NETWORK AND APPLICATION SECURITY

УДК 004 (056.55+738.5)

АРТЕМ ЖИЛІН,
СЕРГІЙ ВАЛОВИЙ,
ДМИТРО МАРИНІН

ОСОБЛИВОСТІ ПОБУДОВИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПРОТОКОЛІВ ВІРТУАЛЬНИХ ЗАХИЩЕНИХ МЕРЕЖ

У статті проведено аналіз основних протоколів побудови віртуальних захищених мереж, які широко використовуються при побудові захищених з'єднань в мережах загального призначення. Зазначено можливі види реалізацій віртуальних захищених мереж та наведено приклади сучасної телекомунікаційної апаратури, що використовує віртуальні захищені з'єднання для захисту інформації, що передається відкритими каналами зв'язку. Водночас визначено, що всі провідні телекомунікаційні компанії мають обладнання для побудови захищених віртуальних мереж. Приведено характеристики таких основних протоколів як IPSec, PPTP, L2TP та TLS. Розглянуто та проаналізовано їх будову, та наведено схеми логічної побудови кожного протоколу, а також їх переваги та недоліки. Приведено перелік криптографічних алгоритмів, які використовуються в цих протоколах. Проаналізовані протоколи працюють на різних рівнях моделі взаємодії відкритих систем, але мають загальні риси побудови й криптографічні алгоритми, що використовуються. Так, кожен з проаналізованих протоколів має підпротоколи, які відповідають за тунелювання, аутентифікацію, шифрування та забезпечення цілісності даних. Однак, кожен з них містить свої можливі реалізації криптографічних алгоритмів. Визначено, що перспективним варіантом розвитку технологій віртуальних приватних мереж для захисту інформації, що є власністю держави при її передачі відкритими каналами зв'язку є використання в реалізації віртуальних приватних мереж криптографічних алгоритмів, що пройшли Державну експертизу. Це можуть бути алгоритм блочного шифрування ДСТУ 7624:2014, алгоритм хешування ДСТУ 7564:2014 та алгоритм електронного цифрового підпису ДСТУ 4145:2002.

Ключові слова: віртуальні захищені мережі, крипто протокол, IPSec, PPTP, L2TP, TLS, тунелювання, автентифікація, шифрування.

Постановка проблеми. Необхідність забезпечення цілісності, конфіденційності та доступності інформації, що є власністю держави, при її передачі по відкритим каналам зв'язку є нагальною проблемою, адже використання таких мереж знижує вартість передачі даних. Одним із варіантів рішення цієї проблеми є побудова віртуальних захищених мереж (Virtual Private Network, VPN) за допомогою різних протоколів. Тому ***актуальним є*** аналізування протоколів побудови VPN в комп'ютерних мережах.

Аналіз останніх досліджень і публікацій. Віртуальні приватні мережі набули широкого впровадження в інформаційно-телекомунікаційних системах. Їх застосуванню передували чисельні дослідження, які були формалізовані у вигляді технічних специфікацій (Request for Comments, RFC) [1]. Проведені порівняння відомих VPN протоколів в [2] - [4] тільки коротко дають інформацію про них, не розкриваючи криптографічні алгоритми, які використовуються в цих протоколах, й не окреслюють можливості впровадження інших криптографічних алгоритмів, зокрема тих, що пройшли Державну експертизу.

Тому **метою** даної роботи є аналізування найпоширеніших протоколів віртуальних захищених мереж для проведення порівняння їхньої реалізації й криптографічних алгоритмів, що вони використовують, а також вибору найбільш доцільного протоколу, в залежності від цілей та можливостей організації.

Виклад основного матеріалу дослідження. У наш час VPN реалізуються як апаратно, так і програмно. Існує широкий вибір мережевого обладнання, для побудови захищених віртуальних мереж. Наприклад компанія Cisco випускає VPN-маршрутизатори серії 800-3800, HP серії PS110 та HPE R100, маршрутизатори D-Link серії DSR та мережеві екрани серії NetDefend, моделі яких працюють на основі протоколів IPSec, PPTP, L2TP та TLS [5]-[7].

