МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет Магістерської підготовки
Кафедра Інформаційних технологій

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Аналіз технологій захисту інформаційних мереж на базі VPN протоколів»

Виконав студент 2 курсу групи МІС-18 спеціальності 122 Комп'ютерні науки
Гашімов Джавід Бахтіяр оглу

Керівник д.т.н., проф.
Казакова Н.Ф.

Консультант

Рецензент д.т.н., проф.
Положаєнко С.А

Одеса 2020

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

МВВД – моніторинг відкритих і відносно-відкритих джерел
СІ – соціальна інженерія
AES – Advanced Encryption Standartd
CHAP – Challenge Handshake Authentication Protocol
DES – Data Encryption Standartd
DoS – Denial of Service
NMS – Network Management System
PAP – Password Authentication Protocol
PGP – Pretty Good Privacy
SIEM – Security Information and Event Management
SSH – Secure Shell
SMS – System Management System
SSL – Secure Sockets Layer
VPN – Virtual Private Network

ВСТУП

Необхідність в забезпеченні безпеки мереж на основі протоколу IP (Internet Protocol) постійно зростає. Перші засоби захисту з'явилися практично відразу після того, як вразливість IP-мереж дала про себе знати на практиці. Характерними прикладами розробок в цій області можуть служити PGP (Pretty Good Privacy – дуже хороший захист) для шифрування повідомлень електронної пошти, SSL (Secure Sockets Layer – рівень захищених сокетів) для захисту Web-трафіка, SSH (Secure Shell – програма для віддаленого доступу) для захисту сеансів і процедур.

Загальним недоліком подібних широко поширених рішень є їх приналежність до певного типу трафіку, а значить, нездатність задовольнити вимогам до систем мережного захисту, які вимагають великі корпорації або Internet-провайдери. Найрадикальніший спосіб подолати вказане обмеження зводиться до того, аби будувати систему захисту не для окремих класів трафіку. а для мережі в цілому. Стосовно IP-мереж це означає, що системи захисту повинні діяти на мережному рівні моделі OSI (Open Systems Interconnection Basic Reference Model – базова еталонна модель взаємодії відкритих систем).

Перевага такого вибору полягає в тому, що в IP-мережах саме даний рівень відрізняється найбільшою однорідністю: незалежно від вищенаведених протоколів, фізичного середовища передачі і технології канального рівня транспортування даних по мережі не може бути здійснено в обхід протоколу IP.

Тому реалізація захисту мережі на третьому рівні автоматично гарантує, як мінімум, таку ж ступінь захисту всіх мережних засобів. Архітектура IPSec (скорочення від IP Security) сумісна з протоколом IPv4 (Internet Protocol version), тому її підтримку досить забезпечити на обох кінцях з'єднання.

Таким чином, якщо використовувати IPsec, то можна захистити передачу даних в мережі для всіх застосувань і для всіх користувачів прозоріше, ніж при використанні будь-яких інших засобів.

1 ІНФОРМАЦІЙНА БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Інциденти інформаційної безпеки

Інцидент (incident, здійснена загроза) – це дія зловмисника, яка завдає шкоди програмно-апаратним засобам комп'ютерної мережі та конфіденційності, цілісності й доступності комп'ютерних даних. Згідно із запропонованою Конвенцією Ради Європи класифікацією кібернетичних втручань і загроз інциденти поділяють на такі види:

- несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної мережі або її частини, здійснений в обхід систем безпеки);
- втручання в роботу мережі (протиправне порушення або створення перешкод функціонуванню комп'ютерної мережі завдяки розробленню та поширенню вірусного програмного забезпечення, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й телекомунікаційні системи);
- перехоплення (протиправне навмисне аудіовізуальне або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних в обхід заходів безпеки);
- незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

Розрізняють внутрішні й зовнішні інциденти. Внутрішні інциденти виникають внаслідок шкідливих дій осіб, безпосередньо пов'язаних із постраждалою системою. До найбільш поширених внутрішніх інцидентів відносять неправомірний доступ до конфіденційної інформації та її витік, вилучення інформації та її використання в протизаконних операціях [1][1)]. Під зовнішнім інцидентом розуміють подію, джерелом якого є порушник, безпосередньо не

[1)] [1] Бобало Ю.Я. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. 580 с.

пов’язаний із постраждалою комп’ютерною мережею. До подій такого типу належать вірусні атаки на програмне та технічне забезпечення мережі, атаки типу “відмова в обслуговуванні”, перехоплення трафіку, неправомірний доступ до конфіденційної інформації та її розміщення в мережі Інтернет, сканування порталу корпоративної мережі, шахрайство в системах електронного документообігу тощо.

Мережу Інтернет зловмисники все частіше використовують для розсилання фальшивих електронних листів із метою шантажу та шахрайства, організації бот-мереж для здійснення атак на приватні сайти, розповсюдження нових видів шпигунських програм. Програми-шпигуни призначені для виявлення та викрадення конфіденційної інформації. Серед них найбільш поширеними є сканери даних із портів комп’ютерів, клавіатури та екрана. У комп’ютерних мережах кібершпигуни здійснюють аналіз трафіку, електронної пошти, сайтів, розмов через звукову карту тощо.

Для організації атак на інформаційну систему зловмисники часто використовують **вразливості** програмного забезпечення мережі, які дають змогу отримати несанкціонований доступ до даних. Для виявлення вразливостей системи зловмисники останнім часом використовують набір спеціальних програм – сканерів вразливостей відомої платформи **Burp Suite**. Платформа містить ряд розширень, які забезпечують моніторинг системи, тестування програмного забезпечення, складання карти веб-додатків, пошуку файлів і папок, модифікації запитів, підбору паролів тощо. Отримані результати використовують для створення експлойтів. **Експлойт** (exploit – експлуатувати) – це розширення шкідливої програми, яке використовує виявлені вразливості в роботі програмного забезпечення мережі та призначене для проведення атаки на інформаційну систему. Метою атаки може бути як захоплення контролю над мережею з усіма можливими наслідками, так і порушення її функціонування (наприклад, шляхом організації DoS-атаки). Атаки можуть бути направлені на системне та прикладне програмне забезпечення, інформаційні дані, браузери, інтернет-сайти тощо. У залежності від способу отримання доступу

до вразливого програмного забезпечення та їх запуску експлойти можуть бути як зовнішніми (віддаленими), так і внутрішніми (локальними). [2][1)]

В останні роки зловмисники почали активно застосовувати методи **моніторингу відкритих і відносно-відкритих джерел** (МВВД) та **соціальної інженерії** (СІ). Моніторинг відкритих і відносно-відкритих джерел полягає в збиранні різного виду інформації про об'єкт розвідки з її подальшим опрацюванням та підготовленням оперативних дій. Соціальна інженерія використовує різноманітні способи, спрямовані на отримання зловмисником доступу до конфіденційної інформації завдяки зовнішньому впливу на працівників об'єкту атаки та наступним провокуванням внутрішнього інциденту.

Для підготовки атаки агенти соціальної інженерії користуються, переважно, такими засобами, як фішинг, претекстинг і бейтинг. **Фішинг** (Phishing – риболовля) – використання фальшивих веб-сайтів легальних організацій, соціальних мереж та електронних повідомлень користувачам із метою їх дезорієнтації й спонукання до розкриття своїх персональних даних. **Бейтинг** (To bait – підгодовування, використання наживки) – знайомство через соціальні мережі, спеціально створені веб-сайти та форуми з фахівцями тих галузей, які цікавлять агентів соціальної інженерії, та отримання від них конфіденційної інформації.. **Претекстинг** (Pretexting – привід) – дії, при яких зловмисник, видаючи себе за іншу людину та використовуючи телефон, електронну пошту або програму **Skype** мережі Інтернет, згадуючи імена реальних людей, відомі події та дати, входить у довіру до жертви й отримує від неї інформацію, яка його цікавить.

Разом із тим, методи соціальної інженерії передбачають використання різних закладок (пристроїв підслуховування, відео та аудіо спостереження тощо), замаскованих під предмети побуту, аксесуари індивідуального користування, іграшки тощо.

[1)] [2] 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

Для доступу до інформаційних ресурсів комп'ютерних мереж зловмисники можуть використовувати технічні канали витоку інформації. Технічні канали витоку інформації поділяють на канали первинних електромагнітних випромінювань, канали вторинних наведень у навколишніх конструкціях і системах комунікацій, акустичні й оптичні канали. Перечислені канали зловмисники можуть використовувати для несанкціонованого доступу до конфіденційної інформації в процесі її передавання, опрацювання та зберігання.

Останніми роками зловмисники активно використовують методи соціальної інженерії для проведення шахрайських дій із картками банківських клієнтів, тобто виманюють реквізити банківських карток або заохочують власників платіжних карток перерахувати гроші на свої рахунки. Шахраї публікують на сайтах оголошення про продаж за передоплатою товарів за привабливою ціною або спеціально створюють інтернет-магазини із продажу неіснуючих товарів. Серед банкоматного шахрайства зловмисники широко використовують кеш-трепінг і скімінг. **Кеш-трепінг** (Cash Trapping – захоплення готівки) – це встановлення на отвір для видавання готівки шахрайських пристроїв, які унеможливлюють отримання готівки жертвою й дають змогу зловмиснику отримати готівку після відходу жертви від банкомата. **Скімінг** (Skimming – проглядати) – установлення на картрідер (зчитувач карток) банкомату спеціальних пристроїв, які дають можливість зловмисникам копіювати магнітну смугу платіжної картки. При цьому **персональний ідентифікаційний номер** (Personal Identification Number – PIN-код) платіжної картки шахраї отримують за допомогою встановленої на банкоматі мініатюрної відеокамери розміром менше голівки сірника.

У процесі проникнення інформаційних технологій в усі сфери діяльності людини залежність кожної людини від інформаційних систем і мереж, а також та його вразливість щодо стороннього кібернетичного впливу постійно зростають. Сучасний кібертероризм вийшов за межі викрадення секретної інформації та отримання фінансової вигоди від проведення атаки. Розміщення неправдивої (фейкової) інформації на спеціально створених сайтах

(consumer opinion sites), а також поширення небезпечного контенту (вмісту) через соціальні мережі, форуми, блоги, електронну пошту може не лише спровокувати соціальні заворушення та паніку серед населення, а й запустити незворотні процеси в державних масштабах (зруйнувати банківську та фінансову системи держави, вплинути на роботу об'єктів критичної інфраструктури тощо).

Діяльність злочинців у сфері інформаційних технологій характеризується відсутністю національних кордонів, а їхні дії можуть бути спрямовані як на приватні, так і на урядові об'єкти. У міжнародних стосунках на заміну військовим діям із застосуванням армійських підрозділів усе частіше приходять інформаційні та гібридні війни, при яких активно використовують кібершпіонаж та кібератаки на об'єкти критичної інфраструктури. Зловмисники спрямовують свої атаки на урядові сервери, сервери політичних партій, громадських організацій, виборчих комісій тощо.

Яскравим прикладом міжнародного кібертероризму є проведення атак із допомогою відомих шкідливих програм-вірусів **WannaCry** та **Petya**, які використали вразливості системного й прикладного програмного забезпечення інформаційних систем. Перший вірус у 2016 році масово шифрував дані заражених комп'ютерів із метою отримання викупу, а другий улітку 2017 року атакував об'єкти критичної інфраструктури багатьох країн у різних частинах світу. В обох випадках заражені комп'ютери були атаковані через електронну пошту. Міжнародного розголосу набули викрадення зловмисниками конфіденційної інформації з сайтів державних установ, використання соціальних мереж для впливу на результати виборів до державних органів влади у ряді європейських країн та США, результати проведення референдумів тощо.

Успішна боротьба з міжнародним кібертероризмом можлива лише за умови тісної співпраці національних і міжнародних правоохоронних органів із провідними компаніями в галузі інформаційних технологій та кібербезпеки.

1.2 Принципи організації безпеки комп’ютерних мереж

Безпека комп’ютерної мережі передбачає організацію такого її стану, при якому її інформаційні й програмно-технічні ресурси, а також допоміжна інфраструктура будуть захищеними від шкідливого впливу як звичайних користувачів, так і зловмисників. Захист мережі від несанкціонованих дій із боку як внутрішнього, так і зовнішнього середовища забезпечують політикою інформаційної безпеки. Організація служби безпеки комп’ютерної мережі ґрунтується на дотриманні ряду принципів, найбільш важливими з яких є:

- надання працівникам підприємства мінімальних прав, достатніх для виконання ними своїх обов’язків;
- забезпечення надійного захисту всіх рівнів багаторівневої інформаційної системи;
- використання єдиного міжмережевого екрану для захисту внутрішньої корпоративної (приватної) мережі від зовнішніх загроз;
- блокування входу в корпоративну мережу при виході з ладу міжмережевого екрану;
- використання захищених каналів для зв’язку з користувачами, які знаходяться в зовнішніх мережах;
- шифрування трафіку безпроводових мереж;
- захист технічних каналів витоку інформації;
- регулярне резервне копіювання найбільш важливих даних.

Для здійснення цих принципів необхідно забезпечити автентифікацію взаємодіючих сторін, конфіденційність передавання інформації, підтвердження достовірності й цілісності переданої інформації. Перераховані функції

багато в чому пов’язані між собою, а їх здійснення засноване на криптографічному захисті даних, які передають по мережі.[3][1)]

Автентифікацію взаємодіючих сторін у сучасних комп’ютерних мережах здійснюють із використанням спеціальних протоколів (правил). Існує багато різних протоколів автентифікації, які забезпечують надійну ідентифікацію користувачів інформаційної мережі.

Найбільш поширеними є протокол **автентифікації за паролем** (Password Authentication Protocol – PAP) і протокол **автентифікації за запитом** (Challenge Handshake Authentication Protocol – CHAP). протокол автентифікації за паролем PAP вимагає від користувача вказати своє ім’я й пароль, які сервер порівнює із записаними в його пам’яті зашифрованими образами. Протокол автентифікації за запитом CHAP, який входить у сімейство протоколів “точка-точка” (Point-to-Point Protokol – PPP) використовують при автентифікації під’єднаних до Інтернет віддалених користувачів. За цим протоколом паролі користувачів зберігають у їх агентів автентифікації на сервері Інтернет-провайдера. При встановленні зв’язку користувач і агент автентифікації обмінюються послідовністю зашифрованих повідомлень. При отриманні позитивних результатів їх аналізу користувач отримує дозвіл на доступ до ресурсів мережі.

У мережах із великою кількістю користувачів замість автентифікації за паролем використовують автентифікацію за сертифікатами, які містять інформацію, що підтверджує особистість користувачів. Сертифікати видають користувачам спеціальні уповноважені організації – **центри сертифікації** (Certifikat Authority – CA). Користувачі у своїх запитах до серверів мережі вказують сертифікати із закритими ключами, за якими здійснюють їх автентифікацію.

[1)] [3] 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)

Автентифікацію можуть застосовувати не лише для підтвердження особистості учасників сеансу зв'язку, але й для підтвердження достовірності документів, програмних та технічних засобів тощо. Так, деякі розробники програмних засобів із метою захисту авторського права вносять у свої програми спеціальні коди, які дають можливість виконати автентифікацію їхніх програм.

Одночасно з автентифікацією здійснюють авторизацію користувача.

Авторизація забезпечує контроль доступу легальних користувачів до ресурсів мережі й надання їм прав, визначених адміністратором мережі. У деяких мережах використовують ідентифікацію фізичної особи. Найбільш поширеним і надійним способом ідентифікації фізичної особи є її ідентифікація за біометричними параметрами: сітківкою ока, відбитком пальця, рисами обличчя, особливостями голосу тощо.

Конфіденційність передбачає, що лише відправник і отримувач пакету здатні зрозуміти зміст повідомлень, які передають по мережі. Одним із найбільш уживаних способів забезпечення конфіденційності повідомлень є їх шифрування й дешифрування з використанням одного або декількох ключів. Розрядність ключа визначає число можливих комбінацій, які можуть бути використані для шифрування одного символу текстової інформації. [4], [5][1)]

У сучасних мережах можуть використовувати асиметричні й симетричні, відкриті та особисті ключі, моноалфавітні та поліалфавітні шифри, одинарне, подвійне та потрійне шифрування. З середини 90-их років для шифрування й дешифрування несекретних повідомлень почали використовувати стандарт **DES** (Data Encryption Standartd – стандарт шифрування даних). Шифр DES кодує 64-розрядні блоки повідомлення за допомогою 64-розрядного

[1)] [4] Класифікація автоматизованих систем і стандартні функціональні 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).

[5] 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).

ключа. Шифр **3DES** (потрійний DES) кодує блоки повідомлення тричі з використанням трьох різних ключів. З 2001 року в комп'ютерних мережах почали використовувати покращений стандарт шифрування **AES** (Advanced Encryption Standartd – удосконалений стандарт шифрування), який опрацьовує дані 128-розрядними блоками із ключами довжиною 128, 192 і 256 біт.

