити дешевшим зв'язком через Інтернет, де відстань жодним чином не впливає на вартість з'єднання.

Міжкорпоративна мережа VPN

Екстранет — це мережна технологія, яка забезпечує прямий доступ із мережі однієї організації до мережі іншої та у такий спосіб сприяє підвищенню якості зв'язку, що підтримується в ході ділового співробітництва. Екстрамережі загалом подібні до внутрішньокорпоративних віртуальних захищених мереж за тою різницею, що проблема захисту інформації є для них ще гострішою. Коли кілька організацій приймають рішення працювати разом і відкривають одна для одної свої мережі, вони мають потурбуватися про те, щоб їхні нові партнери мали доступ лише до певного кола інформації. У цьому випадку конфіденційна інформація має бути надійно захищена від несанкціонованого використання. Саме тому потрібно, щоб у міжкорпоративних мережах велику увагу було приділено контролю доступу з використанням міжмережних екранів. Також дуже важливою є автентифікація користувачів, яка має гарантувати, що доступ до інформації отримують лише ті, кому він дійсно дозволений. Водночас розгорнута система захисту від несанкціонованого доступу має привертати до себе якомога менше уваги, бути максимально прозорою і не потребувати втручання користувачів.

Проблеми побудови віртуальних захищених мереж

Стисло розглянемо основні проблеми, що постають перед розробниками віртуальних захищених мереж.

Забезпечення конфіденційності

Найпростішим і найпоширенішим способом забезпечення конфіденційності інформації є її шифрування, або криптографічне закриття. Попри те що алгоритми шифрування є дуже складними, їх реалізація великих ускладнень не викликає. А от організація криптосистеми, зокрема підсистеми керування ключами, може викликати багато проблем, насамперед у випадку, коли кількість користувачів стрімко зростає. У реалізації VPN керування ключами є одним із головних завдань, що потребує надійного та ефективного рішення.

Щоразу, коли йдеться про шифрування, згадують про його неминучий побічний ефект, що полягає у деякій втраті продуктивності. Апаратно реалізоване шифрування передбачає застосування у пристроях захисту спеціалізованих інтегральних схем прикладної орієнтації (Application Specific

Integrated Circuit, ASIC), що звільняють ці пристрої від додаткового навантаження, пов'язаного з виконанням алгоритмів шифрування, і забезпечують кодування трафіку без втрати швидкості обміну. Основною перевагою апаратно реалізованих засобів шифрування над програмно реалізованими насамперед вважають забезпечення необхідних показників продуктивності. Є й інша перевага: у разі здійснення атаки на засоби захисту VPN існує загроза підміни програмних компонентів, зокрема тих, що забезпечують шифрування. Загроза несанкціонованого впливу на апаратні засоби є малоймовірною.

Забезпечення цілісності

Як і конфіденційності, цілісності досягають використанням криптографічних алгоритмів, але не шифрування, а хешування. Алгоритми хешування також потребують значних ресурсів процесора, що знов-таки свідчить на користь реалізації цих алгоритмів апаратними засобами з використанням інтегральних схем прикладної орієнтації.

Автентифікація та унеможливлення відмови від авторства

Унеможливлення відмови від авторства — це додаткова функція, яку реалізовано на основі автентифікації. Захищене спілкування часто потребує не лише підтвердження того, що абонент є тим, за кого себе видає, але й незаперечних доказів того, що повідомлення отримане від конкретного користувача. Інколи захищене спілкування потребує доказового підтвердження ще й того факту, що певний користувач справді отримав деяке повідомлення. Ці функції захисту в окремих випадках розглядають як невід'ємну складову реалізації VPN.

Способи утворення захищених віртуальних каналів

Будь-який із двох вузлів віртуальної мережі, між якими формується захищений тунель, може належати кінцевій чи проміжній точці потоку повідомлень, який захищають. Відповідно є різні способи утворення захищеного віртуального каналу.

Найкращим із міркувань безпеки є варіант, коли кінцеві точки тунелю збігаються з кінцевими точками потоку повідомлень. Наприклад, це може бути сервер у центральному офісі компанії та робоча станція користувача у віддаленій філії або портативний комп'ютер співробітника, який перебуває у відрядженні. Перевагою такого варіанта є те, що захист інформаційного обміну буде забезпечено на всьому шляху пакетів повідомлень. Однак такий варіант має суттєвий недолік — децентралізацію керування. Засоби утворення захищених тунелів потрібно встановлювати і належним чином настроювати на кожному клієнтському комп'ютері, що у великих мережах є занадто трудомісткою задачею.