Програмно VPN реалізується у вигляді пакетів або окремих застосунків в операційних системах. Широко відомі застосунки Telegram, Tor, Viber, веб-банкінгу, які також будують VPN для захисту даних при їх передачі по загально доступним каналам зв'язку. В свою чергу в операційній системі Windows є можливість створення VPN-серверу та VPN-клієнтів для підключення до відповідних VPN-серверів. В Linux системах можливе пакетне завантаження та встановлення найбільш поширених VPN-серверів та VPN-клієнтів.

Із всієї сукупності VPN слід відзначити базові протоколи, які реалізуються на певних рівнях моделі взаємодії відкритих систем (Open Systems Interconnection, OSI) й виступають підґрунтям для побудови більш розширених систем захисту трафіку в відкритих каналах зв'язку. Так на транспортному рівні найбільш поширеним базовим протоколом побудови VPN є протокол захисту транспортного рівня (Transport Layer Security, TLS), на мережевому – набір протоколів для забезпечення захисту даних, що передаються за допомогою міжмережевого протоколу IP (IP Security, IPSec), на канальному – протокол тунелювання "точка-точка" (Point-to-Point Tunneling Protocol, PPTP) та протокол тунелювання другого рівня (Layer 2 Tunneling Protocol, L2TP). Розглянемо більше детально кожен з них.

PPTP є протоколом тунелювання канального рівня моделі OSI, який забезпечує тунелювання, автентифікацію та шифрування даних, що передаються. Протокол PPTP будується на основі протоколу точка-точка (Poinl-to-Point Protocol, PPP) і є його розширенням. Протокол PPP, розроблений для інкапсуляції даних і їх доставки за типом з'єднання точка-точка. Цей протокол служить також для організації асинхронних (наприклад, комутованих) з'єднань [8].

У набір PPP входять протокол управління з'єднанням (Link Control Protocol, LCP), яким забезпечується конфігурування, встановлення і завершення з'єднання "точка-точка", і протокол управління мережею (Network Control Protocol, NCP), здатний інкапсулювати в PPP протоколи мережевого рівня для транспортування через з'єднання "точка-точка".

Згідно з протоколом PPTP при створенні захищеного віртуального каналу робиться автентифікація віддаленого користувача і шифрування даних, що передаються (див. рис. 1).

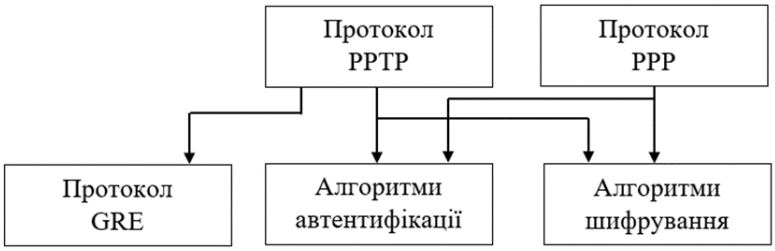

Рисунок 1 – Архітектура протоколу PPTP

PPTP працює, встановлюючи звичайну PPP сесію з протилежною стороною за допомогою протоколу загальної інкапсуляції маршрутів(Generic Routing Encapsulation, GRE). GRE є протоколом тунелювання, який забезпечує інкапсуляцію пакетів мережевого рівня моделі OSI в IP пакети.