Цілісність повідомлень передбачає забезпечення незмінності повідомлення при його пересиланні по мережі. Одним із найбільш надійних і розповсюджених засобів забезпечення цілісності повідомлень є використання цифрового підпису. Цифровий підпис підтверджує, що повідомлення зашифроване й надіслане дійсно відправником, що ніхто інший надіслати його не міг, що відмовитися від свого підпису відправник не може. При використанні цифрового підпису здійснення трудомісткого шифрування цілого повідомлення не є обов'язковим. Формування цифрового підпису часто виконують шляхом хешування характерного блоку обмеженої довжини (дайджесту) повідомлення з його наступним шифруванням за допомогою особистого ключа користувача. **Хешуванням** (гешування, hashing) називають перетворення з допомогою **хеш-функції** (геш-функція, hash function) повідомлення довільної довжини у вихідний бітовий рядок фіксованої довжини. Ця бітова послідовність носить назву **хеш-код** (геш-код, хеш-сума, хеш, hash) або **дайджест повідомлення** (message digest). Зміна вхідного тексту навіть на один символ повністю змінює результат обчислення хеш-коду. Для хешування повідомлень використовують велику кількість хеш-функцій, які відрізняються як розрядністю хешів, так і обчислювальними алгоритмами та криптостійкістю. Серед простих і надійних хеш-алгоритмів широкого застосування знайшли алгоритми, побудовані на використанні математичних операцій ділення із залишком, множення із застосуванням "золотого перерізу", коефіцієнтів поліномів тощо. Випадок, коли хеш-функція перетворює різні повідомлення в одинакові хеші, називають **колізією** (collision). На практиці хеш-функції часто вибирають із заданої множини за допомогою випадкових чисел, що дає можливість зменшити ймовірність виникнення колізій.

Цифровий підпис можуть також використовувати для автентифікації користувача чи отриманих повідомлень.

У загальному випадку захист комп'ютерних мереж від загроз із боку зовнішнього середовища вимагає якісного вирішення двох базових задач:

1 Захист підключених до публічних каналів зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій із боку зовнішнього середовища.

2 Захист інформації в процесі її передавання відкритими каналами зв'язку.

Захист приватних мереж від загроз зі сторони публічної мережі здійснюють за допомогою міжмережевих екранів (брандмауерів) та програмних засобів виявлення й знешкодження загроз. Міжмережеві екрани, функції яких залежать від їх типу, моделі та конкретної конфігурації, можуть застосовувати різні алгоритми опрацювання вхідних та вихідних даних і забезпечувати різні ступені захисту мережі від зовнішніх загроз.

Виконання постійного аудиту мережі дає можливість підвищити ступінь її захисту. При здійсненні аудиту аналізують поведінку підозрілих об'єктів мережі, вносять відповідні записи в журнал реєстрації та ідентифікують порушника. Функції аудиту можуть виконувати різні засоби забезпечення безпеки мережі: мережевими моніторами, системами виявлення вторгнень, міжмережевими екранами, антивірусними програмами тощо.

Захист даних при їх передаванні через публічну мережу відкритими лініями зв'язку забезпечують шляхом створення окремих **захищених каналів** або **віртуальних приватних мереж** (Virtual Private Network – VPN), які забезпечують виконання взаємної автентифікації користувачів при встановленні логічного з'єднання, шифрування даних та підтвердження цілісності отриманих повідомлень.

1.3 Методи та засоби забезпечення вимог політики безпеки комп'ютерної мережі

Згідно з вимогами стандартів ISO 7498-4 та X.700 заходи, направлені на підвищення безпеки мережі, впроваджує й супроводжує системний адміністратор, а у великих мережах – адміністратор безпеки мережі. Він здійснює статичні записи в таблицях адресації комутаторів, маршрутних таблицях вузлів (хост, гост) і маршрутизаторів, виділяє статичні IP-адреси вузлам мережі, визначає IP-адресу шлюзу за замовчуванням тощо. До його функцій входять реєстрація користувачів, надання їм пріоритетів, паролів, забезпечення доступу до мережевих ресурсів тощо.

Вимоги політики безпеки щодо захисту приватної мережі від внутрішніх та зовнішніх загроз можуть бути забезпечені на різних рівнях стеку комунікаційних протоколів. На фізичному рівні захист приватних мереж від витоку інформації забезпечують різноманітними способами, зорієнтованими на тип каналу витоку. Політика інформаційної безпеки мережі передбачає використання таких заходів запобігання витоку інформації:

- розміщення комп'ютерного та допоміжного обладнання, а також розташування приміщень для офісних працівників у спеціалізованих екранованих будівлях;
- використання для екранування приміщень металевих сіток, металізованих вікон та побудова спеціальних екранованих приміщень;
- прокладання проводів і кабелів мережі в екранованих оболонках, заміна неекранованих кабелів на волоконно-оптичні кабелі;
- установлення на лініях зв'язку та мережах електропостачання високочастотних фільтрів;
- використання екранованого як основного, так і допоміжного обладнання;
- установлення активних систем зашумлення навколишнього середовища;

– використання систем сканування для виявлення радіо- та відеозакладок. Для створення електромагнітного шумового бар'єру використовують різноманітні широкосмугові генератори шуму. Ефективним є запаковування кабелів у наповнену інертним газом герметичну металеву трубу, при пошкодженні якої зловмисником тиск газу понижується, що активізує відповідні давачі й викликає сигнал тривоги. Практично повністю позбутися електромагнітного випромінювання лініями зв'язку можливо при використанні волоконно-оптичних кабелів.

На канальному рівні мережі Ethernet використовують фільтрацію кадрів комутаторами за MAC-адресами та технологію створення **віртуальних локальних мереж** (ВЛМ, Virtual LAN – VLAN). Стандарт IEEE 802.1Q описує побудову віртуальних мереж на базі одного або декількох **комутаторів** (switch). При побудові VLAN адміністратор за допомогою спеціальної програми закріплює порти комутаторів за номерами та іменами робочих груп. Обмін кадрами допускається між вузлами тільки в границях тієї групи, до якої вони належать.

На мережевому рівні з метою зменшення чутливості до широкомовного трафіку, полегшення адміністрування, зменшення завантаженості та покращення захищеності мережу з великою кількістю вузлів розбивають на декілька підмереж, тобто структуризують. Згідно з вимогами стандарту RFC 950 структуризацію IP-мережі здійснюють шляхом її розбиття на окремі підмережі з використанням масок як постійної, так і змінної довжини. При цьому під ідентифікатори підмереж виділяють старші біти адресного поля вузлів виділеної IP-адреси певного класу, а підмережі з'єднують між собою за допомогою маршрутизаторів або комутаторів 3-го рівня.

Захист даних від загрозливих дій зі сторони агресивного середовища виконують за допомогою апаратно-програмних **міжмережевих екранів** (мережевий екран, захисний екран, brandmauer – брандмауер, firewall – фаєрвол). Брандмауери можуть застосовувати різні алгоритми опрацювання мережевого трафіку, програмні засоби виявлення й знешкодження загроз, забезпечувати

різні ступені захисту інформаційної системи на мережевому, сеансовому та прикладному рівнях моделі OSI. [6][1)]

Важливими різновидами міжмережевих екранів є **проксі-сервери** (proxy- server, сервер-посередник**,** уповноважений сервер) – програмні додатки, які виконують функції посередника між клієнтськими й серверними розподіленими додатками. Проксі-сервер може бути встановлений не тільки на платформі міжмережевого екрану, але й на будь-якому вузлі мережі. При цьому програмне забезпечення комп'ютерів користувачів повинно бути сконфігуроване так, щоб їх запити до ресурсного сервера не могли обійти проксі-сервер. Проксі-служби такого програмного сервера-посередника зорієнтовані на конкретні протоколи різних рівнів, що дає змогу здійснювати аналіз отриманого повідомлення й приймати рішення про підозрілий характер поточного сеансу.

Сучасні **маршрутизатори** (роутер – router) володіють багатьма додатковими функціями, які дають можливість будувати на їх базі досить ефективні брандмауери для захисту інформаційної системи на канальному та мережевому рівнях.

Для забезпечення інформаційної безпеки мережі системні адміністратори найбільш часто використовують такі підходи:

– виконання вимог стандарту IEEE 802.1x;
– застосування сервера автентифікації RADIUS (Remote Authentication Dial-In User Service – віддалена автентифікація користувацьких сервісів);
– використання технологій захищених каналів та віртуальних приватних мереж (Virtual Private Network).

Стандарт IEEE 802.1x описує організацію контролю доступу до LAN на рівні портів комунікаційного обладнання і використовується у мережах,

---

[1)] [6] 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.

побудованих на основі технологій Token Ring, FDDI, сімейства Ethernet та стека TCP / IP. При цьому комутатори, до портів яких підключають кінцеве обладнання користувачів з унікальними MAC-адресами (Media Access Control – управління доступом до середовища), конфігурують відповідно до поставлених вимог. Це забезпечує можливість ідентифікації користувача за його MAC-адресою вже в точці доступу. Фільтрацію кадрів за MAC-адресою здійснюють комутаторами мережі на основі записів, указаних адміністратором. Це запобігає несанкціонованому доступу до вузлів мережі та створює основу для детального обліку (білінг, billing) послуг, що надають користувачу в мережі.

Сервер автентифікації, авторизації та обліку різноманітних послуг на основі протоколу **RADIUS** застосовують для ідентифікації, обліку та контролю прав користувачів. Взаємодію між комутаторами мережі й сервером RADIUS забезпечують шляхом обміну керуючими повідомленнями при забезпеченні взаємної автентифікації та шифрування переданих даних. Для контролю за правами користувачів комутатор надсилає запит серверу RADIUS і на підставі наявної інформації про користувача дозволяє йому доступ до певних мережевих ресурсів або відмовляє в цьому. Рішення про віднесення обладнання з певною MAC-адресою до якої-небудь VLAN або переадресацію запитів приймає центральна база даних RADIUS. Невідоме обладнання може бути підключене до спеціальної VLAN із подальшим доступом до некритичних базових послуг.

Для здійснення діагностики й моніторингу комп'ютерних мереж, комп'ютерів та програмного забезпечення з метою виявлення можливих проблем у системі безпеки, оцінювання й усунення вразливості використовують спеціальні програмні або апаратні засоби – **сканери вразливостей**. Сканери вразливостей забезпечують перевірку програмних додатків на наявність ознак, якими можуть скористатися зловмисники для порушення роботи мережі, погіршення якості надання послуг та несанкціонованого доступу до інформаційних ресурсів мережі. Сканери дають можливість виявляти активні програмні додатки, IP-адреси, відкриті порти та параметри мережевої

операційної системи. Вони визначають рівень можливого втручання в операційну систему або програмні додатки та формують звіт про рівень безпеки мережі. [6] [1)]

Системний адміністратор систематично виконує моніторинг мережі: аналізує її стан, виконує аналіз мережевого трафіку, контролює й керує параметрами апаратно-програмних компонентів. При інтегрованому моніторингу складної комп'ютерної мережі використовують здебільшого дві системи централізованого керування: **систему керування мережею** (Network Management System – NMS) та **систему керування системою** (System Management System – SMS). NMS зорієнтована на керування комунікаційним обладнанням та контроль трафіку мережі, а SMS збирає інформацію про встановлені в мережі комп'ютери та програмно-апаратні засоби, а також записує отримані параметри в спеціальну базу даних.

Слід зауважити, що надійна безпека інформаційних систем може бути забезпечена лише у випадку застосування методів комплексного захисту з використанням як апаратно-програмних засобів, так і організаційних та технологічних заходів. Політика безпеки визначає необхідний і достатній рівень захисту інформаційної системи за критерієм доцільності, який ґрунтується на співвідношенні коштів, затрачених організацію захисту мережі, до втрат, які може понести підприємство у випадку проникнення зловмисника в мережу.

1.4 Атаки на інформаційні та програмно-технічні ресурси комп'ютерної мережі

Зловмисники здійснюють загрози на інформаційні та програмно-технічні ресурси мережі шляхом використання цілеспрямованих дій, які називають **атаками**. Атаки на ресурси комп'ютерної мережі шляхом використання

[1)] [6] 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.

спеціально створених шкідливих (злоякісних) програм зловмисники можуть використовувати з метою:

- передавання в мережу та поширення вірусів та інших шкідливих програм;
- перехоплення та відтворення конфіденційної інформації з метою особистого збагачення або нанесення шкоди приватним чи державним установам;
- збирання адрес електронної пошти з метою розсилання спаму;
- створення перешкод у роботі антивірусних програм, систем моніторингу подій і мережевих екранів;
- стирання або переписування даних із дисків та пошкодження файлів;
- виведення з ладу комп'ютерного та комунікаційного обладнання мережі.

До найбільш поширених відносять такі види атак на ресурси комп'ютерної мережі.

Відмова в обслуговуванні (Denial of Service – DoS) – атака з поодинокого джерела з метою зробити ресурси комп'ютерної мережі недоступними для авторизованих користувачів шляхом перевищення допустимого рівня функціонування операційної системи, додатків або технічних засобів мережі. У переважній більшості DoS-атаки спрямовують на інформаційні сервери: вебсервери, поштові й файлові сервери, DNS-сервери відображення імен тощо. До найпоширеніших DoS-атак відносять: Flood**,** ICMP flood, TCP SYN flood, Identification flood, UDP flood, TCP flood і Ping of Death.

Flood (затоплення) та **ICMP flood** (**flood ping** – потік коротких запитів, що вимагають відповіді) – це атаки, під час яких система отримує велику кількість ICMP- або UDP-пакетів, які не несуть корисної інформації, але перевантажують мережу непродуктивними діями щодо їх аналізу.

TCP SYN flood – атака, що полягає в надсиланні великої кількості запитів на ініціалізацію TCP-з'єднань без їх закриття, що переповнює

інформаційний канал SYN-пакетами, блокує роботу сервера й не дозволяє йому відповідати на запити інших клієнтів.

Identification flood (запит ідентифікації системи) – атака, під час якої мережа постійно отримує запити на ідентифікацію системи. Це знижує продуктивність системи, оскільки аналіз цих запитів і генерування на них відповідей перевантажують процесор.

UDP flood, **TCP flood** і **Ping of Death** – атаки шляхом посилання в мережу великої кількості, відповідно, пакетів UDP, TCP та фрагментованого ICMP- пакета великого обсягу. Це призводить до зв'язування мережевих ресурсів і зависання операційної системи комп'ютера чи сервера (останнім часом використовують рідко).

Загрозу DoS атак можна послабити шляхом конфігурації на маршрутизаторах і міжмережевих екранах функцій **антиспуфінгу** (Spoof – використання фальшивої адреси) – фільтрації пакетів за підозрілими IP- адресами. Ефективним є обмеження обсягу **некритичного трафіку** (non-critical traffic), який проходить мережею (наприклад, обмеження обсягів пакетів ICMP).

Розподілена DDoS-атака (Distributed Denial of Service) – скоординована DoS-атака відразу з багатьох комп'ютерів. Для її організації комп'ютери, що беруть у ній участь, попередньо заражають спеціальними вірусами-хробаками. Заражені комп'ютери за командою зловмисника починають одночасно надсилати запити до атакованого сервера. У результаті сервер не справляється з навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливим. Фахівці вважають DDoS-атаки одними з найскладніших видів мережевих загроз, що можуть паралізувати роботу комп'ютерної мережі.

До найбільш поширених DDoS-атак відносять TCP SYN flood (SYN flooding), TCP flood, UDP flood, ICMP flood та Smurf Attack.

Атаку **Smurf Attack** здійснюють шляхом передавання в мережу з великою кількістю комп'ютерів широкомовних ICMP-повідомлень, підмінивши в них адресу відправника адресою сервера-жертви. Множина

комп'ютерів, які прийняли такі запити, надсилають серверу-жертві пакети у відповідь. У результаті сервер не справляється з навантаженням, тому доступ до атакованого ресурсу стає неможливим.

Найбільш небезпечними є злоякісні програми, що використовують одночасно кілька видів атак. Так, програма **Stacheldracht** дає можливість генерувати лавини **широкомовних коротких запитів** (пінг-запитів) і здійснювати атаки на програмно-апаратні засоби мережі. Змінюючи значення параметрів **бази керуючої інформації** (Management Information Base) на керованих адміністратором вузлах мережі, злоякісна програма дестабілізує їх роботу.

Протидія DDoS атакам передбачає встановлення на міжмережевих екранах спеціалізованих **antiflood-фільтрів** (antiflood-filters), що здатні в реальному часі блокувати за IP-адресами доступ до веб-серверів тих клієнтів, які генерують інтенсивний потік запитів, сформованих за протоколом **HTTP** HyperText Transfer Protocol – протокол передавання гіпертексту). Використовують також резервування розподілених систем, які не припиняють обслуговувати користувачів навіть тоді, коли деякі їхні ресурси стають недоступними.

Сніфер пакетів (Sniffer – перехоплювач) – програма, яка використовує карту мережевого інтерфейсу, що працює в нерозбірливому режимі (promiscuous mode) приймання й дає змогу перехоплювати всі пакети мережі. Зібрані так дані передають для опрацювання на мережевий монітор, призначений для аналізу трафіку мережі. Зловмисник при цьому може видати себе за санкціонованого користувача, перебуваючи в самій організації, або за її межами. Застосування програми дає можливість перехопити будь-який незашифрований, а іноді й зашифрований трафік із метою отримання корисної для зловмисника інформації (паролі, IP-адреси електронної пошти, інформація про структуру мережі тощо).

IP-спуфінг (spoof – обман, підміна) –атака, що передбачає використання зловмисником, який видає себе за санкціонованого користувача, чужої IP- адреси. Її часто застосовують як складову комплексної атаки (наприклад,

DDoS- атаки, для здійснення якої зловмисник розміщує відповідну програму за чужою IP-адресою).

Знизити загрозу IP-спуфінгу можна шляхом жорсткого контролю за правами доступу користувачів із забороною будь-якого трафіку, вихідна адреса якого не є однією з IP-адрес внутрішньої мережі, запровадженню додаткових заходів автентифікації та системи криптографічного захисту. [7][1)]

Вірус (Virus) – шкідлива програма, здатна до впровадження в інші файли комп'ютера, зокрема у файли системних і прикладних програм. В інші комп'ютери вірус може попасти тільки в тілі переданого користувачем файлу. Шкода, яка може бути нанесена системі вірусом, залежить від мети, яку поставив зловмисник при розробці вірусу: від періодичної появи на екрані різноманітних зображень, що заважають користувачу працювати, аж до порушення інформаційної безпеки, втрати даних, руйнування системних програм і втрати працездатності мережі.