Помітного спрощення завдань адміністрування можна досягти шляхом відмови від захисту трафіку всередині локальної мережі (або локальних мереж), що входить до складу VPN. Така ситуація є достатньо поширеною, оскільки захистити трафік у локальній мережі можна іншими засобами, зокрема реєструючи дії користувачів і вживаючи організаційних заходів. У такому випадку кінцевою точкою захищеного тунелю доцільно обрати брандмауер або граничний маршрутизатор локальної мережі. Захищений тунель утворюють лише у публічній мережі.

3. Рівні реалізації віртуальних захищених мереж.

Реалізацію VPN здійснюють засобами протоколів сеансового, мережного і канального рівнів моделі взаємодії відкритих систем (OSI). Розглянемо переваги та недоліки кожного з рівнів реалізації VPN.

Захист віртуальних каналів на сеансовому рівні

Сеансовий рівень є найвищим рівнем моделі взаємодії відкритих систем, на якому можна створювати захищені віртуальні канали. Побудова VPN на цьому рівні дозволяє досягти найбільшої функціональної повноти захисту інформаційного обміну, надійності контролю доступу, а також простоти настроювання системи безпеки. Протоколи формування захищених віртуальних каналів на

сеансовому рівні є прозорими для прикладних протоколів захисту та мережних протоколів прикладного рівня, на кшталт HTTP, FTP, POP3 та SMTP.

Для криптографічного захисту інформації на сеансовому рівні здебільшого використовують протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security), розроблений компанією Netscape Communications.

Протокол SSL/TLS

Протокол SSL/TLS (скорочено називатимемо його SSL) орієнтовано на захист інформаційного обміну між клієнтом і сервером комп'ютерної мережі. Завдяки своїм позитивним якостям SSL став загальновизнаним стандартом захисту в Інтернеті та в інтранет-мережах, витіснивши такі конкуруючі технології шифрування на прикладному рівні, як Secure HTTP (SHTTP).

В основу протоколу покладено технологію комплексного використання асиметричних і симетричних криптосистем. Як базові використовують криптографічні алгоритми: для асиметричного шифрування — RSA, для симетричного шифрування – RC2, RC4, DES та потрійний DES (Triple DES), для хешування – MD5 і SHA-1. Починаючи з версії SSL 3.0 набір криптографічних алгоритмів розширено (версія TLS 1.0 фактично є розвитком версії SSL 3.0 і мало відрізняється від неї, хоча розробники попереджають про відсутність їхньої сумісності). Для автентифікації сторін, що взаємодіють, а також для криптографічного захисту ключа симетричного шифрування застосовують цифрові сертифікати відкритих ключів, що відповідають стандарту X.509.

Відповідно до протоколу SSL криптозахищені тунелі утворюють між кінцевими точками віртуальної мережі. Ініціаторами створення кожного тунелю є клієнт і сервер. Протоколом SSL передбачено дві стадії взаємодії:

- встановлення SSL-сесії;
- захищена взаємодія.

Процедуру встановлення SSL-сесії називають процедурою «рукостискання», яку виконує протокол «рукостискання» (Handshake Protocol), який входить до складу SSL. За цієї процедури здійснюється:

- автентифікація сторін;
- узгодження криптографічних алгоритмів та алгоритмів ущільнення, які використовуватимуться під час захищеного інформаційного обміну;
- формування спільного секретного майстер-ключа;
- генерування на основі майстер-ключа спільних секретних сеансових ключів для криптографічного захисту інформаційного обміну.

Протокол SSL 3.0 підтримує три режими автентифікації:

- взаємна автентифікація сторін;
- одностороння автентифікація сервера без автентифікації клієнта;
- повна анонімність.

За використання останнього режиму реалізується захищений обмін між клієнтом і сервером, проте не надається жодних гарантій щодо автентичності сторін, які взаємодіють.

Розглянемо етапи здійснення процедури автентифікації, що відповідає другому режиму (автентифікація сервера без автентифікації клієнта).