У реалізації PPTP, яка включена компанією Microsoft в операційні системи Windows, підтримуються наступні протоколи автентифікації: протокол автентифікації за паролем (Password Authontication Protocol, PAP), протокол автентифікації при рукостисканні (Microsoft Challenge – Handshaking Authentication Protocol, MSCHAP) і протокол розширеної автентифікації (Extensible Authentication Protocol – Transport Layer Security, EAP-TLS). При використанні протоколу PAP ідентифікатори і паролі передаються лінією зв'язку в незашифрованому вигляді, при цьому тільки сервер проводить автентифікацію клієнта. При

використанні протоколів MSCHAP і EAP-TLS забезпечуються захист від повторного використання зловмисником перехоплених пакетів із зашифрованим паролем і взаємна автентифікація клієнта і VPN-сервера.

Шифрування за допомогою PPTP гарантує, що ніхто не зможе отримати доступ до даних при пересиланні через Інтернет. Для шифрування PPTP використовує протокол шифрування точка-точка (Microsoft Point-to-Point Encryption, MPPE). MPPE використовує алгоритми шифрування RSA та RC4. MPPE підтримує 40-, 56- і 128-бітові ключі, які змінюються протягом сесії [9].

Протокол PPTP застосовується в схемі тунелювання при прямому підключенню віддаленого клієнта до сервера.

Стек протоколів IPSec використовується для автентифікації учасників обміну, тунелювання трафіку і шифрування IP- пакетів [10]. Основне призначення протоколу IPSec – забезпечення безпечної передачі даних по мережах IP. Оскільки архітектура IPSec забезпечує сумісність з протоколом IPv4, то його підтримку досить реалізувати на обох кінцях з'єднання й проміжні мережеві вузли можуть взагалі нічого "не знати" про IPSec. Протокол IPSec може захищати трафік як поточної версії протоколу IPv4, так і версії IPv6, яка поступово впроваджується в Інтернет.

IPsec може функціонувати у двох режимах: транспортному і тунельному. У транспортному режимі шифруються (чи підписуються) тільки дані IP-пакету, а початковий заголовок зберігається. Транспортний режим, як правило, використовується для встановлення з'єднання між кінцевими пристроями. Він може також використовуватися між шлюзами для захисту тунелів, організованих іншим способом. У тунельному режимі шифрується увесь початковий IP- пакет: дані, заголовок, маршрутна інформація, а потім він вставляється в поле даних нового пакету, тобто відбувається інкапсуляція. Тунельний режим може використовуватися для підключення видалених комп'ютерів до віртуальної приватної мережі або для організації безпечної передачі даних через відкриті канали зв'язку між шлюзами для об'єднання різних частин віртуальної приватної мережі.

Для того, щоб забезпечити автентифікацію, конфіденційність і цілісність даних, що передаються, стек протоколів IPSec побудований на базі стандартизованих криптографічних технології:

– обміни ключами здійснюються згідно з алгоритмом Діфі-Хеллмана для розподілу секретних ключів між користувачами у відкритій мережі;

– використовуються асиметричні криптографічні алгоритми для підпису обміну ключами за схемою Діфі-Хеллмана, щоб гарантувати достовірність двох сторін і уникнути атак типу "людина-по-середині";

– використовуються цифрові сертифікати для підтвердження достовірності відкритих ключів;

– використовуються блокові симетричні алгоритми шифрування даних;

– використовуються алгоритми автентифікації повідомлень на базі функції хешування.

Ядро IPSec складають три протоколи: протокол автентифікаційного заголовка (Authentication Header, AH), протокол інкапсулюючого захисту (Encapsulating Security Payload, ESP) і протокол узгодження параметрів віртуального каналу і управління ключами (Internet Key Exchange, IKE). Архітектура засобів безпеки IPSec представлена на рис. 2.

Протокол узгодження параметрів віртуального каналу і управління ключами IKE визначає спосіб ініціалізації захищеного каналу, включаючи узгодження алгоритмів крипто захисту, що використовуються, а також процедури обміну і управління секретними ключами у рамках захищеного з'єднання.

Протокол автентифікаційного заголовка AH забезпечує автентифікацію джерела даних, перевірку цілісності і достовірності даних після прийому, а також захист від нав'язування повторних повідомлень.