Антивірусний захист передбачає виявлення й діагностування вірусного зараження з допомогою програм антивірусного захисту з наступним відновленням працездатності інформаційної системи. Для цього аналізують поведінку як системних, так і прикладних програм, а також перевіряють вміст підозрілих файлів.

Логічні бомби (Logic bombs) – спеціально сконструйований програмний код, який викликає деструктивну роботу програми, що виконують на комп'ютері, зокрема, її повне припинення.

Керовані атаки (War driving) – отримання несанкціонованого доступу до серверів комп'ютерних мереж, що використовують безпроводові технології. Для проникнення в мережу застосовують антени та безпроводові мережеві адаптери.

Спам (Spam) – це вид атаки за допомогою електронної пошти. Велика кількість листів, яку надсилає зловмисник на певні адреси електронної

[1)] [7] Політика безпеки для Internet. [Електронний ресурс]. Режим доступу : https://lektsii.org/8-12435.html. Загол. з екрана. Дата звернення 12.11.2019.

пошти, унеможливлює роботу поштових скриньок і поштових серверів. Разом із непотрібною інформацією зловмисники засобами електронної пошти можуть надсилати шкідливі програми й організовувати різні види атак. При цьому зловмисники можуть використовувати бот-мережі (будуть описані нижче), генерувати адресу відправника й теми його листа з використанням випадкових чисел. Із цим видом атаки складно боротися, тому що Інтернет-провайдер може обмежити кількість листів тільки від одного відправника.

Ін'єкції (Exploit tools) – вид атаки шляхом впровадження шкідливих команд або даних у працюючу систему з метою впливу на її роботу так, щоб отримати доступ до комп'ютера-жертви та даних або дестабілізувати роботу системи в цілому. Найчастіше цей вид атаки зловмисники використовують для формування шпіонських запитів до баз даних, злому веб-сайтів та внесення неправдивої (фейкової) інформації на веб-сторінки, які користуються популярністю певного кола користувачів. Прикладом такого виду атак може бути SQL-ін'єкція (Structured query language), яку використовують зловмисники для зміни параметрів запитів до бази даних.

Програми-шпигуни (програми мережевої розвідки) – це вид шкідливих програм, які зловмисник таємно встановлює на комп'ютери мережі з метою збирання секретної інформації про будову та принципи функціонування мережі, виявлення проксі-серверів, аналізу їх роботи, перехоплення й аналізу пакетів та інших даних. Зібрану шпигунськими програмами інформацію використовують, здебільшого, для організації наступних атак. Розрізняють такі види шпигунських програм:

- сканери портів, які записують інформацію, що передають через порти комп'ютера, під'єднані до мережевого адаптера, модема, принтера тощо (програма **NeoTrace**);
- клавіатурні та екранні шпигуни, які копіюють інформацію, що вводять у комп'ютер із клавіатури (програма **Hook Dump**), або виводять на екран комп'ютера (програма **Ghost spy**);
- модемні та мережеві кіберрозвідники, які автоматично записують

телефонні розмови в режимі диктофона, копіюють записи через телефонну лінію або звукову карту (програми **Modem spy**, **Flexispy**, **Mobile Spy** й **Mobistealth**), здійснюють моніторинг мережевого трафіку, електронної пошти, веб-сайтів тощо;

– програми для перехоплення й перенаправлення трафіку з метою направити трафік атакованого комп'ютера за фальшивою адресою. У переважній більшості це здійснюють шляхом формування фальшивої ARP- або DNS-відповіді при надсиланні атакованим комп'ютером широкомовних запитів на відображення імен. Перенаправлення трафіку зловмисник може здійснити також шляхом формування від імені маршрутизатора фальшивого ICMP- повідомлення про зміну маршруту.

Бекдор (back door – чорний хід, люк) – злоякісна програма, яка використовує вразливість програмного забезпечення системи й забезпечує зловмиснику доступ до конфіденційної інформації, розміщеної на віддаленому комп'ютері, а також дає змогу виконувати на ньому несанкціоновані дії. Завдяки бекдору зловмисник може витягнути з інфікованої мережі назву та реквізити підприємства, пароль проксі-сервера, ім'я поштового сервера, паролі, адреси електронної пошти клієнтів тощо.

Зловмисники досить часто для організації атак на ресурси комп'ютерної мережі використовують **бот-мережі** (botnet, зомбі-мережі), до складу яких може входити велика кількість інфікованих комп'ютерів зі встановленими зловмисником шкідливими програмами. До отримання команди від зловмисника бот-мережа знаходиться в сонному стані. Отримавши команду, вона починає виконувати закладені в неї функції, наносячи шкоду ресурсам мережі (розкриття IP-адрес та пароля доступу до інформаційних ресурсів, розповсюдження спаму, здійснення атак на сервери з метою спровокувати відмову в обслуговуванні користувачів тощо). Керування ботом зловмисник може здійснювати як шляхом надсилання відповідного коду на адресу одного з комп'ютерів, так і через веб-сайти з використанням наперед сформованої

URL- адреси (Uniform Resource Locator – інфікований вказівник на ресурс) та з використанням **p2p-**мереж (Peer-to-peer network – мережа рівноправних вузлів).

При застосуванні технології однорангового розподілення ресурсів p2p забезпечують безпосередній обмін повідомленнями між кінцевими системами, якими можуть бути персональні комп'ютери, під'єднані до публічної мережі. При цьому для пошуку необхідних ресурсів p2p-технологія передбачає використання як децентралізованого, так і централізованого каталогів, або системи запитів на потрібний ресурс. Найчастіше бот-мережі використовують для організації DDoS-атак.

Для підготовлення атак на інформаційні та програмно-апаратні ресурси мережі зловмисники часто використовують методи та засоби моніторингу відкритих та відносно-відкритих джерел і соціальної інженерії, які були розглянуті вище.

1.5 Виявлення атак на ресурси комп'ютерної мережі

Обов'язки з виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі покладені на адміністратора безпеки, який є відповідальним за безпеку мережі в цілому. Ці функції може також виконувати системний адміністратор. Одним із найбільш поширених адміністративних методів боротьби з атакуючими програмами є заборона тих програм, які не мають дозволу на виконання в конкретній інформаційній системі. Список дозволених програм формує адміністратор мережі.[6][1)]

Мережеві монітори (sniffers), типовими представниками яких є **Wireshark** і **Microsoft Network Monitor**, надають адміністратору засоби для слідкування за мережевим трафіком, відфільтровування пакетів та перегляду

[1)] [6] 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.

їх змісту, збирання статистичної інформації про роботу пристроїв мережі. Отримані дані заносять у журнал реєстрації. Висновки про можливі загрози мережевий адміністратор робить на основі аналізу характеристик мережевого трафіку та записів у журналах реєстрації. Це тривалий і трудомісткий процес, який є ефективним для невеликих локальних мереж, але не завжди приносить очікуваний ефект при моніторингу мережі великого підприємства.

Для централізованого моніторингу подій у режимі реального часу в комп'ютерних мережах використовують системи **управління інформацією та повідомленнями безпеки** (Security Information and Event Management – SIEM). SIEM-системи забезпечують уповноважений персонал та користувачів мережі інформацією про її стан та дають змогу, у відповідності до заданих правил та налаштувань, оперативно реагувати на виникнення загрозливих ситуацій.

Серед сучасних програмно-апаратних засобів моніторингу атак на інформаційну систему широкого застосування знайшли **системи виявлення атак** (Intrusion detection system – IDS) та **системи запобігання втручань** (Intrusion prevention system – IPS). Основним призначенням цих систем є виявлення фактів несанкціонованого доступу до корпоративної мережі та прийняття відповідних заходів протидії: інформування адміністратора з мережевої безпеки про факт вторгнення, припинення з'єднання та переустановлення міжмережевого екрану для блокування подальших дій зловмисника. Ці системи містять спеціальні програми та процедури, призначені для аналізу в режимі реального часу великого обсягу мережевого трафіку з метою виявлення та запобігання атакуючих дій зловмисників. Їх використання дає змогу вирішити цілий ряд завдань, які забезпечують інформаційну безпеку мережі.

Існуючі системи виявлення атак відрізняються між собою як за типом подій, які вони здатні виявляти, так і за методами виявлення атак. До основних функцій цих систем відносять:

– аналіз системної конфігурації та виявлення вразливостей мережі;

– моніторинг користувацької, мережевої та системної активності в

мережі;

– контроль цілісності файлів та інших ресурсів інформаційної системи;
– розпізнавання ознак атакуючих дій, що можуть нести загрозу програмно-апаратним ресурсам мережі;
– контроль за роботою та станом компонентів інформаційної системи й реєстрація інформації про порушення безпеки;
– аналіз характерних ознак, що можуть свідчити про проведення атакуючих дій, а також здійснення їх статистичного опрацювання;
– надання послуг адміністратору мережі в питаннях інформаційної безпеки.

Крім функцій моніторингу та аналізу атакуючих дій та виявлення інцидентів IDS виконують додаткові функції, до яких відносять:

– передавання інформації про виявлені атаки в систему централізованого моніторингу подій;
– повідомлення адміністратору даних про виявлені інциденти інформаційної безпеки по декількох каналах: електронна пошта, SNMP- повідомлення, системний журнал, консоль управління системою IDS;
– генерування звітів за вказаними подіями.

Системи IPS доповнюють системи IDS такими важливими функціями:

– блокування атаки (розірвання з'єднання з користувачем, який порушує політику безпеки, блокування доступу до ресурсів, вузлів (хостів), додатків);
– змінювання конфігурації мережевих пристроїв для запобігання подальших атак;
– видалення інфікованих файлів і відправлення отримувачу лише очищених файлів.

Виникнення загроз для програмно-апаратних компонентів мережі може бути визначене системою виявлення атак двома методами:

– виявлення загроз (misuse detection);
– виявленням аномалій (anomaly detection).

Метод виявлення загроз передбачає наявність формалізованого опису характерних ознак різних видів атак та їх модифікацій і ґрунтується на порівнянні сигнатур, другий ґрунтується на знанні опису очікуваної поведінки контрольованих об'єктів системи. **Сигнатура** – це послідовність байтів, яка є характерною для певного виду загрози. Якщо програма виявлення атак при скануванні файлів інформаційної системи виявляє сигнатуру відомого виду загрози, це кваліфікується як її наявність у мережі. Після виявлення загрози система захисту може запропонувати видалити пошкоджений файл або спробувати його відновити шляхом видалення загрозливої послідовності байтів. Таким чином, метод порівняння сигнатур дає можливість ефективно виявляти шкідливі програми з відомими ознаками, але не дає змоги виявити нові, ще не описані програми.

Метод аномалій ґрунтується на припущенні, що відхилення поведінки контрольованого об'єкта від описаної норми свідчить про наявність ворожих дій. Прикладами аномалій у роботі мережі є різке збільшення інтенсивності мережевого трафіку, перевищення кількістю з'єднань між вузлами мережі заданої норми, високе завантаження центрального процесора та серверів, використання пристроїв, які, зазвичай, не використовують. Метод аномалій дає можливість виявляти нові атаки, але вимагає детального багатопараметричного опису поведінки об'єктів інформаційної системи. Більшість сучасних систем виявлення атак поєднує обидва методи й дає змогу боротися з певним спектром шкідливих програм: вірусами, мережевими хробаками, троянами тощо.

Слід зазначити, що системи IDS/IPS не роблять інформаційну систему цілком безпечною, проте вони є корисним доповненням до міжмережевого екрану, який згідно з політикою мережевої безпеки створює бар'єр для забороненого типу трафіку. Вони можуть виявити атаки, які обійшли брандмауер, і запобігти нанесенню шкоди інформаційній системі. Вибір системи виявлення атак залежить від особливостей побудови та функціонування інформаційної системи й вимог політики мережевої безпеки.

Важливим є використання методів запобігання можливим атакуючим діям зловмисників на ресурси комп'ютерних мереж. Методи соціального інжинірингу для боротьби з інцидентами передбачають використання механізму оповіщення користувачів мережі Інтернет про злоякісні веб-сайти, які спеціально створюють зловмисники для збору конфіденційних даних із метою підготовки атак на інформаційні ресурси мережі. Так, антифішинг здійснюють шляхом введення в популярні браузери (**Microsoft Internet Explorer**, **Firefox** тощо) спеціальних програмних додатків – **плагінів** (Plug-in – під'єднувати), що попереджають користувачів про їх звертання до підроблених або підозрілих веб-сайтів.

2 АНАЛІЗ ПРОТОКОЛІВ ПОБУДОВИ VPN

2.1 Класифікація VPN-технологій

Так історично склалося, що під одним терміном VPN (Virtual Private Network − віртуальна приватна мережа) розуміються дві різні по своїх цілях, завданнях і використовуваних алгоритмах інформаційні технології [8][1], [9][2]:

– технології забезпечення гарантованої якості обслуговування для корпоративного трафіку, що транспортується через глобальні мережі.
– технології забезпечення інформаційної безпеки корпоративного трафіку передаваного через глобальні мережі.

До першої групи VPN-технологій відносяться різні спеціалізовані технології управління QOS (RSVP, DiffServ, MPLS), а також деякі базові мережеві технології з вже вбудованими елементами QOS (ATM, Frame relay).

Друга група VPN-технологій виконує функції авторизації абонентів корпоративних мереж і функції криптографічного захисту передаваних даних. Як правило, технології цієї групи є різними реалізаціями механізму інкапсуляції стандартних мережевих пакетів канального (технології PPTP, L2F, L2TP), мережевого (технології SKIP, IPSec/IKE) і вище розміщених рівнів моделі OSI (технології SOCKS, SSL/TLS).

Слід зазначити, що існують різні види реалізації VPN-тунелювання: VPN на базі маршрутизаторів; VPN на базі мережевих операційних систем; VPN на базі міжмережевих екранів; VPN на базі спеціалізованого програмного забезпечення. [10][3]

---

[1] [8] Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. 714с., іл.

[2] [9] А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [Навчальний посібник] (Лист МОНУ №1/11-8052 ВІД 28.05.12Р.) Львів, «МАГНОЛІЯ 2006», 2013. 256 С.

[3] [10] Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. К 63 Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька // К.: Компрінт, 2017. 821с.

Більшість технологій VPN-шифрування розроблені Національним Інститутом Стандартів і Технологій, проте уряд США вже багато років намагається зламати і обійти їх.

Проаналізуємо основні відмінності між протоколами VPN і тим, як вони впливають на користувачів. [11][1)]

2.2 Протокол PPTP

Протокол PPTP розроблений асоціацією, очолюваною Microsoft і є стандартом VPN з моменту створення. Це перший VPN-протокол, підтримуваний Windows, безпека забезпечується різними методами аутентифікації, наприклад, найпоширеніший з них MS-CHAP v2.

Кожен пристрій, що працює з VPN, підтримує PPTP за замовчуванням, і оскільки його дуже просто налаштувати, цей протокол продовжує залишатися найпопулярнішим серед власників компаній і VPN-провайдерів. Це також найшвидший протокол, оскільки для його реалізації вимагається менше всього обчислень.

Проте, хоча за замовчуванням використовується 128-бітове шифрування, є визначені уразливості безпеки, одна з найсерйозніших − неінкапсульована автентифікація MS-CHAP v2. Із-за цього PPTP можна зламати протягом двох днів. І хоча ця проблема була виправлена Microsoft, все ж рекомендується використовувати протоколи SSTP або L2TP для підвищеної безпеки.

Звичайно ж, такий низький захист PPTP обумовлює те, що розшифрування цього протоколу − стандартна процедура на сьогодні. Також Агентство національної безпеки США розшифровує не лише поточний трафік, але і дані, які були зашифровані ще в той час, коли протокол PPTP вважався безпечним.

Переваги:

[1)] [11] А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) Львів, «Магнолія 2006», 2014. 312 с.

– Висока швидкість
– Вбудований клієнт практично на усіх платформах
– Просте налаштування

Недоліки:

– Протокол зламаний Агентством національної безпеки США
– Не гарантує повну безпеку

2.3 Протоколи L2TP L2TP/IPSec

Протокол другого рівня L2TP, на відміну від інших протоколів VPN, не шифрує і не захищає дані. Через це часто використовуються додаткові протоколи, зокрема IPSec, за допомогою якого дані шифруються ще до передачі. Усі сучасні пристрої і системи, сумісні з VPN, мають вбудований протокол L2TP/IPSec. Установка і налаштування здійснюються легко і не займає багато часу, проте може виникнути проблема з використанням порту UDP 500, який блокується фаєрволами (мережевими екранами) NAT (Network Address Translation). Отже, якщо протокол використовується з брандмауером, може бути потрібна переадресація портів.

Не відомо про будь-які критичні вразливості IPSec, і при правильному застосуванні, цей протокол забезпечує повний захист конфіденційних даних. Проте, Едвард Сноуден (американський програміст, системний адміністратор, колишній працівник ЦРУ та АНБ США) відмічає, що цей протокол не такий безпечний. Джон Гілмор, засновник і фахівець з безпеки Electric Frontier Roundation, заявляє, що Агентство національної безпеки США навмисно послабляє протокол.

Переваги:

– Вважаються відносно безпечними протоколами
– Доступні в більшості систем і майже на усіх пристроях
– Просте налаштування

Недоліки:

– Повільніші, ніж OpenVPN
– Захист порушений Агентством національної безпеки США
– Складно використовувати за наявності блокування з боку брандмауера
– Агентство національної безпеки США навмисно послабляє протокол.

2.4 Протокол OpenVPN

OpenVPN – відносно нова технологія з відкритим кодом, використовує протоколи SSLv3/TLSv1 і бібліотеку OpenSSL, а також деякі інші технології, що в цілому забезпечує надійне і потужне VPN-рішення для користувачів. Протокол гнучкий в налаштуванні і краще всього працює через UDP-порт, проте його можна налаштувати для роботи з будь-яким іншим портом.