1. Клієнт надсилає серверу запит на встановлення захищеного з'єднання, в якому передається:

- поточний час і дата;
- випадкова послідовність RAND_CL;
- набір алгоритмів симетричного шифрування та алгоритмів обчислення хеш- функцій, які підтримує клієнт;

- набір алгоритмів ущільнення, які підтримує клієнт.

2. Сервер надсилає у відповідь узгоджений набір параметрів:

- ідентифікатор SSL-сесії;
- обрані криптографічні алгоритми з числа запропонованих клієнтом (якщо запропоновані алгоритми чи їхні параметри з якихось причин не влаштовують сервер, сесію буде закрито);
- сертифікат сервера, завірений цифровим підписом центру сертифікації;
- випадкову послідовність RAND SERV.

3. Клієнт за допомогою відкритого ключа центру сертифікації перевіряє отриманий від сервера сертифікат (якщо перевірка дасть негативний результат, сесію буде закрито) та виконує такі дії:

- виробляє випадкову 48-байтову послідовність Pre-Master Secret, зашифровує її на відкритому ключі сервера, який містився в сертифікаті сервера, і надсилає її серверу;
- використовуючи обраний сервером алгоритм хешування, виробляє спільний таємний майстер-ключ (MasterSecret), використовуючи для цього послідовності Pre-MasterSecret, RAND SERV і RAND_CL;
- за допомогою MasterSecret обчислює сеансові таємні ключі для симетричного шифрування і обчислення хеш-функцій;
- переходить у режим захищеної взаємодії.

4. Сервер, отримавши зашифровану послідовність Pre-MasterSecret, розшифровує її за допомогою свого таємного ключа, а потім виконує такі операції:

- так само, як і клієнт, застосовуючи обраний алгоритм хешування, виробляє спільний таємний майстер-ключ (MasterSecret), використовуючи для цього послідовності Pre-MasterSecret, RAND SERV і RAND_CL; оскільки алгоритм і вихідні послідовності ті самі, що й у клієнта, результат (Master- Secret) має бути ідентичним;
- так само, як і клієнт, за допомогою MasterSecret обчислює сеансові таємні ключі для симетричного шифрування і обчислення хеш-функцій; результати, знов-таки, мають бути ідентичні тим, що отримав клієнт;
- переходить у режим захищеної взаємодії.

5. Клієнт і сервер здійснюють перевірку ідентичності параметрів SSL-сесії (тобто ключів):

- клієнт формує тестове повідомлення із даних, які він надіслав серверу на кроці 1, даних, які він отримав від сервера на кроці 2, та послідовності MasterSecret; після цього він формує код перевірки цілісності повідомлення (MAC-код), зашифровує повідомлення на спільному таємному сеансовому ключі та надсилає його серверу;
- сервер так само формує тестове повідомлення і надсилає його клієнту;
- кожна зі сторін розшифровує одержане тестове повідомлення і здійснює перевірку цілісності.

6. Якщо перевірку ідентичності параметрів здійснено успішно, SSL-сесія вважається встановленою і сторони розпочинають захищену взаємодію.

У ході подальшої захищеної взаємодії кожна із сторін, надсилаючи повідомлення для перевірки його цілісності щоразу формує MAC-код, а потім зашифровує це повідомлення разом із MAC-кодом. Після отримання повідомлення його розшифровують і здійснюють перевірку його цілісності. У разі виявлення порушення цілісності повідомлення SSL-сесію буде закрито.

Протокол SOCKS

Протокол SOCKS було розроблено в 1990 році як посередницький протокол взаємодії клієнт-серверних застосувань сеансового рівня моделі OSI. Він реалізує багато посередницьких

функцій, на кшталт трансляції мережних адрес (Network Address Translation, NAT), контролю за напрямками інформаційних потоків, розмежування доступу відповідно до атрибутів користувачів та інформації, що передається. Порівняно з посередницькими функціями прикладного рівня, SOCKS пропонує більшу швидкодію та незалежність від високорівневих протоколів (HTTP, FTP, POP3, SMTP тощо).

Розрізняють SOCKS-сервер, який здебільшого встановлюють на шлюз або брандмауер мережі, та SOCKS-клієнти, які встановлюють на кожний комп'ютер користувача. SOCKS-сервер взаємодіє з будь-яким прикладним сервером від імені прикладного клієнта, який відповідає цьому серверу. SOCKS-клієнт перехоплює запити від справжніх клієнтів до прикладних серверів і передає їх SOCKS-серверу.