Протокол інкапсулюючого захисту ESP забезпечує шифрування, автентифікацію і цілісність даних, а також захист від нав'язування повторних повідомлень.

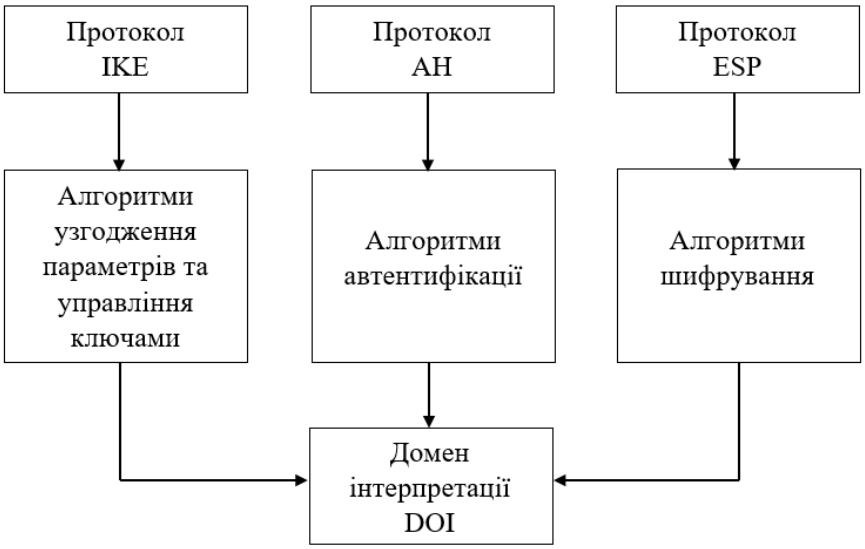

Рисунок 2 – Архітектура протоколу IPSec

Розділення функцій захисту між двома протоколами AH і ESP обумовлене існуванням у багатьох країнах практикою обмеження експорту або імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з протоколів AH і ESP може використовуватися як самостійно, так і спільно з іншим. З короткого переліку функції протоколів AH і ESP видно, що можливості цих протоколів частково перекриваються.

Протокол AH відповідає тільки за забезпечення цілісності і автентифікації даних, тоді як протокол ESP шифрує дані, та крім того, здатний виконувати функції протоколу AH.

Протокол ESP може підтримувати функції шифрування і автентифікації, забезпечення цілісності у будь-яких комбінаціях, тобто або і ту і іншу групу функцій, або тільки автентифікацію і забезпечення цілісності, або тільки шифрування.

Для шифрування даних в IPSec (протокол ESP) може бути застосований практично будь-який симетричний алгоритм шифрування з секретними ключами. Для забезпечення автентифікації даних (протоколи AH і ESP) використовується одностороння геш-функція.

Конфіденційність забезпечується шифруванням повідомлень з використанням симетричних сесійних ключів, якими сторони обмінюються при встановленні з'єднання. Сесійні ключі передаються також в зашифрованому виді, при цьому вони шифруються за допомогою відкритих ключів, отриманих з сертифікатів абонентів. Використання для захисту повідомлень симетричних ключів пов'язане з тим, що швидкість процесів шифрування і розшифрування на основі симетричного ключа істотно вища, ніж при використанні несиметричних ключів.

Достовірність і цілісність циркулюючої інформації забезпечується за рахунок формування і перевірки електронно-цифрового підпису. Для цифрових підписів і обміну ключами шифрування використовуються алгоритми з відкритим ключем.

В асиметричному шифруванні застосовуються алгоритм RSA для електронного цифрового підпису, а також алгоритм Діфі-Хеллмана для обміну ключами шифрування. Допустимими алгоритмами симетричного шифрування є RC2, RC4, DES, 3-DES і AES. Для обчислення хеш-функцій можуть застосовуватися стандарти MD5 і SHA-1.