Інша значуща перевага полягає в тому, що бібліотека OpenSSL підтримує різні алгоритми шифрування, у тому числі 3DES, AES, Camellia, Blowfish, CAST-128, хоча провайдери VPN використовують практично виключно тільки Blowfish або AES. За замовчуванням використовується 128-бітне шифрування Blowfish. Зазвичай воно вважається безпечним, проте були відмічені деякі вразливості.

Якщо говорити про шифрування, AES − це найновіша технологія і вона вважається «золотим стандартом». На даний момент не відомо про вразливості цієї системи, так що вона навіть використовується урядом і секретними службами США для захисту даних. AES краще справляється з об'ємними файлами, ніж, наприклад, Blowfish, оскільки розмір блоку складає 128 біт, тоді як у Blowfish − 64 біта.

Передусім, швидкість OpenVPN залежить від рівня шифрування, хоча зазвичай вона вища, ніж у IPSec. OpenVPN підключення, використовуване за замовчуванням більшістю VPN-провайдерів не підтримується на будь-яких платформах. Проте активно розробляються додатки від сторонніх виробників, зокрема для Android і iOS.

Установка складніша, ніж для L2TP/IPSec і PPTP, зокрема коли використовується загальне застосування для OpenVPN. Потрібно викачати і встановити клієнт, та ще і згаяти час на зміну файлів налаштування. Деякі VPN-провайдери пропонують заздалегідь налагоджені клієнти.

Проте, з урахуванням усіх чинників і інформації, представленої Едвардом Сноуденом, здається, що протокол OpenVPN є найбезпечнішим на даний момент. Також передбачається, що він захищений від втручання Агентства національної безпеки США, оскільки протокол використовує експериментальні методи шифрування. Без сумніву, ніхто не знає усіх можливостей Агентства національної безпеки, проте, швидше за все це єдиний по-справжньому безпечний протокол на сьогодні. [12][1)]

Переваги:

– дозволяє обходити більшість фаєрволів;
– гнучке налаштування;
– відкритий код − може швидко адаптуватися до нових небезпек;
– різні алгоритми шифрування;
– висока міра безпеки.

Недоліки:

– складно налаштувати;
– потрібне стороннє ПЗ;
– підтримка комп'ютерів непогана, але на мобільних пристроях протокол працює не кращим чином.

2.5 Протокол SSTP

Вперше цей протокол був представлений компанією Microsoft в SP1 для Windows Vista, на сьогодні цей протокол доступний для Linux, RouterOS, але

[1)] [12] А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) Львів, «Магнолія 2006», 2014. 312 с.

переважно розрахований для роботи в Windows. Він використовує SSL v3, так що має практично ті ж переваги, що і у OpenVPN, зокрема, можливість обходити фаєрволи NAT. SSTP − це стабільний і простий у використанні протокол, інтегрований в Windows.

Проте, усіма правами на нього володіє Microsoft. Відомо, що гігант індустрії активно працює із спецслужбами.

Переваги:

– дозволяє обходити більшість фаєрволів
– рівень безпеки залежить від вибраного шифру, зазвичай він досить високий
– хороша взаємодія з ОС Windows
– підтримка Microsoft

Недоліки:

– оскільки протоколом володіє компанія Microsoft, перевірити або поліпшити його неможливо
– працює тільки на платформі Windows

2.6 Протокол IKEv2

IKEv2 – протокол обміну ключами, 2 версії, розроблений Cisco і Microsoft, він вбудований в Windows 7 і наступні версії. Протокол допускає модифікації з відкритим кодом, зокрема для Linux і інших платформ, також підтримуються пристрої Blackberry.

Він добре підходить для установки автоматичного VPN-підключення, якщо інтернет-з'єднання періодично розривається. Користувачі мобільних пристроїв можуть скористатися ним як протоколом для безпровідних мереж за замовчуванням − дуже гнучкий і дозволяє без зусиль перемикати мережі. Крім того, прекрасно підійде для користувачів Blackberry − це один з небагатьох протоколів, з підтримкою подібних пристроїв. Хоча IKEv2 доступний на меншій кількості платформ в порівнянні з, наприклад, IPSec, він вважається

досить хорошим протоколом з точки зору стабільності, безпеки і швидкості роботи.

Переваги:

– Висока міра безпеки − підтримка різних шифрів, зокрема 3DES, AES, AES 256.
– Підтримує пристрої Blackberry.
– Стабільно підключається після розриву з'єднання або зміни мереж
– Просто встановити і настроїти, принаймні, для користувача
– Швидший, ніж L2TP, PPTP і SSTP

Недоліки:

– Порт UDP 500 блокується простіше, ніж рішення на основі SSL, як, наприклад, SSTP або OpenVPN

Найбільш безпечним шифром для VPN вважається AES, особливо характерне те, що саме цим шифруванням користується уряд США. Проте, є певні причини сумніватися в надійності цього шифру.

SHA − 1, SHA − 2, RSA і AES − усі вони сертифіковані Національним інститутом стандартів і технологій США (НІСТ), який тісно пов’язаний з Агентством національної безпеки в розробці шифрів. 17 вересня 2013 року зросла недовіра до шифрів, коли RSA Security порекомендували своїм користувачам утриматися від використання конкретного алгоритму, що містить вразливості, навмисно впроваджені в нього Агентством національної безпеки США. Більше того, з'ясувалося, що стандарт, розроблений НІСТ, Dual EC DRBG, багато років був небезпечний. Це було відмічено Університетом технології в Нідерландах в 2006 році. Проте, незважаючи на усі ці проблеми і складнощі, НІСТ є лідером в індустрії, у тому числі і через те, що відповідність стандартам НІСТ є обов'язковою умовою для отримання контракту з урядом США. Стандарти НІСТ використовуються по всьому світу, в усіх сферах бізнесу і виробництва, де потрібний захист особистих даних, зокрема, в індустрії VPN, − і ці проблеми є значущими для усіх. Багато виробників покладаються на ці стандарти і не бажають визнавати проблему. Єдина компанія, Silent Circle, закрила

свій сервіс Silent Mail, замість того, щоб дозволити скомпрометувати його, потім вони відійшли від стандартів HICT в листопаді 2013 року.

В матеріалі Едварда Сноудена йдеться про те, що була розроблена нова програма «Cheesy Name», спрямована на визначення ключів шифрування, які можуть бути зламані суперкомп'ютерами в Штабі урядового зв'язку. Виявляється, що сертифікати, захищені 1024-бітовим шифруванням, слабші, ніж передбачалося, їх можна досить швидко дешифрувати, набагато швидше, ніж очікувалося. Після того, як шифр буде зламаний, це торкнеться усіх користувачів, оскільки можна буде дешифрувати усі дані. Внаслідок цього, будуть зламані системи шифрування, засновані на подібних ключах, у тому числі і TLS і SSL. Це дуже сильно вплине на трафік HTTPS. Проте, OpenVPN ці зміни не торкнуться, оскільки протокол змінює тимчасові ключі шифрування. Для кожного обміну даними генерується новий ключ. Навіть якщо хтось отримав ключ до сертифікату, дешифрувати усі дані неможливо. При атаці «людина посередині» (MitM) можливо перехватити з'єднання OpenVPN, проте потрібно дістати доступ до ключа. З моменту, як стало відомо про вразливості в 1024-бітовому шифруванні, багато провайдерів перейшли на 2048-ми або навіть 4096-бітне.

Таким чином, найбезпечніший протокол VPN − це OpenVPN. PPTP − дуже небезпечний протокол. Його зламали спецслужби і навіть Microsoft відмовилися від його підтримки, так що на сьогодні слід його уникати. І хоча зручність налаштування та висока сумісність привертає до нього увагу, все ж таки краще скористатися L2TP/IPSec.

Якщо не йдеться про дійсно важливі дані, L2TP/IPSec − це те, що потрібно, хоча цей протокол і ослаблений і скомпрометований. Проте, якщо потрібний швидкий і зручний в налаштуванні VPN, який не вимагає установки додаткового ПЗ, він прекрасно підійде, особливо з урахуванням того, що VPN для мобільних пристроїв підтримується не кращим чином.

Не дивлячись на те, що потрібно буде встановлювати сторонні застосування, OpenVPN − кращий протокол у будь-якому випадку.

IKEv2 теж працює швидко і безпечно, і якщо використовується у поєднанні з іншими засобами забезпечення безпеки, він може прекрасно підійти для користувачів мобільних пристроїв, зокрема завдяки автоматичному відновленню підключення. Крім того, це один з небагатьох протоколів з підтримкою пристроїв Blackberry.

SSTP пропонує практично ті ж переваги, що і OpenVPN, проте він працює тільки на платформі Windows. Проте, підтримка провайдерів обмежена, по-перше, із-за підтримки систем, по-друге, через те, що компанія Microsoft відома давньою співпрацею з Агентством національної безпеки, так що рівень довіри мінімальний.

Отже, при можливості потрібно використовувати OpenVPN, для мобільних пристроїв підійде IKEv2.

3 СТЕК ПРОТОКОЛІВ IPSEC

3.1 Розподіл функцій між протоколами IPSec

Протокол IPSec в стандартах Інтернету називають системою. IPSec – це погоджений набір відкритих стандартів, що має сьогодні цілком окреслене ядро, яке в той же час може бути досить просто доповнене новими функціями і протоколами. [13][1)]

Ядро IPSec складають три протоколи:

– AH (Authentication Header – заголовок автентифікації) гарантує цілісність і автентичність даних;
– ESP (Encapsulating Security Payload – інкапсуляція зашифрованих даних) шифрує дані, що передаються, забезпечуючи конфіденційність, може також підтримувати автентифікацію і цілісність даних;
– IKE (Internet Key Exchange – обмін ключами Інтернету) вирішує допоміжну задачу автоматичного надання кінцевим точкам захищеного каналу секретних ключів, необхідних для роботи протоколів автентифікації і шифрування даних.

Як видно з короткого опису функцій, можливості протоколів AH і ESP частково перекриваються (табл. 1).

Таблиця 1 – можливості протоколів AH і ESP

Виконувані функції	Протокол	
Забезпечення цілісності	AH	ESP
Забезпечення автентичності		
Забезпечення конфіденційності		
Розподіл секретних ключів	IKE	

У той час як AH відповідає тільки за забезпечення цілісності і автентифікації даних, ESP може шифрувати дані і, крім того, виконувати функції протоколу AH (хоча автентифікація і цілісність забезпечуються ним в дещо

[1)] [13] В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципи, технологи, протоколи: Ученик для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.

скороченому вигляді). ESP може підтримувати функції шифрування і автентифікації/цілісності в будь-яких комбінаціях, тобто або всю групу функцій, або тільки автентифікацію/цілісність, або тільки шифрування.

Поділ функцій захисту між протоколами AH і ESP викликано застосованою у багатьох країнах практикою обмеження експорту і/або імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з цих протоколів може використовуватися як самостійно, так і одночасно з іншим, так що в тих випадках, коли шифрування через діючі обмеження застосовувати не можливо, систему можна постачати тільки з протоколом AH. Подібний захист даних у багатьох випадках виявляється недостатнім. Приймаюча сторона отримує лише можливість перевірити, що дані були відправлені саме тим вузлом, від якого вони очікуються, і дійшли в тому вигляді, в якому були відправлені. Однак від несанкціонованого перегляду даних на шляху їх просування по мережі протокол AH захистити не може, тому що не шифрує їх. Для шифрування даних необхідний протокол ESP.

3.2 Безпечна асоціація

Для того, щоб протоколи AH і ESP могли виконувати свою роботу із захисту даних, що передаються, протокол IKE встановлює між двома кінцевими точками логічне з'єднання (рис. 1), яке в стандартах IPSec носить назву безпечної асоціації (Security Association, SA).

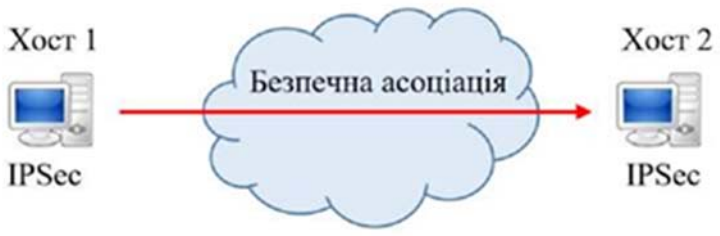

Рисунок 1 – Безпечна асоціація

Стандарти IPSec дозволяють кінцевим точкам захищеного каналу використовувати єдину безпечну асоціацію для передачі трафіку всіх взаємодіючих через цей канал хостів або створювати для цієї мети довільне число безпечних асоціацій, наприклад по одній на кожне TCP-з'єднання. Це дає можливість вибирати потрібну ступінь деталізації захисту – від однієї загальної асоціації для трафіку безлічі кінцевих вузлів до індивідуально налаштованих асоціацій для захисту кожної програми.

Безпечна асоціація в протоколі IPSec являє собою односпрямоване (симплексне) логічне з'єднання, тому, якщо потрібно забезпечити безпечний двосторонній обмін даними, необхідно встановити дві безпечні асоціації. Ці асоціації в загальному випадку можуть мати різні характеристики: наприклад, в одну сторону при передачі запитів до бази даних досить лише автентифікації, а для зворотних даних, що несуть цінну інформацію, додатково можна забезпечити конфіденційність.

Встановлення безпечної асоціації починається зі взаємної автентифікації сторін, тому що всі заходи безпеки втрачають сенс, якщо дані передаються або приймаються не тією особою або не від тієї особи. Параметри SA визначають, який з двох протоколів, AH або ESP, буде застосовуватися для захисту даних, які функції буде виконувати протокол (наприклад, можна виконувати тільки автентифікацію і перевірку цілісності, а можна, крім того, ще й забезпечувати конфіденційність). Дуже важливими параметрами безпечної асоціації є також секретні ключі, що використовуються в роботі протоколів AH і ESP.

Протокол IPSec допускає як автоматичне, так і ручне встановлення безпечної асоціації. При ручному способі адміністратор конфігурує кінцеві вузли так, щоб вони підтримували узгоджені параметри асоціації, включаючи секретні ключі. При автоматичній процедурі встановлення SA протоколи IKE, що працюють по різні боки каналу, вибирають параметри в ході переговорного процесу. Для кожного завдання, що вирішуються протоколами AH і ESP, пропонується кілька схем автентифікації і шифрування (рис. 2). Це робить протокол IPSec дуже гнучким засобом.

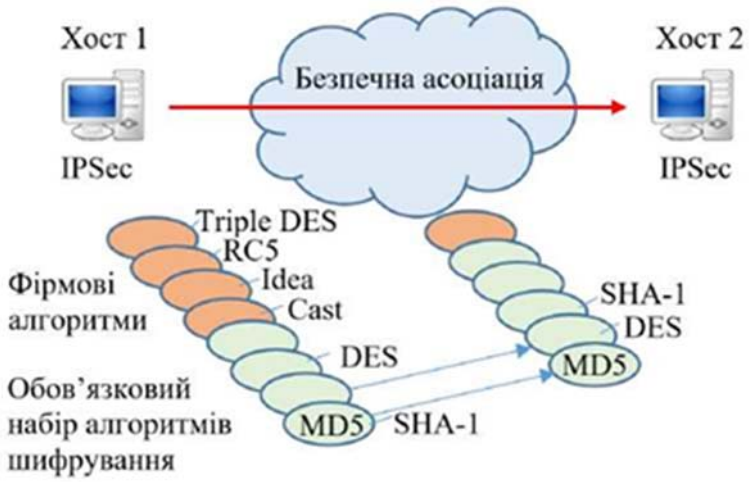

Рисунок 2 – Узгодження параметрів в протоколі ESP

Для забезпечення сумісності в стандартній версії IPSec визначено певний обов'язковий «інструментальний» набір; зокрема, для автентифікації даних завжди може бути використана одна з стандартних дайджест-функцій MD5 або SHA-1, а в число алгоритмів шифрування неодмінно входить DES. При цьому виробники продуктів, в яких використовується IPSec, можуть розширювати протокол шляхом включення інших алгоритмів автентифікації і симетричного шифрування. Наприклад, багато реалізацій IPSec підтримують популярний алгоритм шифрування Triple DES, а також порівняно нові алгоритми: Blowfish, Cast, CDMF, Idea, RC5.

3.3 Транспортний і тунельний режими

Протоколи AH і ESP можуть захищати дані в двох режимах: транспортному і тунельному. У транспортному режимі передача IP-пакета через мережу виконується за допомогою оригінального заголовка цього пакета, а в тунельному режимі вихідний пакет поміщається в новий IP-пакет, і передача даних по мережі виконується на підставі заголовка нового IP-пакету.

Застосування того чи іншого режиму залежить від вимог, що висуваються до захисту даних, а також від ролі, яку відіграє в мережі вузол, що завершає захищений канал. Так, вузол може бути хостом (кінцевим вузлом) або шлюзом (проміжним вузлом). Відповідно є три схеми застосування протоколу IPSec:

– хост-хост;
– шлюз-шлюз;
– хост-шлюз.

У схемі «хост-хост» захищений канал, або, що в даному контексті одне і те ж, безпечна асоціація, встановлюється між двома кінцевими вузлами мережі (рис. 2). Тоді протокол IPSec працює на кінцевих вузлах і захищає дані, що передаються від хоста 1 до хоста 2. Для схеми хост-хост найчастіше використовується транспортний режим захисту.