Розглянемо версію 5 протоколу SOCKS (SOCKS v5), запропоновану як стандарт інтернету (RFC 1928, 1929).

Особливості цього протоколу.

- SOCKS v5 підтримує протоколи TCP та UDP, охоплюючи, таким чином, майже всі прикладні протоколи. Використання протоколу SOCKS v5 дає змогу вирішити численні проблеми з безпекою, проте робить недоступними діагностичні утиліти ping і tracert.
- У протоколі SOCKS v5 передбачено автентифікацію не лише SOCKS-клієнтів, але й користувачів, від імені яких ці клієнти звертаються. Є можливість двосторонньої автентифікації.
- SOCKS v5 припускає використання схем адресації IPv4 і IPv6.
- Автентифікацію користувача, яку виконує SOCKS-сервер, може бути засновано на сертифікатах X.509 або на паролях.
- Для шифрування трафіку між SOCKS-клієнтом і SOCKS-сервером можна застосовувати будь-які протоколи сеансового чи нижчих рівнів моделі OSI.

Захист віртуальних каналів на мережному рівні

Стандартні засоби захисту обміну даними на мережному рівні для IP-мережі (зокрема, для Інтернету) визначають набори протоколів IPSec (Internet Protocol Security). Протокол IPv6 обов'язково підтримує IPSec (останній є його складовою), протокол IPv4, як правило, підтримує IPSec (сумісний із IPv4).

IPSec вимагає підтримки стандарту IPSec лише від пристроїв, що безпосередньо спілкуються між собою з обох боків з'єднання. Решта пристроїв, що знаходяться між ними, забезпечують передавання IP-пакетів.

Архітектура засобів захисту IPSec

Технологія IPSec охоплює кілька різних сфер, до яких належать шифрування, автентифікація та керування ключами. Відповідно до IPSec, архітектура засобів безпеки інформаційного обміну є трирівневою (рис. 1) До верхнього рівня належать:

- протокол узгодження параметрів віртуального каналу й керування ключами (Internet Security Association Key Management Protocol, ISAKMP);
- протокол автентифікаційного заголовка (Authentication Header, AH);
- протокол інкапсулюючого захисту вмісту (Encapsulating Security Protocol, ESP).

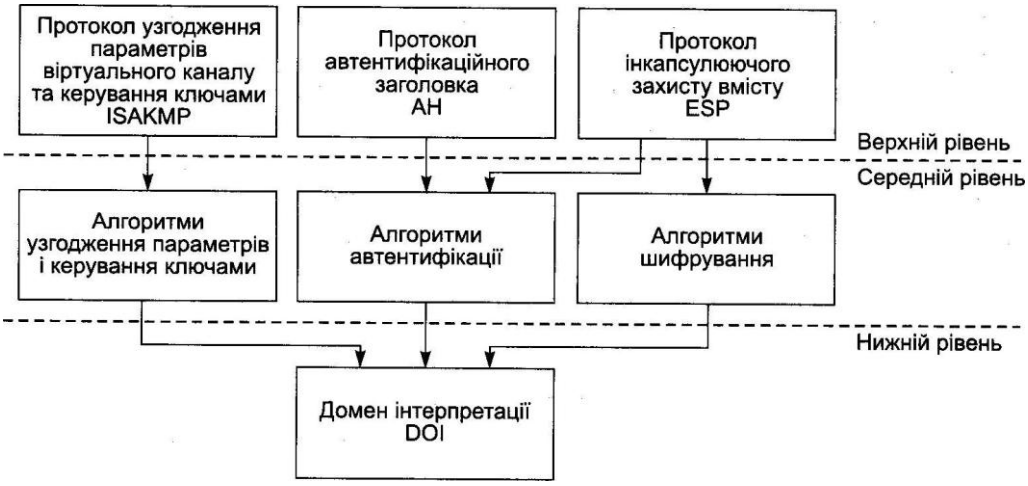

Рис. 1. Архітектура засобів безпеки IPSec

Протокол AH передбачає автентифікацію джерела даних, перевірку цілісності та справжності даних після їх отримання, а також унеможливлення повторних повідомлень. Окрім того, що протокол ESP забезпечує всі функції протоколу AH, він ще й підтримує криптографічний захист пакетів повідомлень.