Для побудови захищених віртуальних мереж на канальному рівні моделі OSI компанією Cisco Systems розроблено протокол L2F (Layer – 2 Forwarding) як альтернатива протоколу PPTP. В порівнянні з PPTP протокол L2F відрізнявся підтримкою різних мережевих протоколів і зручний у використанні для провайдерів Інтернету. Але він не забезпечував криптографічно захищеного тунелю між кінцевими пристроями. Тому протокол L2F був фактично поглинений протоколом L2TP.

Протокол L2TP розроблено Інженерною радою Інтернету (Internet Engineering Task Force, IETF) за підтримки компаній Microsoft і Cisco Systems. L2TP розроблявся як протокол

захищеного тунелювання PPP-трафіка через мережі загального призначення з довільним середовищем. Робота над цим протоколом велася на основі протоколів PPTP і L2F, і в результаті він увібрав в себе кращі якості початкових протоколів [11]. У протокол L2TP включена можливість роботи з протоколами AH і ESP стека протоколів IPSec (див. рис. 3).

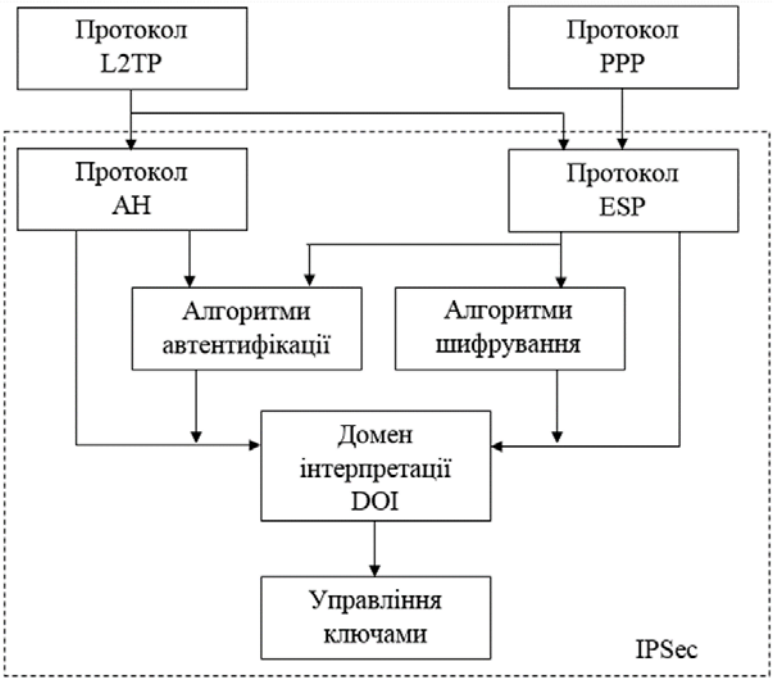

Рисунок 3 – Архітектура протоколу L2TP

Протоколи AH і ESP є основними компонентами стека протоколів IPSec. Ці протоколи допускають вибір користувачами за узгодженням різних криптографічних алгоритмів шифрування і автентифікації. На домен інтерпретації (Domain of Interpretation, DOI) покладені функції забезпечення спільної роботи використовуваних протоколів і алгоритмів.

По суті, гібридний протокол L2TP є розширенням протоколу PPP функціями автентифікації віддалених користувачів, створення захищеного віртуального з'єднання і управління потоками даних.

Протокол L2TP застосовує як транспорт протокол датаграм користувача (User Datagram Protocol, UDP) і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилки даних. У реалізації фірмою Microsoft протоколу L2TP використовуються контрольні повідомлення пакету UDP, що містять шифровані пакети PPP.

Хоча протокол PPTP забезпечує достатню степінь безпеки, але все таки протокол L2TP (на основі IPSec) надійніший. Протокол L2TP на основі IPSec забезпечує автентифікацію на рівнях “користувач” і ”комп’ютер”, а також виконує автентифікацію і шифрування даних.