У відповідності зі схемою шлюз-шлюз захищений канал встановлюється між двома проміжними вузлами, так званими шлюзами безпеки (Security Gateway, SG), на кожному з яких працює протокол IPSec. Захищений обмін даними може відбуватися між будь-якими двома кінцевими вузлами, підключеними до мереж, які розташовані позаду шлюзів безпеки. Від кінцевих вузлів підтримка протоколу IPSec не потрібна, вони передають свій трафік в незахищеному вигляді через внутрішні мережі підприємств, які заслуговують на довіру. Трафік, що направляється в загальнодоступну мережу, проходить через шлюз безпеки, який і забезпечує його захист за допомогою протоколу IPSec. Шлюзам доступний тільки тунельний режим роботи.

Схема хост-шлюз часто застосовується при віддаленому доступі. В цьому випадку захищений канал прокладається між віддаленим хостом, на якому працює протокол IPSec, і шлюзом, який захищає трафік для всіх хостів, що входять у внутрішню мережу підприємства. Цю схему можна ускладнити, створивши паралельно ще один захищений канал – між віддаленим хостом і будь-яким хостом, що належить внутрішній мережі, що захищається шлюзом

(рис. 3). Таке комбіноване використання двох безпечних асоціацій дозволяє надійно захистити трафік у внутрішній мережі.

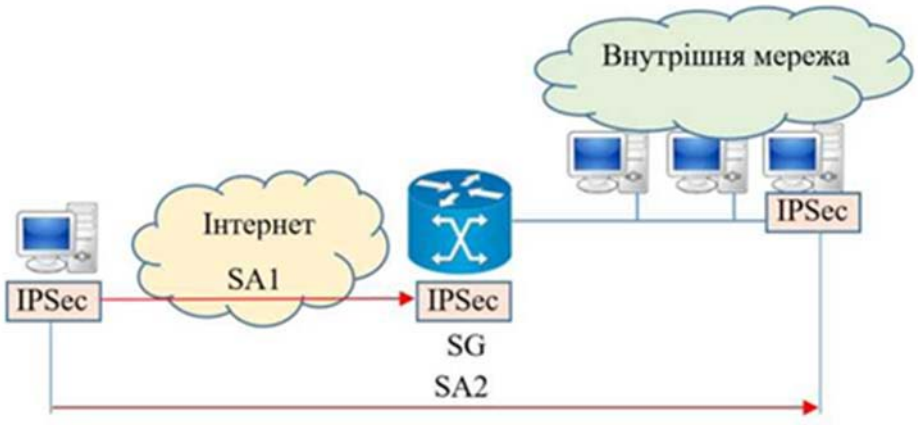

Рисунок 3 – Схема захищеного каналу хост-шлюз

3.4 Протоколи IPSec

Протокол AH дозволяє приймаючій стороні переконатися, що:

– пакет був відправлений стороною, з якою встановлена безпечна асоціація;
– вміст пакету не був спотворений в процесі його передачі по мережі;
– пакет не є дублікатом вже отриманого пакета.

Дві перші функції обов'язкові для протоколу AH, а остання вибирається за бажанням при встановленні асоціації. Для виконання цих функцій протокол AH використовує спеціальний заголовок (рис. 4).

Рисунок 4 – Структура заголовку протоколу AH

В полі наступного заголовка (Next Header) вказується код протоколу більш високого рівня, тобто протоколу, повідомлення якого розміщено в полі даних IP- пакета. Швидше за все, ним буде один з протоколів транспортного рівня (TCP або UDP) або протокол ICMP, але може зустрітися і протокол ESP, якщо він використовується в комбінації з AH.

В полі корисне навантаження (Payload Length) міститься довжина заголовка AH.

Індекс параметрів безпеки (Security Parameters Index, SPI) використовується для зв'язку пакета з передбаченою для нього безпечною асоціацією.

Поле порядкового номера (Sequence Number, SN) вказує на порядковий номер пакета і застосовується для захисту від його зловмисного відтворення (коли третя сторона намагається повторно використовувати перехоплені захищені пакети, відправлені реально автентифікованим відправником). Відправник послідовно збільшує значення цього поля в кожному новому пакеті, що передається в рамках даної асоціації, так що дублікат виявиться приймаючою стороною (якщо, звичайно, в рамках асоціації буде активована функція захисту від зловмисного відтворення). Однак, в будь-якому випадку у функції протоколу AH не входить відновлення загублених і упорядкування вхідних пакетів – він просто відкидає пакет, коли виявляє, що аналогічний пакет вже отримано.

Поле даних автентифікації (Authentication Data), яке містить значення перевірки цілісності (Integrity Check Value, ICV), служить для автентифікації і перевірки цілісності пакету. Це значення, зване також дайджестом, обчислюється за допомогою однієї з двох обов'язково підтримуваних протоколом AH односторонніх функцій (One-way function, OWF) MD5 або SAH-1, але може використовуватися і будь-яка інша функція, про яку сторони домовилися в ході встановлення асоціації. При обчисленні дайджесту пакета в якості параметра функції OWF виступає симетричний секретний ключ, який був заданий для даної асоціації вручну або автоматично за допомогою протоколу IKE. Так

як довжина дайджесту залежить від обраної функції, це поле має в загальному випадку змінний розмір.

Протокол AH намагається охопити при обчисленні дайджесту якомога більше число полів вихідного IP-пакета, але деякі з них в процесі передачі пакета по мережі змінюються непередбачуваним чином, тому не можуть включатися в автентифіковану частину пакету. Наприклад, цілісність значення поля часу життя (TTL) в приймальній точці каналу оцінити не можна, так як воно зменшується на одиницю кожним проміжним маршрутизатором і ніяк не може збігатися з вихідним. Місцезнаходження заголовка AH в пакеті залежить від того, в якому режимі – транспортному або тунельному – налаштований захищений канал. Результуючий пакет в транспортному режимі виглядає так, як показано на рис. 5.

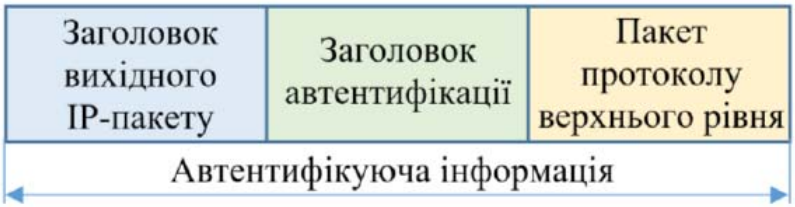

Рисунок 5 – Структура IP-пакету, обробленого протоколом AH в транспортному режимі

При використанні тунельного режиму, коли шлюз IPSec приймає вихідний пакет, що проходить через нього транзитом і створює для нього зовнішній IP- пакет, протокол AH захищає всі поля вихідного пакета, а також незмінні поля нового заголовку зовнішнього пакета (рис. 6).

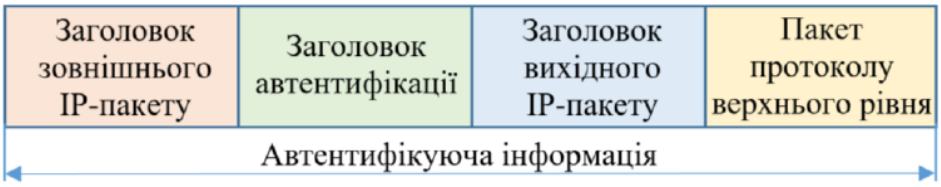

Рисунок 6 – Структура IP-пакету, обробленого протоколом АН в тунельному режимі

Протокол ESP вирішує дві групи завдань. До першої групи належать завдання забезпечення автентифікації і цілісності даних на основі дайджесту, аналогічні завданням протоколу АН, до другої – захист переданих даних шляхом їх шифрування від несанкціонованого перегляду.

Як видно на рис. 7, заголовок ділиться на дві частини, що розділяються полем даних. Перша частина, яка називається заголовком ESP, утворюється двома полями (SP1 і SN), призначення яких аналогічно однойменним полям протоколу АН, і розміщується перед полем даних. Інші службові поля протоколу ESP, які називаються кінцевиком ESP, розташовані в кінці пакета.

Рисунок 7 – Структура IP-пакету, обробленого протоколом ESP в транспортному режимі

Два поля кінцевика – наступного заголовку і дані автентифікації також аналогічні полям заголовка АН. Поле даних автентифікації відсутнє, якщо при встановленні безпечної асоціації прийнято рішення не використовувати засоби протоколу ESP, що стосуються забезпечення цілісності. Крім цих полів кінцевик містить два додаткових поля – заповнювач і довжина заповнювача.

Заповнювач може знадобитися в трьох випадках. По-перше, для нормальної роботи деяких алгоритмів шифрування необхідно, щоб шифрований текст містив кратне число блоків певного розміру. По-друге, формат заголовка ESP вимагає, щоб поле даних закінчувалося на межі чотирьох байтів. І нарешті, заповнювач можна використовувати, щоб приховати дійсний розмір пакета з метою забезпечення так званої часткової конфіденційності трафіку.

На (рис. 7) показано розміщення полів заголовка ESP в транспортному режимі. В цьому режимі ESP не шифрує заголовок IP-пакету, інакше маршрутизатор не зможе прочитати поля заголовка і коректно здійснити просування пакета між мережами. У число шифрованих полів не потрапляють також поля SPI і SN, які повинні передаватися у відкритому вигляді для того, щоб вхідний пакет можна було віднести до певної асоціації і запобігти зловмисному відтворенню пакета.

У тунельному режимі заголовок вихідного IP-пакета поміщається після заголовка ESP і повністю потрапляє в число захищених полів, а заголовок зовнішнього IP-пакета протоколом ESP не захищається (рис. 8).

Рисунок. 8 – Структура IP-пакету, обробленого протоколом ESP в тунельному режимі

Протокол IKE є гібридним протоколом, об'єднуючим методи обміну ключами Oakley і SKEME (Secure Key Exchange Mechanism) у рамках протоколу ISAKMP (Internet Security Association and Key Management Protocol – протокол управління асоціаціями і ключами захисту в мережі Internet).

IPSec можна використовувати і без IKE, але IKE розширює можливості IPSec, забезпечуючи додаткову гнучкість і зручність налаштування стандарту IPSec. Використання протоколу IKE забезпечує наступні переваги:

– виключається необхідність вручну описувати всі параметри асоціації захисту для обох сторін IPSec;
– існує можливість захищеного вибору ключів для використання обома сторонами;
– можна вказати максимальний час існування для асоціації захисту IPSec;
– можна заміняти ключі шифрування в ході сеансів IPSec;
– існує можливість використовувати в рамках IPSec сервіс захисту від відтворення;
– забезпечується підтримка центрів сертифікації, що відкриває широкі можливості управління і масштабування IPSec;
– можлива динамічна автентифікація сторін.

У рамках протоколу IKE використовуються наступні методи і алгоритми:

– ISAKMP. Протокол, який визначає формати корисного навантаження, а також механізми здійснення протокольного обміну ключами і узгодження параметрів асоціацій захисту;
– Oakley. Протокол обміну ключами, що визначає процедуру знаходження автентифікованного матеріалу для ключів;
– SKEME. Протокол обміну ключами, що визначає процедуру знаходження автентифікованного матеріалу для ключів і швидкого оновлення ключів;
– DES. Алгоритм шифрування, використовуваний для шифрування пакетів даних, аби гарантувати конфіденційність даних при обміні IKE. Для IKE використовуються DES з 56-бітовим ключем і 3DES;
– алгоритм Діффі-Хеллмана. Побудований на використанні відкритих ключів, криптографічний протокол, який дозволяє сторонам

створювати спільні секретні ключі, використовуючи незахищені канали зв'язку. Алгоритм Діффі- Хеллмана використовується в рамках IKE для створення сеансових ключів;

– MD5 і SHA (варіант HMAC). Алгоритми хешування, використовуються для автентифікації пакетів даних у процесі обміну IKE;
– підписи RSA. Підписи RSA забезпечують неможливість створення помилкової інформації;

Підтримка сертифікатів X.509v3 відкриває можливість масштабування захищених мереж, забезпечуючи еквівалент цифрової ідентифікаційної карти для мережних пристроїв. Коли двом пристроям потрібний зв'язок, вони обмінюються цифровими сертифікатами, що доводять їх автентичність (тим самим виключається необхідність вручну обмінюватися відкритими ключами взаємодіючих сторін або вручну вказувати спільний ключ для кожної сторони).

У рамках IKE узгоджуються параметри SA як для IKE, так і для IPSec і відповідних процесів формують дві фази, для яких допускаються різні режими. У ході першої фази IKE ведуться переговори про параметри SA IKE. У ході другої фази IKE ведуться переговори про параметри SA IPSec.

3.5 Бази даних SAD і SPD

Протокол IPSec, що працює на хості або на шлюзі, визначає метод захисту, який він повинен застосувати до трафіку, на основі двох типів баз даних, які підтримує IPSec в кожному вузлі:

– безпечних асоціацій (Security Associations Database, SAD);
– політики безпеки (Security Policy Database, SPD).

При встановленні безпечної асоціації, як і при будь-якому іншому логічному з’єднанні, дві сторони приймають ряд угод, що регламентують процес передачі потоку даних між ними. Угоди фіксуються у вигляді набору параметрів. Для безпечної асоціації такими параметрами є, зокрема, тип і режим роботи протоколу захисту (AH або ESP), методи шифрування, секретні ключі,

значення поточного номера пакета в асоціації та інша інформація. Набори поточних параметрів, що визначають всі активні асоціації, зберігаються на обох кінцевих вузлах захищеного каналу у вигляді баз даних безпечних асоціацій (SAD). Кожен вузол IPSec підтримує дві бази SAD – одну для вихідних асоціацій, іншу для вхідних.

Інший тип бази даних – база даних політики безпеки (SPD) – визначає відповідність між IP-пакетами та встановленими для них правилами обробки.

Записи SPD складаються з полів двох типів – полів селектора пакета і полів політики захисту для пакета з даними значенням селектора (рис. 9).

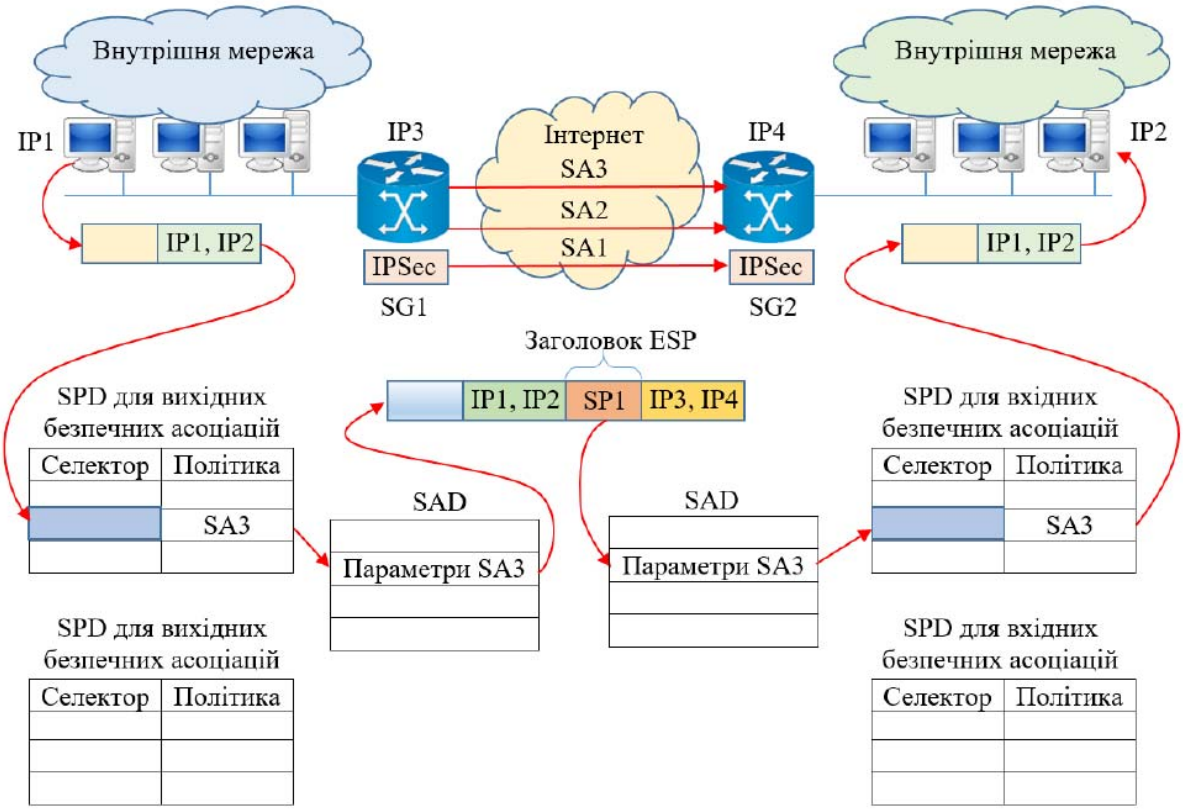

Рисунок 9 – Використання баз даних SAD і SPD

Селектор в SPD включає наступний набір ознак, на підставі яких можна з великим ступенем деталізації виділити захищений потік [14][1)]:

IP-адреси відправника і отримувача можуть бути представлені як у вигляді окремих адрес (індивідуальних, групових або широкотрансляційних), так і діапазонами адрес, заданими за допомогою верхньої і нижньої меж або за допомогою маски;

– порти відправника і отримувача (тобто TCP- або UDP-порти);
– тип протоколу транспортного рівня (TCP, UDP);
– ім’я користувача в форматі DNS або X.500;
– ім’я системи (хоста, шлюзу безпеки і т. п.) в форматі DNS або X.500.

Для кожного нового пакета, що надходить в захищений канал, IPSec переглядає всі записи в базі SPD і порівнює значення селекторів цих записів з відповідними полями IP-пакета. Якщо значення полів збігається з будь-яким селектором, то над пакетом виконуються дії, визначені в полі політики безпеки цього запису. Політика передбачає передачу пакета без зміни, відкидання або обробку засобами IPSec.