Протоколи AH та ESP не залежать від конкретних алгоритмів шифрування й автентифікації та підтримують різні методи автентифікації, типи ключів, алгоритми шифрування та розподілу ключів. Тому криптографічні алгоритми, що використовують у протоколах AH та ESP, відносять до окремого (середнього) рівня архітектури IPSec.

Протокол ISAKMP. За його допомогою взаємодіючі сторони створюють спільний контекст, елементи якого вони зможуть вільно використовувати в подальшому. Протокол ISAKMP використовує також певні алгоритми узгодження і керування ключами, розташовані на середньому рівні архітектури IPSec.

Нижній рівень архітектури IPSec — це домен інтерпретації (Domain Of Interpretation, DOI) — база даних, яка містить інформацію про всі застосовані в IPSec протоколи й алгоритми та їхні параметри, ідентифікатори тощо.

Обмін ключами

У разі використання технології IPSec ключі потрібно застосовувати дуже обережно. В IPSec ключі передають у два способи: вручну і шляхом обміну через IP-мережу (Internet Key Exchange, IKE). У першому випадку ключі вручну завантажують у відповідні пристрої IPsec безпосередньо на об'єктах. Оскільки шифруванню ці ключі не піддаються, їх передають особисто системному адміністратору або надсилають поштою.

Протокол IKE — це протокол на базі UDP, який передбачає використання порту 500 для узгодження параметрів асоціацій захисту, що створюються, і для автентифікованого обміну ключами, якими будуть користуватись учасники цих асоціацій. Протокол IKE дає змогу утворити між двома учасниками обміну автентифікований захищений тунель, за яким будуть узгоджуватися параметри асоціації захисту, що створюється для IPSec.

Протокол IKE може функціонувати у трьох режимах.

1. Основний режим (Main Mode) застосовують, коли дві сторони вперше встановлюють зв'язок.
2. Активний режим (Aggressive Mode) є стислою версією основного режиму.
3. Швидкісний режим (Quick Mode) застосовують, коли асоціацію захисту вже було створено в основному чи активному режимі, але є потреба в узгодженні функцій захисту або обміну новими ключами.

Протокол IKE передбачає кілька способів автентифікації. За спільного використання однакових ключів усі хост-системи (чи шлюзи VPN) володіють одними й тими самими таємними

ключами. IKE автентифікує учасників обміну за хеш-значенням ключа, інша сторона шифрує власний ключ і порівнює отримані значення.

Захист віртуальних каналів на канальному рівні

Утворення захищених тунелів на канальному рівні моделі взаємодії відкритих систем забезпечує незалежність від протоколів мережного та вищих рівнів.

На цьому рівні використовують наступні протоколи формування криптозахищених тунелів:

- ♦ PPTP (Point-to-Point Tunneling Protocol)
- ♦ L2F (Layer-2 Forwarding)
- ♦ L2TP (Layer-2 Tunneling Protocol)

Протокол PPTP

Протокол PPTP дає змогу створювати криптозахищені тунелі на канальному рівні моделі OSI, було розроблено за участі корпорації Майкрософт. Основне призначення протоколу — організація доступу віддалених користувачів до локальних мереж як у разі прямого з'єднання віддаленого комп'ютера з публічною мережею, так і у разі підключення до публічної мережі по телефонній лінії через провайдера.

Передбачено три схеми застосування протоколу PPTP.

1. Пряме з'єднання комп'ютера віддаленого користувача з Інтернетом.
2. Комп'ютер віддаленого користувача з'єднується з Інтернетом по телефонній лінії через провайдера, криптозахищений тунель утворюється між сервером провайдера і граничним маршрутизатором локальної мережі.
3. Комп'ютер віддаленого користувача з'єднується з Інтернетом по телефонній лінії через провайдера, криптозахищений тунель утворюється між кінцевими точками взаємодії.

Найчастіше застосовують третю схему, коли трафік захищений від комп'ютера віддаленого користувача і до сервера віддаленого доступу локальної мережі. При цьому від провайдера нічого додаткового не вимагається.

На рис. 2 показано структуру пакетів, що циркулюють у межах сесії PPTP.