На першому етапі автентифікації клієнтів і серверів VPN протокол L2TP використовує локальні сертифікати, отримані від служби сертифікації. Клієнт і сервер обмінюються сертифікатами і створюють захищене з’єднання.

Після того, як L2TP (на основі IPSec) завершує процес автентифікації комп'ютера, виконується автентифікація на рівні користувача. Для цієї автентифікації можна задіяти будь-який протокол, навіть PAP, який передає ім’я користувача і пароль у відкритому виді. Це цілком безпечно, оскільки L2TP (на основі IPSec) шифрує усю сесію. Проте проведення автентифікації користувача за допомогою MSCHAP шифрування, що застосовує різні ключі, для автентифікації комп’ютера і користувача, може підвищити безпеку.

Протокол L2TP припускає використання схеми, в якій тунель утворюється між сервером і клієнтом. На відміну від своїх попередників - протоколів PPTP і L2F, L2TP надає можливість відкривати між кінцевими абонентами відразу декілька тунелів, кожен з яких може бути виділений для окремого застосування. Ці особливості забезпечують гнучкість і безпеку тунелювання [12].

Найвищим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів, є четвертий – транспортний рівень. При побудові захищених віртуальних мереж на транспортному рівні з'являється можливість криптографічного захисту інформаційного обміну, включаючи автентифікацію, а також реалізацію ряду функцій посередництва між сторонами, що взаємодіють. Для захисту інформаційного обміну на транспортному рівні широке поширення отримав протокол TLS (див. рис.4).

TLS – використовує криптографічні методи захисту інформації для забезпечення безпеки інформаційного обміну [13]. Цей протокол виконує усі функції по створенню захищеного каналу між двома абонентами мережі, включаючи їх взаємну автентифікацію, забезпечення конфіденційності, цілісності і автентичності даних, що передаються. Ядром протоколу є технологія комплексного використання асиметричних і симетричних криптосистем.

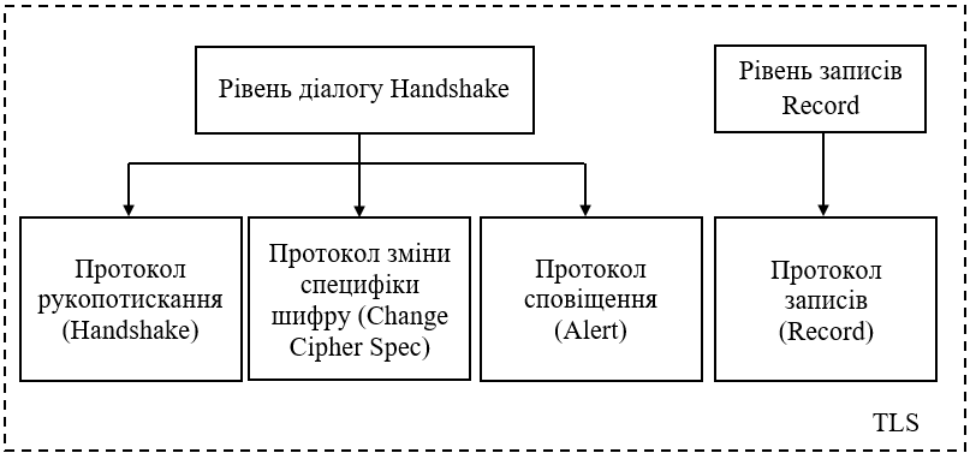

Рисунок 4 – Архітектура протоколу TLS

Протокол має два рівні: рівень записів TLS та рівень діалогу TLS, який в свою чергу, складається з трьох суб-протоколів: протокол зміни специфікації шифру, протокол сповіщення та протокол рукопотискання.

Протокол записів TLS забезпечує безпеку з'єднань, які мають дві основні властивості:

1. З'єднання є конфіденційним. Для шифрування даних використовується симетрична криптографія (напр., DES, RC4). Ключі для шифрування генеруються незалежно для кожного з'єднання і базуються на секретних даних, що отримуються за допомогою рівня діалогу TLS. Протокол записів може використовуватися і без шифрування.