В останньому випадку поле політики захисту повинно містити посилання на запис в базі даних SAD, в яку поміщений набір параметрів безпечної асоціації для даного пакета (на рисунку для вихідного пакету встановлено зв’язок SA3). На підставі заданих параметрів безпечної асоціації до пакету застосовується відповідний протокол (на рисунку – ESP), функції шифрування і секретні ключі.

Якщо до вихідного пакету потрібно застосувати деяку політику захисту, але покажчик запису SPD показує, що в даний час немає активної безпечної асоціації з необхідною політикою, то IPSec створює нову асоціацію за допомогою протоколу IKE, поміщаючи нові записи в бази даних SAD і SPD.

[1)] [14] Комплексна безпека інформаційних мережевих систем : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. Тернопіль : Вид-во ТНТУ імені Івана Пулюя , 2016. 256 с.

Бази даних політики безпеки створюються і адмініструються або користувачем (цей варіант більше підходить для хоста), або системним адміністратором (варіант для шлюзу), або автоматично (додатком).

Встановлення зв’язку між вихідним IP-пакетом і заданою для нього безпечною асоціацією відбувається шляхом селекції. Для того, щоб приймаючий вузол IPSec визначив спосіб обробки вхідного пакету (при шифруванні багато ключових параметрів пакету, що відображені в селекторі, виявляються недоступними, а значить, неможливо визначити відповідний запис в базах даних SAD і SPD) в заголовках AH і ESP передбачено поле SPI. У це поле поміщається покажчик на той рядок бази даних SAD, в якому записані параметри відповідної безпечної асоціації. Поле SPI заповнюється протоколом AH або ESP під час обробки пакета в відправній точці захищеного каналу. Коли пакет приходить в кінцевий вузол захищеного каналу, з його зовнішнього заголовка ESP або AH (на рисунку з заголовка ESP) зчитується значення SPI, і подальша обробка пакету виконується з урахуванням всіх параметрів, що задані цим вказівником асоціації.

Таким чином, для розпізнавання пакетів, що відносяться до різних безпечних асоціацій, використовуються:

– на вузлі-відправнику – селектор;

– на вузлі-отримувачі – індекс параметрів безпеки (SPI).

Після дешифрування пакету приймальний вузол IPSec перевіряє його ознаки (що стали тепер доступними) на предмет збігу з селектором запису SPD для вхідного трафіку, щоб переконатися, що не відбулося помилки і виконувана обробка пакету відповідає політиці захисту, що задана адміністратором.

Використання баз SPD і SAD для захисту трафіку дозволяє досить гнучко поєднувати механізм безпечних асоціацій, який передбачає встановлення логічного з’єднання, з датаграмним характером трафіку протоколу IP.

У даному розділі розглянуті протоколи, алгоритми, стандарти, режими і типи перетворень, які використовуються для організації IPSec. Цією інформацією необхідно володіти для успішної побудови мережі IPSec. Налаштування

шифрування може виявитися досить складним завданням. Його рішення повинне починатися з визначення політики захисту IPSec, заснованого на вимогах загальної політики захисту організації.

Двома головними протоколами IPSec є AH, який забезпечує цілісність і автентифікацію даних (але не конфіденційність), і ESP, що забезпечує всі можливості AH, а також конфіденційність даних за допомогою шифрування.

Для автентифікації сторін IPSec і спрощення процесу створення секретних ключів, використовуваних алгоритмами шифрування IPSec, застосовується протокол IKE.

Параметри IPSec і секретні ключі, використовувані в сеансах IPSec, визначають асоціації захисту IPSec, які є однобічними. Параметри асоціацій захисту IPSec зберігаються в динамічній пам'яті в базі даних асоціацій захисту.

4 РЕАЛІЗАЦІЯ ЗАХИСТУ VPN-МЕРЕЖ

4.1 Інфраструктура відкритих ключів

Автентифікація стосовно до обчислювальної системи – це доказ достовірності різних елементів цієї системи при їх взаємодії. Користувач при вході в систему повинен пред'явити системі докази, що він саме той користувач, ідентифікатор якого він вводить. Таким доказом може служити пароль[14][1)].

Документ, отриманий користувачем по електронній пошті, повинен супроводжуватися додатковою інформацією, яка переконує користувача, що документ не був змінений при передачі і що автором цього документа є саме та людина, від імені якого цей лист було надіслано. Тут доказом може служити електронний підпис. Пристрої, що взаємодіють по мережі, мають довести один одному, що жоден з них не підмінений зловмисником з метою відгалуження або прослуховування трафіку. Для цього в протоколі взаємодії цих пристроїв повинна бути передбачена процедура взаємної автентифікації. Взаємна автентифікація потрібна і для організації безпечного сеансу користувача і серверного додатка. Автентифікація може проводитися по відношенню не тільки до окремого користувача, але і до групи користувачів. Методи автентифікації розрізняються залежно від того, що служить автентифікатором, а також від того, яким чином організовано обмін автентифікаційними даними між елементами системи.

Автентифікація з застосуванням цифрових сертифікатів є альтернативою застосуванню паролів і видається природним рішенням в умовах, коли число користувачів мережі (нехай і потенційних) дуже багато. В таких обставинах процедура попередньої реєстрації користувачів, пов'язана з призначенням і зберіганням їх паролів, стає вкрай обтяжливою, небезпечною, а іноді і просто нездійсненною. При наявності сертифікатів мережа, яка дає

[1)] [14] Комплексна безпека інформаційних мережевих систем : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. Тернопіль : Вид-во ТНТУ імені Івана Пулюя , 2016. 256 с.

користувачеві доступ до своїх ресурсів, не зберігає ніякої інформації про своїх користувачів − вони її надають самі в своїх запитах у вигляді сертифікатів, що засвідчують особу користувачів. Сертифікати видаються спеціальними уповноваженими сертифікуючими організаціями (СО) − центрами сертифікації (Certificate Authority, CA). Тому завдання зберігання секретної інформації (закритих ключів) покладається на самих користувачів, що робить це рішення більш масштабованим, ніж варіант з централізованою базою паролів.

Сертифікат являє собою електронну форму, в якій міститься наступна інформація:

– відкритий ключ власника даного сертифікату;
– відомості про власника сертифіката, такі, наприклад, як ім’я, адреса електронної пошти, найменування організації, в якій він працює, і т. п.;
– назва сертифікуючої організації, що видала цей сертифікат;
– електронний підпис сертифікуючої організації, тобто зашифровані закритим ключем цієї організації дані, що містяться в сертифікаті.

Сертифікати можуть бути представлені в трьох формах:

– у відкритій формі сертифікат містить всю інформацію в незашифрованому вигляді;
– в формі з двох частин – відкритій, що містить всю інформацію в незашифрованому вигляді, і закритій, що являє собою відкриту частину, зашифровану закритим ключем сертифікуючої організації;
– в формі з трьох частин – по-перше, відкритій, по-друге, відкритій, але зашифрованій закритим ключем сертифікуючої організації, по-третє, частини, що являє собою перші дві частини, зашифровані закритим ключем власника.

Коли користувач хоче підтвердити свою особистість, він пред’являє свій сертифікат в двох формах: відкритій (тобто такий, в якій він отримав його в сертифікуючій організації) і зашифрованій із застосуванням свого закритого ключа. Сторона, яка проводить автентифікацію, бере з незашифрованого

сертифікату відкритий ключ користувача і розшифровує за допомогою його зашифрований сертифікат. Збіг результату з відкритим сертифікатом підтверджує, що пред'явник дійсно є власником закритого ключа, який відповідає вказаному відкритому.

Потім за допомогою відомого відкритого ключа зазначеного в сертифікаті організації проводиться розшифрування підпису цієї організації в сертифікаті. Якщо в результаті виходить той же сертифікат з тим же ім'ям користувача і його відкритим ключем, значить, він дійсно пройшов реєстрацію в сертифікаційному центрі, є тим, за кого себе видає, і вказаний в сертифікаті відкритий ключ дійсно належить йому.

Сертифікати можна застосовувати не тільки для автентифікації, але і для надання прав доступу до ресурсів. Для цього в сертифікат можуть вводитися додаткові поля, в яких вказується приналежність його власників до тієї чи іншої категорії користувачів. Ця категорія призначається центром сертифікації в залежності від умов, на яких видається сертифікат.

Сертифікат є посвідченням не тільки особистості, але і приналежності відкритого ключа. Цифровий сертифікат встановлює і гарантує відповідність між відкритим ключем і його власником.

Це запобігає загрозі підміни відкритого ключа. Якщо деякий абонент А отримує по мережі сертифікат від абонента Б, то він може бути впевнений, що відкритий ключ, який міститься в сертифікаті, гарантовано належить абоненту Б, адреса та інші відомості про якого містяться в цьому сертифікаті. Це означає, що абонент А може без побоювань використовувати відкритий ключ абонента Б для секретних повідомлень на його адресу.

При наявності сертифікатів відпадає потреба зберігати на серверах організацій списки користувачів з їх паролями, замість цього достатньо мати на сервері список імен і відкритих ключів центрів сертифікації. Може також знадобитись деякий механізм для встановлення відповідності категорій власників сертифікатів традиційним групам користувачів, щоб можна було в незмінному

вигляді задіяти механізми управління вибірковим доступом більшості операційних систем або додатків.

Сертифікат є засобом автентифікації користувача при його зверненні до мережевих ресурсів, роль автентифікуючої сторони виконують при цьому інформаційні сервери корпоративної мережі або Інтернету. У той же час і сама процедура отримання сертифіката також включає етап автентифікації, коли автентифікатором виступає центр сертифікації. Для отримання сертифіката клієнт повинен повідомити центру сертифікації свій відкритий ключ і певні відомості, що засвідчують його особу. Всі ці дані клієнт може відправити електронною поштою або принести на знімному носії особисто. Перелік необхідних даних залежить від типу одержуваного сертифіката. Сертифікуюча організація перевіряє докази достовірності, поміщає свій цифровий підпис в файл, який містить відкритий ключ, і посилає сертифікат назад, підтверджуючи факт приналежності даного конкретного ключа конкретній особі. Після цього сертифікат може бути вбудований в будь-який запит на використання інформаційних ресурсів мережі.

Важливим є питання про те, хто має право виконувати функції сертифікуючої організації. По-перше, завдання забезпечення своїх співробітників сертифікатами може взяти на себе саме підприємство. У цьому випадку спрощується процедура первинної автентифікації при видачі сертифіката. Підприємства достатньо обізнані про своїх співробітників, щоб брати на себе завдання підтвердження їх особи. Для автоматизації процесу генерації, видачі та обслуговування сертифікатів підприємства можуть використовувати готові програмні продукти: наприклад, компанія Netscape Communications випустила сервер сертифікатів, який організації можуть у себе встановлювати для випуску своїх сертифікатів. По-друге, ці функції можуть виконувати незалежні центри з видачі сертифікатів, що працюють на комерційній основі, наприклад сертифікуючий центр компанії Verisign. Сертифікати компанії Verisign виконані відповідно до міжнародного стандарту X.509 і використовуються в багатьох продуктах, орієнтованих на захист даних, в тому числі в популярному протоколі

захищеного каналу SSL. Будь-який бажаючий може звернутися із запитом на отримання сертифіката на веб-сервер цієї компанії.

Механізм отримання користувачем сертифіката добре автоматизується в мережі в моделі «клієнт-сервер», коли браузер виконує роль клієнта, а в сертифікуючій організації встановлено спеціальний сервер видачі сертифікатів. Браузер генерує для користувача пару ключів, залишає закритий ключ у себе і передає частково заповнену форму сертифіката серверу. Для того, щоб не підписаний ще сертифікат не можна було підмінити при передачі по мережі, браузер ставить свій електронний підпис, зашифровуючи сертифікат створеним закритим ключем. Сервер сертифікатів підписує отриманий сертифікат, фіксує його в своїй базі даних і повертає його будь-яким методом власнику. Після отримання сертифіката браузер зберігає його разом з закритим ключем і використовує при автентифікації на тих серверах, які підтримують такий процес. В даний час існує велика кількість протоколів і продуктів, які застосовують сертифікати. Зокрема, практично всі браузери і операційні системи реалізують підтримку сертифікатів.

Незважаючи на активне використання технології цифрових сертифікатів в багатьох системах безпеки, ця технологія ще не вирішила цілий ряд серйозних проблем. Це, перш за все, підтримка бази даних про видані сертифікати. Сертифікат видається не назавжди, а на певний визначений термін. Після закінчення терміну придатності сертифікат повинен або оновлюватися, або анулюватися. Крім того, необхідно передбачити можливість дострокового припинення повноважень сертифіката. Всі зацікавлені учасники інформаційного процесу повинні бути вчасно сповіщені про те, що деякий сертифікат вже недійсний. Для цього сертифікуюча організація повинна оперативно підтримувати список відкликаних сертифікатів.

Є також ряд проблем, пов’язаних з тим, що сертифікуючі організації існують не в однині. Всі вони випускають сертифікати, але навіть якщо ці сертифікати відповідають єдиному стандарту (зараз це, як правило, стандарт X.509), все одно залишаються невирішеними багато питань. Яким чином

можна перевірити повноваження того чи іншого сертифікуючого центру? Чи можна створити ієрархію сертифікуючих центрів, при якій сертифікуючий центр, що стоїть вище, міг би сертифікувати центри, які розміщені нижче в ієрархії? Як організувати спільне використання сертифікатів, випущених різними сертифікуючими організаціями?

Для вирішення цих та багатьох інших проблем, що виникають в системах, які використовують технології шифрування з відкритими ключами, виявляється необхідним комплекс програмних засобів і методик, званий інфраструктурою з відкритими ключами (Public Key Infrastructure, PKI).

Дана схема автентифікації включає три основних елементи: це користувачі, цифрові сертифікати і центри сертифікації. Для того щоб дана схема працювала надійно і ефективно, в неї повинні бути включені додаткові елементи, які в сукупності з основними і утворюють PKI.

У число додаткових елементів може входити, наприклад, реєстраційний центр (Registration Authority), який служить посередником між користувачем, що запросив сертифікат, і центром сертифікації. Користувач, зазвичай, звертається до реєстраційного центру за допомогою веб-інтерфейсу і повідомляє дані про себе. Реєстраційний центр перевіряє цю інформацію і в разі її достовірності передає дані про користувача, підписані власним закритим ключем, центру сертифікації. Реєстраційний центр може обслуговувати кілька центрів сертифікації. При відсутності реєстраційного центру його функції виконує центр сертифікації.

Іншим типом додаткових елементів PKI є різноманітні сховища сертифікатів, що містять інформацію про діючі, відкликані і сертифікати, у яких закінчився термін дії.

Сертифікати зберігаються в спеціальних системних сховищах, зазвичай представляють собою захищену область реєстру. Існують сховища комп'ютера, сховища користувачів цього комп'ютера і сховища служб. До сховища можна звернутися по ID, або за допомогою назви. Помістивши сертифікат у сховище, ми автоматично забезпечуємо довіру до нього.

Закриті ключі найчастіше також зберігаються в системному реєстрі, але окремо від сертифікатів. Якщо на комп'ютері є закритий ключ, відповідний сертифікату, у змінних властивості сертифіката є посилання на контейнер закритого ключа. Дуже важливо, щоб закритий ключ зберігався в тій же галузі реєстру, що і сертифікат, тобто або обидва в гілці HKLM, або обидва в HKCU. В іншому випадку можуть бути проблеми доступу до закритого ключу сертифіката.

Крім системних сховищ, сертифікати можуть зберігатися у файлах. Файли з розширенням. CER,. CRT,. DER містять сертифікат без закритого ключа в кодуванні DER або base64. Якщо для сертифіката з такого файлу є парний закритий ключ, він зазвичай зберігається файлом захищеним паролем з розширенням PVK. Для зберігання ланцюжка сертифікатів без закритих ключів використовується файл із розширенням P7B (стандарт PKCS#7). Для зберігання ланцюжка сертифікатів і закритих ключів призначаються файли з розширенням P12 і PFX (стандарт PKCS #12). Закритий ключ у PFX- файлі, як і в PVK-файлі, захищається паролем.

Цифровий сертифікат є ядром загальної інфраструктури інформаційної безпеки та її програмної складової зокрема. Сертифікати не є невід'ємною частиною систем цифрового підпису та шифрування. Однак, саме шифрування (і особливо цифровий підпис) часто мають сенс тільки за умови, що учасники транзакції довіряють використовуваним ключам. У цій ситуації цифрові сертифікати виявляються справді необхідні.

Компоненти інфраструктури відкритих ключів і їхні функції (PKI) мають містити елементи, наведені на (рис. 10) та (рис. 11).

IPSec може бути налаштований на використання загальних ключів або сертифікатів X.509 для захисту з’єднання VPN. Крім того, він використовує сертифікати X.509, одноразові паролі або протоколи (ім'я користувача/пароль) для авнтентифікації VPN-з’єднання. Одним з головних недоліків IPSec є те, що багато виробників реалізували власні розширення до цього стандарту, що

ускладнює конфігурування (або призводить до не сумісності) мережевого обладнання різних вендорів, при встановленні VPN-тунелю.