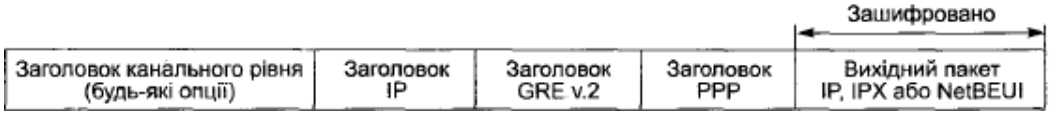

Рис. 2. Структура пакетів PPTP

Протокол L2F

Протокол L2F, основним розробником якого є компанія Cisco Systems, є альтернативою протоколу PPTP. На відміну від PPTP, L2F значно зручніший для провайдерів Інтернету, він підтримує різні мережні протоколи.

У цілому протокол L2F дуже подібний до PPTP. Схема застосування протоколу L2F подібна до другої схеми застосування протоколу PPTP. Захищений тунель утворюється лише між сервером провайдера і сервером локальної мережі.

Якщо політика безпеки вимагає утворення криптозахищеного тунелю між кінцевими точками інформаційного обміну, в L2F для цього пропонується використовувати IPSec. Різниця між використанням самого IPSec і IPSec через L2F- з'єднання полягає в тому, що L2F застосовують для утворення захищеного каналу віддаленого доступу через провайдера, тоді як сам IPSec — лише у разі безпосереднього підключення до мережі.

Протокол L2TP

Протокол L2TP було розроблено організацією IETF на основі протоколів PPTP і L2F. Увібравши в себе кращі риси обох цих протоколів, він підтримує ще кілька додаткових функцій. Недоліком протоколу L2TP є те, що він не забезпечує захист з'єднання комп'ютера віддаленого користувача із сервером провайдера.

Захищений тунель утворюється лише між сервером провайдера і сервером локальної мережі. Як і в L2F, для утворення захищених тунелів між кінцевими точками пропонується використовувати IPSec.

4. Вимоги нормативної бази до реалізації віртуальних захищених мереж в Україні.

Вітчизняна нормативна база змушує замовників (власників ІКС) і розробників дуже обережно ставитися до створення і експлуатації VPN. Розглянемо обмеження стосовно реалізації VPN, які є сьогодні.

Приватні компанії можуть, як правило, без будь-яких обмежень створювати власні VPN для захисту своєї інформації. Якщо в ІКС компанії (незалежно від її організаційно-правової форми та форми власності) обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначена законодавством, то до такої системи мають бути дотримані жорсткі вимоги. Вони полягають у необхідності створювати в таких системах комплексну систему захисту інформації (про те, як це зробити, йтиметься в наступних розділах). Однією з вимог до створення КСЗІ є використання лише таких засобів технічного захисту інформації та криптографічного захисту інформації, які пройшли в Україні процедуру сертифікації або державної експертизи з ТЗІ та (або) КЗІ та отримали дозвіл на використання для оброблення інформації відповідної категорії.

Щодо засобів криптографічного захисту інформації (а саме на них базується технологія VPN), то слід зазначити, що для них перелік дозволених алгоритмів і протоколів шифрування, обчислення хеш-функцій і цифрового підпису — дуже короткий. Тут можна застосовувати лише ті з них, що відповідають вітчизняним стандартам. Виняток робиться для банківських систем, для яких інтеграція з міжнародними системами електронних платежів є життєво необхідною. За процедуру оцінювання таких систем і надання дозволу на їх використання відповідає Національний банк України.

Вітчизняні криптографічні алгоритми вирізняються з-поміж інших своєю високою стійкістю, вони справді забезпечують надійний захист інформаційного обміну. Але існує велика проблема їх інтеграції із типовими рішеннями VPN. Розглянуті в цьому розділі протоколи канального та мережного рівнів припускають можливість використання будь-яких алгоритмів шифрування й хешування за умови дотримання процедури їх впровадження (реєстрація у відповідних міжнародних органах, наявність ідентифікаційного номера тощо). Наразі така робота триває. На практиці це означає, що немає готового програмного продукту іноземного виробництва, а тим паче програмно-апаратного рішення, що можна було б застосовувати для створення на теренах нашої держави розподіленої ІКС, яка використовує технологію VPN і призначена для оброблення інформації, що є власністю держави, або такої, потребу в захисті якої визначено законодавством. Це не виключає можливості побудови такої системи цілковито на базі вітчизняних рішень (є програмні та апаратні рішення, що пройшли процедуру сертифікації і отримали дозволи на застосування), але суттєво ускладнює її повноцінну інтеграцію з будь-якими міжнародними системами.