2. З'єднання є надійним. Процедура передачі повідомлення включає перевірку цілісності за допомогою обчислення геш-функції. Для розрахунку MAC використовуються геш-функції (напр., SHA, MD5). Протокол записів може працювати і без геш-функції, але в цьому режимі він застосовується тільки у разі, коли інший протокол використовує протокол записів як транспортний при з'ясуванні параметрів безпеки.

Протокол записів TLS використовується для інкапсуляції рівня діалогу. Рівень діалогу TLS складається з трьох субпротоколів, які використовуються для погоджування параметрів безпеки для рівня запису, а також для аутентифікації і повідомлення про помилки. Протокол діалогу TLS забезпечує безпечне з'єднання, яке має три базові властивості:

1. Ідентичність партнерів може бути з'ясована з використанням асиметричної криптографії (напр., RSA , DSS). Ця автентифікація може бути реалізована як опція, але вона потрібна, принаймні, для однієї зі сторон.

2. Виявлення загального сесійного ключа є безпечним: цей ключ недоступний зловмисникові, навіть якщо він підключитися до з'єднання. Це забезпечується шляхом використання протоколу Діфі-Хеллмана (DH), а також Діфі-Хеллмана на еліптичних кривих (ECDHE).

3. Діалог надійний: той, що атакує не може модифікувати обговорюване з'єднання, без того щоб не бути виявленим сторонами обміну.

Взаємна аутентифікація обох сторін в TLS виконується шляхом обміну цифровими сертифікатами відкритих ключів користувачів (клієнта і сервера), завіреними цифровим підписом спеціальних сертифікаційних центрів. Протокол TLS підтримує сертифікати, що відповідають загальноприйнятому стандарту X.509, а також стандарти інфраструктури відкритих ключів PKI (Public Key Infrastructure), допомогою якої організовуються видача і перевірка достовірності сертифікатів.

До недоліків протоколів TLS можна віднести те, що для транспортування своїх повідомленні вони використовують тільки один протокол мережевого рівня - IP і, отже, можуть працювати тільки в IP- мережах.

Висновки. Використання загальнодоступної мережі Інтернет для передачі даних породжує проблему їх захисту. Ефективним способом рішення цієї проблеми є використання VPN протоколів та їх апаратно-програмних реалізацій. Згідно з наведеною класифікацією, VPN будується на транспортному (TLS), мережевому (IPSec) й канальному (PPTP, L2TP) рівнях OSI.

У залежності від потреб та можливостей реалізації захищених з'єднань, здійснюється вибір протоколу, використання якого буде найбільш доцільним для побудови VPN, адже кожен з розглянутих протоколів має свої переваги та недоліки. Так, наприклад, PPTP простий в налаштуванні, має високу швидкість передачі даних, але не може забезпечити надійний криптографічний захист, тоді як L2TP на основі IPSec є досить надійним, простим у налаштування, сумісним з різноманітними платформами для програмно-апаратної реалізації, але у нього також є свої недоліки – він значно повільніший ніж PPTP та конфліктує з міжмережевими екранами. TLS виконує усі функції зі створення захищеного каналу між двома абонентами мережі, включаючи їх взаємну автентифікацію, забезпечення конфіденційності, цілісності і автентичності даних, що передаються, але він може працювати лише в IP-мережах.

У той же час розглянуті VPN протоколи мають й спільні риси в побудові (див. табл.. 1). Так в їх структурах можна виокремити підпротоколи які відповідають за тунелювання, аутентифікацію, шифрування та забезпечення цілісності даних, але містять свої можливі реалізації крипто алгоритмів.