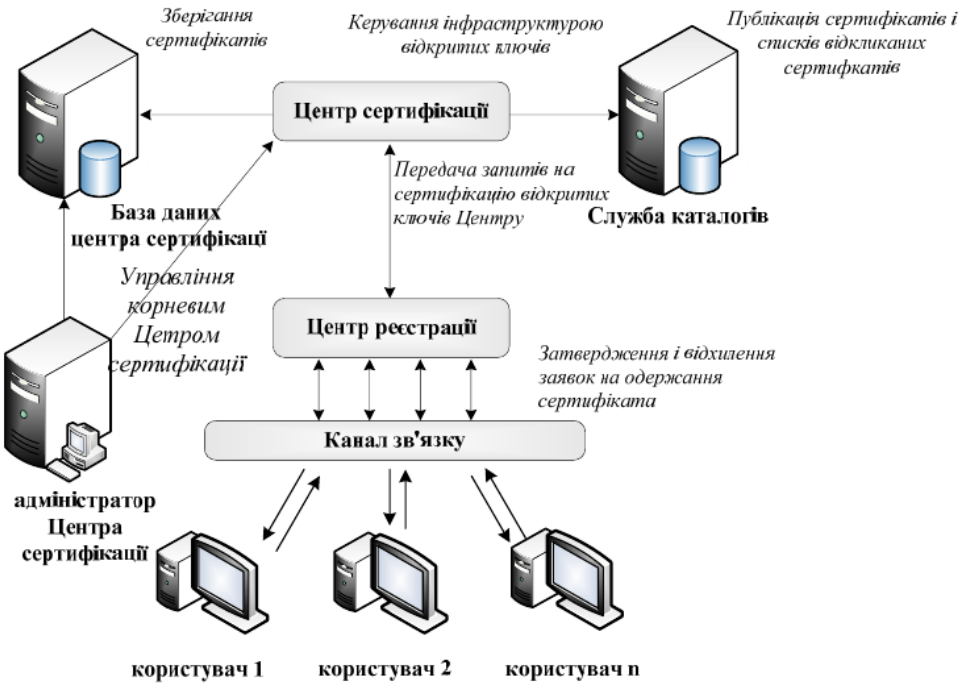

Рисунок 10 – Компоненти інфраструктури відкритих ключів

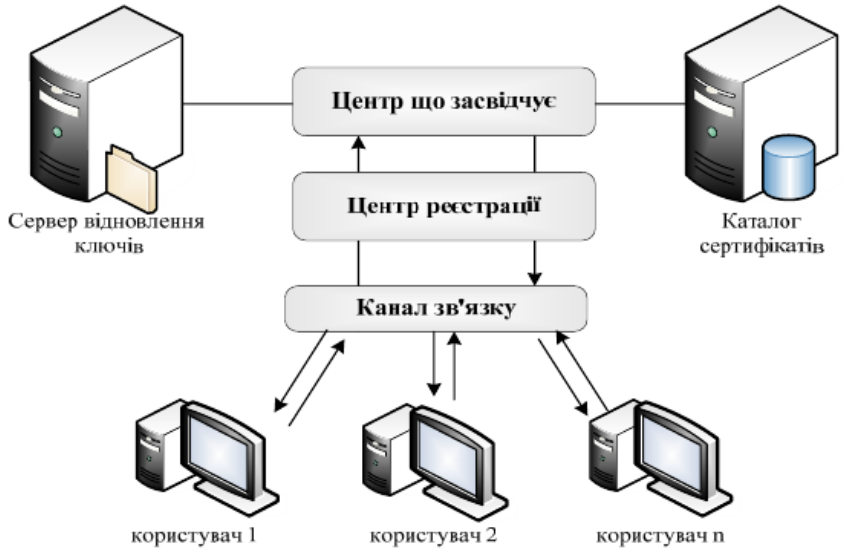

Рисунок 11 – Взаємодія між різними компонентами інфраструктури відкритих ключів

Також необхідно відмітити, що однією з сучасних технологій віртуальних приватних мереж є Secure Sockets Layer (SSL), тобто захист на рівні

сокетів. Вона заснована на протоколі SSL (криптографічний протокол, що забезпечує встановлення безпечного з'єднання між клієнтом і сервером за рахунок асиметричного шифрування і використання сертифікатів X.509) та протокол Transport Layer Security (TLS), який усуває недоліки SSL та прийнятий як стандарт RFC. SSL розташований між транспортним рівнем і рівнем додатків та здійснює шифрування на рівні додатків.

Але немає чітко визначеного стандарту для побудови VPN на основі SSL та більшість програмних рішень використовують протокол SSL/TLS, лише для захисту при встановленні з'єднання.

Однією з перспективних SSL-подібних захищених приватних мереж є технологія OpenVPN. OpenVPN – інструмент з відкритим вихідним кодом, що дозволяє шифрувати TCP або UDP тунелі в мережах типу site-to-site та клієнт/сервер. Особливістю даної технології полягає в тому, що OpenVPN має власний формат для шифрування і підписування трафіку даних, а саме HMAC (алгоритм цифрового підпису пакету) в поєднанні з алгоритмом дайджест (або хешування) за необхідності налаштований на використання загальних (pre-shared) ключів, а також сертифікатів X.509. Також вона дозволяє встановлювати VPN-з'єднання між комп'ютерами, що знаходяться за NAT і мережевим екраном, без необхідності зміни їх налаштувань.

Перевага OpenVPN полягає в легкості інсталяції і конфігурування, надання широкого спектру алгоритмів шифрування (симетричні алгоритми: Blowfish, DES, 3DES, AES; сертифікати: x509; хеш-функції: HMAC, MD5) та аунтентифікації користувачів на основі інфраструктури відкритих ключів (Public Key Infrastructure) PKI. Це реалізовано за рахунок інтеграції OpenSSL до складу OpenVPN. Тобто для аутентифікації VPN вузлів перед тим як почати передавати зашифровані дані створюються ключі, здійснюється їх підпис, а також є можливість шифрування даних і тестування SSL/TLS з'єднань.

При чому на OpenVPN сервері один і той же порт може бути використаний для кількох тунелів.

При використанні Open VPN в мережі типу клієнт/сервер існує два режими: режим тунелювання і режим транспорту (TUN/TAP). У режимі TUN можливо маршрутизувати IP-трафік, TAP – можливо передавати Ethernet-трафік [15][1)]. Для визначення продуктивності приватної мережі на основі Open VPN використовується утиліта iperf. При використанні OpenVPN спостерігається зниження пропускної здатності каналу приблизно 4.5%. Це пояснюється, тим що використання VPN вносить деякі накладні витрати для інкапсуляції, шифрування і аутентифікації вихідних даних. Також істотний влив на ефективність роботи тунелю OpenVPN є апаратна платформа вузлів мережі та метод шифрування.

4.2 Реалізація IPSEC IKEV2 на базі MIKROTIK

Проаналізувавши інформацію, яка міститься в попередніх розділах дипломної роботи, було зроблено висновок, про те, що оптимальним рішення для створення захищеного каналу зв'язку є технологія IPSec з протоколом обміну ключами IKEv2. Для автентифікації обрано саме метод цифрових сертифікатів інфраструктури відкритих ключів. Дане рішення є універсальним і штатним для багатьох операційних систем, на відміну від OpenVpn, яке потребує додаткового програмного забезпечення. Для демонстрації технології реалізуємо IKEV2 на обладнанні Mikrotik, яке позиціонується, як найкраще з представленого на ринку в порівнянні якість/ціна/продуктивність з аналогами.

Усі сучасні ОС (Windows Vista/7/8/8.1, OS X, Linux), мобільні пристрої (Android, iOS, Windows Phone, Blackberry) і деякі роутери, наприклад, Mikrotik

---

[1)] [15] Нестеренко, Н.Н. Аналіз методів побудови корпоративних мереж на основі VPN-технологій // ММ Нестеренко, БВ Саєнко, АС Кукліна / Збірник матеріалів XI Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (Проблеми телекомунікацій) [електроний ресурс] https://www.google.com /url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwi2_6OVs7jmAhWyw6YKHbV5AVUQFjABegQIARAC&url=http%3A%2F%2Fconfer-enc.its.kpi.ua%2Fproc%2Farticle%2Fdownload%2F100773%2F96017&usg=AOv-Vaw2JaX9fuSExw6PWWFpREzV7.

підтримують VPN з використанням IPsec ESP в тунельному режимі і його налаштування через протокол IKE версії 1 або 2.

Протокол IKE дозволяє проводити автентифікацію клієнта з використанням X.509-сертифікатів, Pre-Shared Key і Extensible Authentication Protocol (EAP). Підтримується двоетапна автентифікація.

IKE (як 1 так і 2 версії) забезпечують ESP (або AH) необхідною ключовою інформацією, потрібною вказаним протоколам для безпосереднього захисту даних.

Основні особливості і відмінності IKEv2 від IKEv1:

1 Обидва протоколи працюють по UDP/500 (4500 у випадку з NAT-T), але між собою несумісні, тобто не вийде так, щоб на одному кінці тунелю був IKEv1, а на іншому–IKEv2. При цьому один і той же маршрутизатор може термінувати на собі і IKEv2 і IKEv1 тунелі одночасно. У заголовках IKEv1 і 2 досить відмінностей для того, щоб маршрутизатор зміг визначити з чим має справу, незважаючи на одні і ті ж порти.

2 У IKEv2 більше немає таких понять як aggressive/main mode, що є одним з аспектів, які роблять протокол простішим для розуміння.

3 У IKEv2 термін фаза1 замінений на IKE_SA_INIT (обмін двома повідомленнями, що забезпечує узгодження протоколів шифрування/хешування і генерацію DH ключів), а фаза 2 − на IKE_AUTH (теж два повідомлення, що реалізують безпосередньо автентифікацію і генерацію ключів для ESP).

4 У IKEv2 метод автентифікації між з’єднаннями більше не узгоджується автоматично і не прив'язаний до тих або інших політик IKEv2. Якщо раніше в IKEv1 вказувалося, який буде тип аутентифікації, у випадку якщо буде вибрана саме ця політика, то тепер метод автентифікації задається вручну і явно визначається що ось з цим з’єднанням буде автентифікація за сертифікатами, а з другим за допомогою pre-shared key. Крім того, в IKEv2 стала можлива асиметрична автентифікація.

5 Mode Config (те, що в ikev1 називається phase 1.5 і використовується для налаштування віддалених підключень RAVPN/EasyVPN), NAT-T і keepalives

тепер безпосередньо описані в специфікації протоколу і є його невід'ємною частиною. Раніше ці речі реалізовувалися виробниками по-своєму в міру необхідності.

6 До IKEv2 додався додатковий механізм захисту control-plane (services plane) від DoS атак. Суть його в тому, що перш ніж відповідати на кожен запит у встановленні захищеного з'єднання (IKE_SA_INIT) IKEv2 VPN-шлюз шле джерелу такого запиту деякий cookie, і чекає, що той дасть відповідь тим же. Якщо отримано успішну відповідь, можна починати генерацію DH. Якщо ж джерело не відповідає (у випадку з DoS атакою так і відбувається, − це по суті порівняно з TCP SYN flood attack), VPN-шлюз просто забуває про нього. Без цього механізму, при кожному запиті IKE_SA_INIT IKEv2 від кого завгодно VPN-шлюз би намагався згенерувати DH ключ, що, як відомо, високонавантажений процес).

Налаштування IKEv2 на Mikrotik (RouterOS) починається з генерації цифрових сертифікатів (рис. 12).

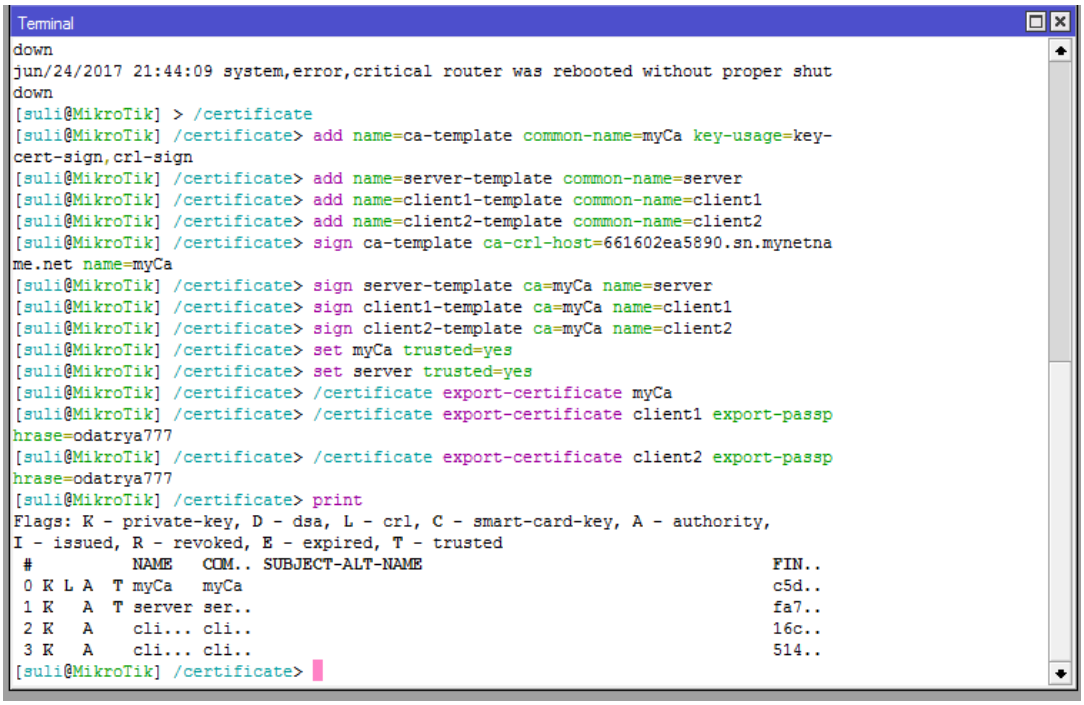

Рисунок 12 – Генерація сертифікатів

```
/certificate
add name=ca-template common-name=myCa key-usage=key-cert-
sign,crl-sign
```

– – додаємо шаблон для сертифікату центра сертифікації

```
add name=server-template common-name=server
```

– додаємо шаблон для сервера

```
add name=client1-template common-name=client1
add name=client2-template common-name=client2
```

– – додаємо клієнтські шаблони

Генеруємо всі сертифікати:

```
/certificate
sign ca-template ca-crl-host=10.5.101.16 name=myCa
sign server-template ca=myCa name=server
sign client1-template ca=myCa name=client1
sign client2-template ca=myCa name=client2
```

Помічаємо як надійні:

```
/certificate
set myCa trusted=yes
set server trusted=yes
```

Результат виконання команд відображений на рис.13.

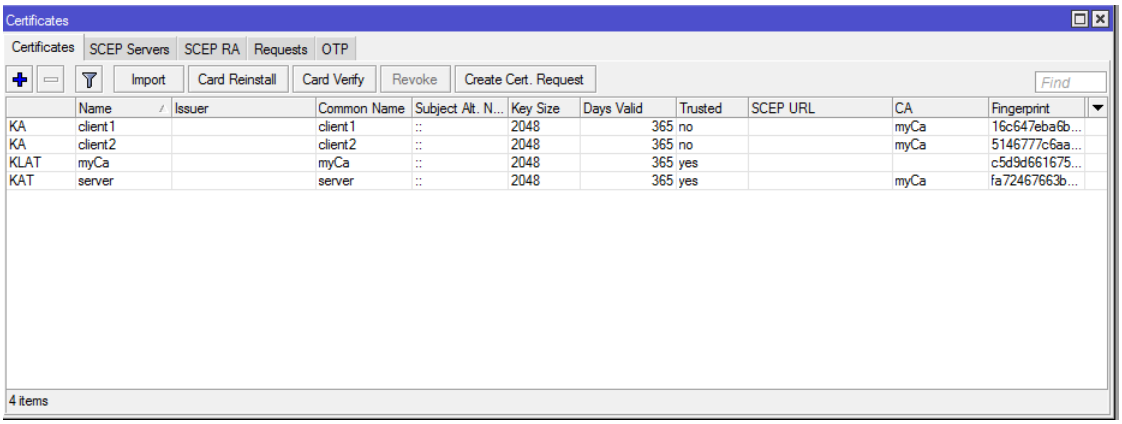

Рисунок 13 – Отримані сертифікати

Експортуємо сертифікати центру сертифікації та сертифікати користувачів (рис. 14):

```
/certificate export-certificate myCa
/certificate export-certificate client1 export-
passphrase=odatrya777
/certificate export-certificate client2 export-
passphrase=odatrya777
```

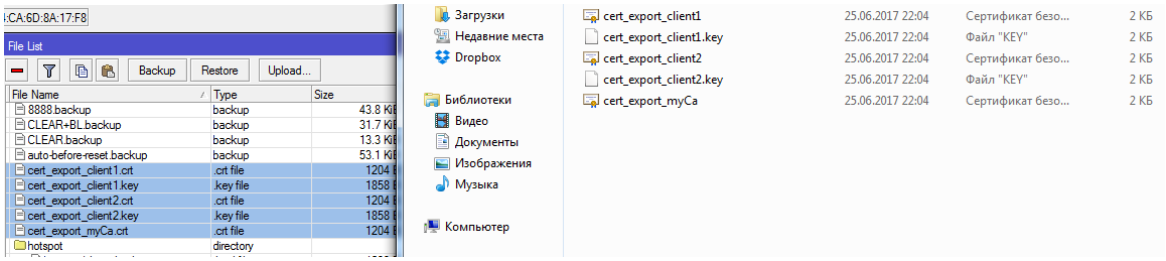

Рисунок 14 – Експорт сертифікатів

Фрагменти конфігурації автентифікації та шифрування на (рис. 15-17).

```
/ip ipsec proposal
set [ find default=yes ] auth-algorithms=sha1 enc-
algorithms=aes-256-cbc pfs-group=modp1024
```

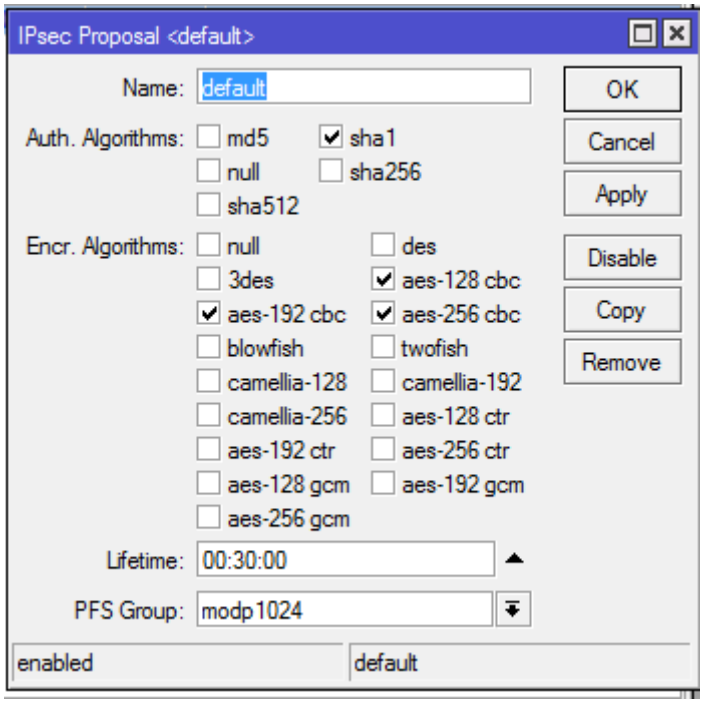

Рисунок 15 – Налаштування IPSec Proposal

Створення Proposals можна порівняти із створенням профілів шифрування. Серед доступних опцій передбачено:

– алгоритми генерації даних для автентифікації, які можуть приймати значення: md5, sha1, null;

– алгоритми генерації даних для шифрування зі значеннями: des, 3des,

aes-128, aes-192, aes-256, null.

Також є можливість вказати час працездатності профілю в секундах.

Алгоритми шифрування конфігуруються в IPSec Peer Encryption (рис.16) та сертифікати в IPSec Peer General (рис. 17).

```
/ip ipsec peer
add address=0.0.0.0/0 auth-method=rsa-signature
certificate=server1 dh-group=modp1024 enc-algorithm=aes-128
exchange-mode=ike2 generate-policy=port-strict hash-
algorithm=sha256 \
mode-config=test passive=yes
/ip ipsec policy
set 0 dst-address=192.168.33.0/27 src-address=0.0.0.0/0
```

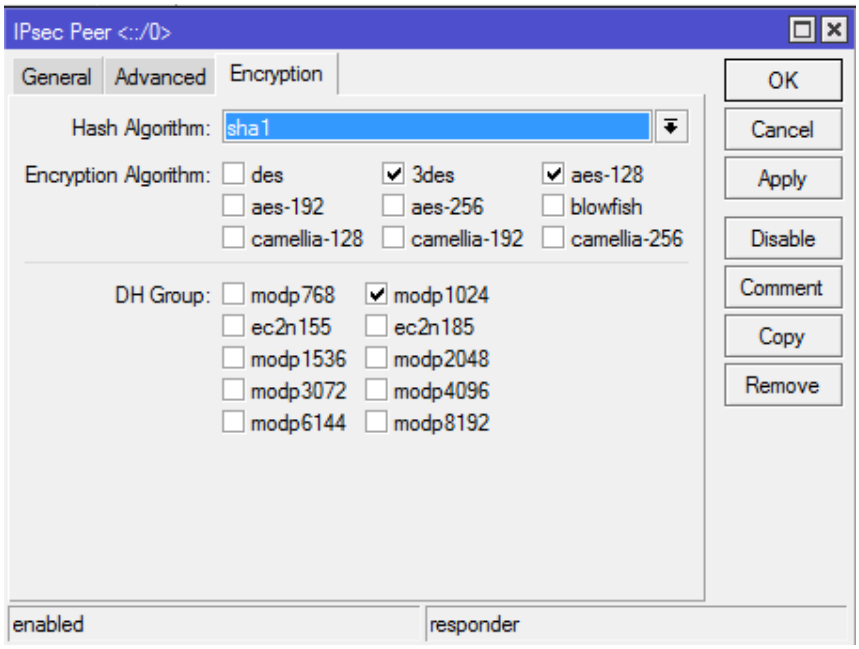

Рисунок 16 – Налаштування IPSec Peer Encryption

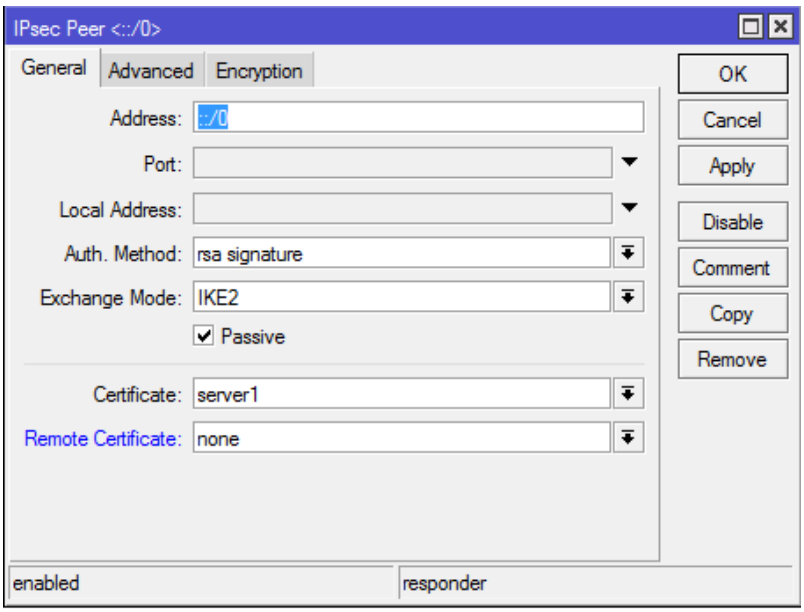

Рисунок 17 – Налаштування IPSec Peer General

Клієнт Windows не дозволяє імпортувати сертифікат та ключ окремо. Отже, потрібно скористатися зовнішнім інструментом (наприклад, OpenSSL) для перетворення файлів .crt та .key у формат pkcs12.

Отриманий результат перетворення зображений на (рис.18).

```
openssl pkcs12 -export -out cl1.pfx -inkey
cert_export_client1.key -in cert_export_client1.crt -certfile
cert_export_ca.crt
```

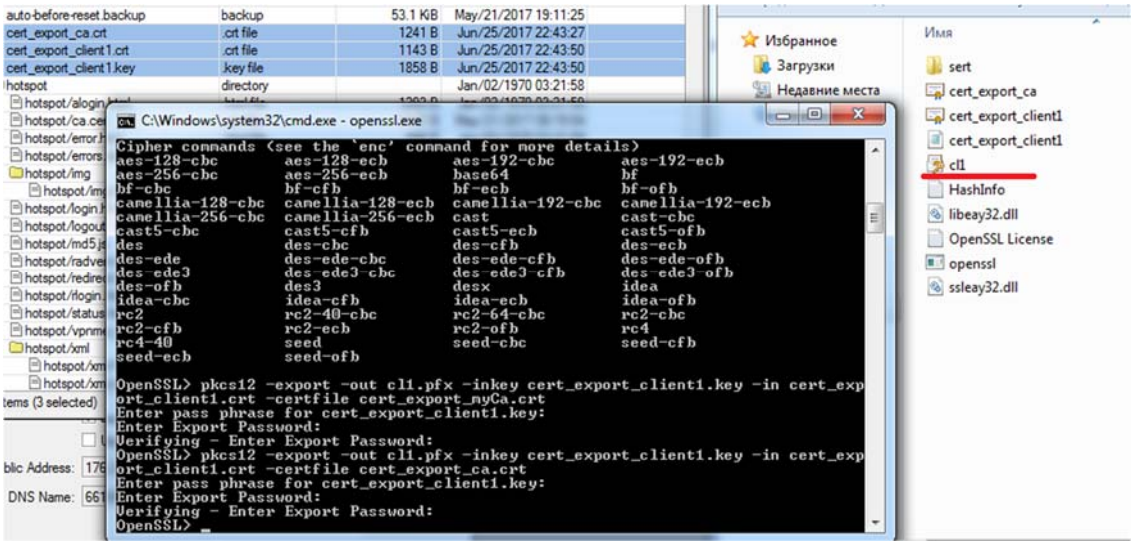

Рисунок 18 – Трансформація файлів .crt та .key у формат pkcs12

Наступним кроком є імпорт файлу pkcs12, який виконується через mmc і відповідну оснастку (рис. 19).

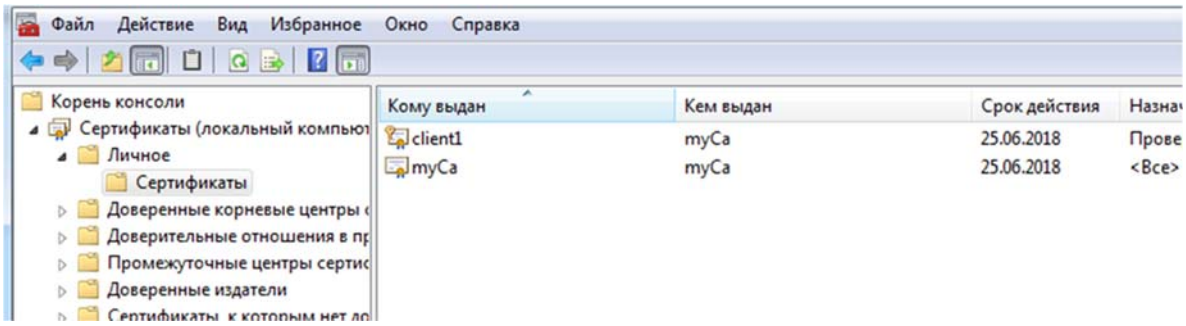

Рисунок 19 – Імпортовані файли сертифіката та закритого ключа

Сертифікат центру сертифікації потрібно додати до довірених. На рисунку 20 показаний зовнішній вигляд сертифікату.

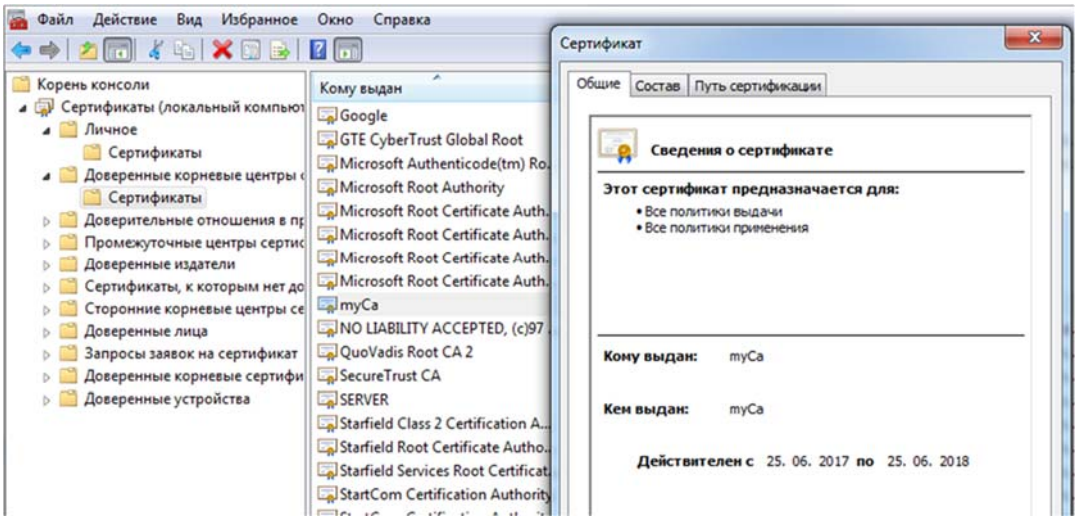

Рисунок 20 – Вигляд сертифікату центру сертифікації

Останнім кроком виступає підключення до VPN сервера, налаштування якого показане на рис. 21.

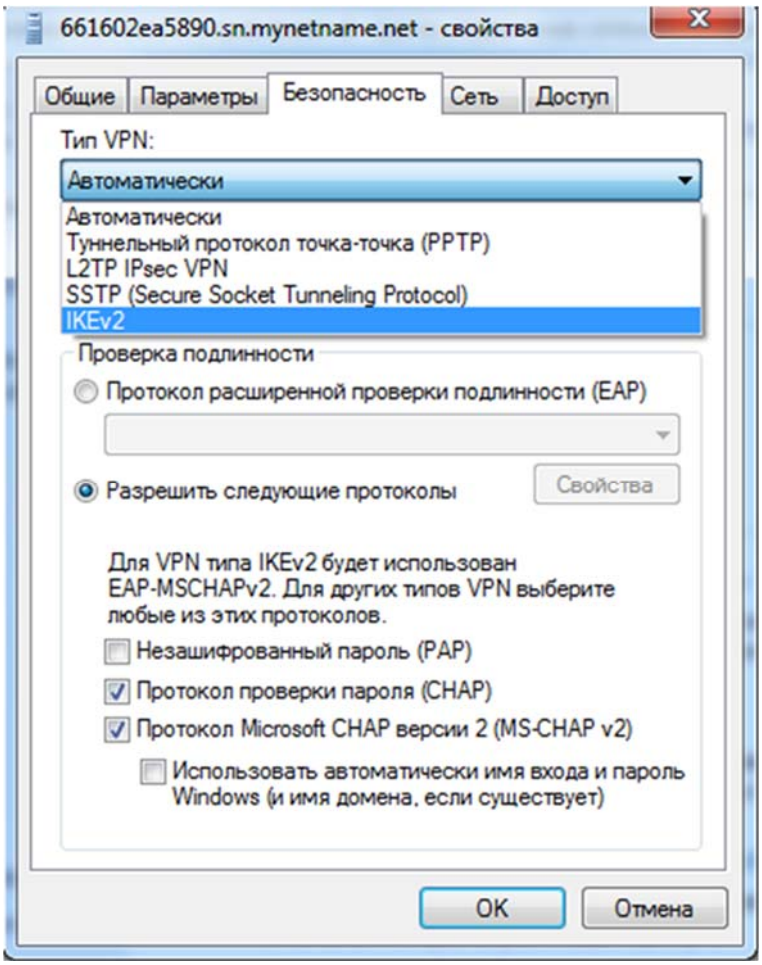

Рисунок 21 – Налаштування типу VPN

ВИСНОВКИ

В дипломній роботі розкрите питання аналізу захисту інформаційних мереж на базі VPN протоколів. Проаналізувавши різні протоколи захисту мереж дійшли висновку, що найбезпечніші протоколи VPN − це OpenVPN та IPSec IKEv2. Протокол IKEv2 працює швидко і безпечно, крім того, це один з небагатьох протоколів з підтримкою пристроїв Blackberry.

Оптимальним рішення для створення захищеного каналу зв'язку є технологія IPSec з протоколом обміну ключами IKEv2. Для автентифікації потрібно використовувати цифрові сертифікати інфраструктури відкритих ключів. Дане рішення є універсальним і штатним для багатьох операційних систем, на відміну від OpenVpn, яке потребує додаткового програмного забезпечення. В дипломній роботі показана реалізація IKEv2 на обладнанні Mikrotik, яке позиціонується, як найкраще з представленого на ринку в порівнянні з аналогами якість/ціна/продуктивність. IKEv2 дозволяє проводити автентифікацію клієнта з використанням X.509-сертификатів, Pre-Shared Key і Extensible Authentication Protocol (EAP). Підтримується двоетапна автентифікація.

Усі сучасні ОС (Windows Vista/7/8/8.1/10, OS X, Linux), мобільні пристрої (Android, iOS, Windows Phone, Blackberry) і більшість маршрутизаторів, наприклад, Mikrotik підтримують VPN налаштування через протокол IKE 2.

Отже, захищені інформаційні мережі рекомендується будувати на основі технологій IPSec IKEv2 або OpenVPN, які показали себе як надійні та безпечні, але перша має практичну перевагу. В якості автентифікації потрібно використовувати цифрові сертифікати інфраструктури відкритих ключів. Все це легко реалізується на маршрутизаторах Mikrotik.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Бобало Ю.Я. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв, С.С. Войтусік, А.Я. Горпенюк, О.А. Нємкова, І.М. Журавель, Б.М. Березюк, Є.І. Яковенко, В.І. Отенко, І.Я. Тишик. Львів: Видавництво Львівської політехніки, 2019. – 580 с.

2 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

3 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)

4 Класифікація автоматизованих систем і стандартні функціональні 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).

5 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).

6 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.

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

8 Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. 714с., іл.

9 А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) Львів, «Магнолія 2006», 2013. 256 с.

10 Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. К 63 Комп'ютерні мережі [навчальний посібник] / А.І.Блозва, Ю.В.Матус, В.В.Смолій, Б.С.Гусєв, Д.Ю.Касаткін, Т.Ю.Осипова, Я.А.Савицька. К.: Компрінт, 2017. 821с.

11 А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) Львів, «Магнолія 2006», 2014. 312 с.

12 А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) Львів, «Магнолія 2006», 2014. 312 с.

13 В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципи, технологи, протоколи: Ученик для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.

14 Комплексна безпека інформаційних мережевих систем : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. Тернопіль : Вид-во ТНТУ імені Івана Пулюя , 2016. 256 с.

15 Нестеренко, Н.Н. Аналіз методів побудови корпоративних мереж на основі VPN-технологій // ММ Нестеренко, БВ Саєнко, АС Кукліна / Збірник матеріалів XI Міжнародної науково-технічної конференції «Перспективи телекомунікацій» (Проблеми телекомунікацій) [електроний ресурс]: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwi2_6OVs7jmAhWyw6YKHbV5AVUQFjABegQIARAC&url=http%3A%2F%2Fconferenc.its.kpi.ua%2Fproc%2Farticle%2Fdownload%2F100773%2F96017&usg=AOvVaw2JaX9fuSExw6PWWFpREzV7.