Таблиця 1 – Порівняльна таблиця найбільш поширених протоколів VPN

Протоколи	Тунелювання	Автентифікація/ Перевірка цілісності	Шифрування	Особливості
PPTP	GRE	PAP, MSCHAP, EAP- TLS	MPPE (RSA,RC4)	Тип з'єднання – точка-точка
L2TP	PPP	AH (Diffie – Hellman/ RSA/ MD5 або SHA-1)	ESP (RC2, RC4, DES, 3 - DES і AES)	Тип з'єднання – точка-точка/багатоточка
IPSec	PPP	AH (Diffie – Hellman/ RSA/ MD5 або SHA-1)	ESP (RC2, RC4, DES, 3 - DES і AES)	Два режими роботи: транспортний і тунельний
TLS	PPP	Handshake Protocol (Diffie – Hellman/ DSA/ MD5 або SHA)	Record Protocol (RC2, RC4, IDEA, DES, Triple DES AES;	Працює тільки в IP-мережах. Використання сертифікатів стандарту X.509

Таким чином, перспективним напрямком розвитку технологій VPN для захисту інформації що є власністю держави при її передачі по відкритим каналам зв'язку є

використання в апаратно-програмних комплексах VPN протоколів з криптографічними алгоритмами, що пройшли Державну експертизу. Так в криптопротоколах необхідно проаналізувати можливість використання як:

- алгоритмів шифрування алгоритмів ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014;
- алгоритмів хешування – ДСТУ 7564:2014 та ГОСТ 34.311-95;
- алгоритмів ЕЦП – ДСТУ 4145:2002.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] RFC Editor. [Online]. Available: www.rfc-editor.org. Accessed on: Sept.14, 2017.
[2] В.В. Майоров "Современные VPN-сети", *Научные труды КубГТУ*, № 13, с. 121-128, 2016.
[3] І.І. Пархоменко, О.О. Квачук, А.О. Воскобойніков, та Г.В. Попов, "Тунелювання, як спосіб захисту корпоративної інформації", *Захист інформації*, Том 14, № 1, с. 36-39, 2012. doi: 10.18372/2410-7840.14.2059.
[4] М.М. Браіловський, Т.В. Погребна, та О.В. Пташок, "Мережі VPN та проблеми їх захисту", *Телекомунікаційні та інформаційні технології*, № 1. с. 76-80, 2014.
[5] Cisco. [Online]. Available: www.cisco.com. Accessed on: Sept.10, 2017.
[6] Hewlett Packard Enterprise. [Online]. Available: https://www.hpe.com. Accessed on: Sept.10, 2017.
[7] D-Link. [Online]. Available: http://www.dlink.ua. Accessed on: Sept.10, 2017.
[8] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, "RFC 2637 Point-to-Point Tunneling Protocol (PPTP)". [Online]. Available: https://tools.ietf.org/html/rfc2637. Accessed on: Sept.10, 2017.
[9] G. Pall, and G. Zorn, "RFC 3078 Microsoft Point-To-Point Encryption (MPPE) Protocol". March 2001. [Online]. Available: https://tools.ietf.org/html/rfc3078. Accessed on: Sept.10, 2017.
[10] S. Kent, and K. Seo, "RFC 4301 Security Architecture for the Internet Protocol". [Online]. Available: https://tools.ietf.org/html/rfc4301. Accessed on: Sept.10, 2017.
[11] B. Patel, B. Aboba, W. Dixon, G. Zorn, and S. Booth, "RFC 3193 Securing L2TP using IPsec". [Online]. Available: https://tools.ietf.org/html/rfc3193. Accessed on: Sept.10, 2017.
[12] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter. "RFC 2661 Layer Two Tunneling Protocol "L2TP". [Online]. Available: https://tools.ietf.org/html/rfc2661. Accessed on: Sept.10, 2017.
[13] T. Dierks, and E. Rescorla. "RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2". [Online]. Available: https://tools.ietf.org/html/rfc5246. Accessed on: Sept.10, 2017.

Стаття надійшла до редакції 11 вересня 2017 року.

REFERENCES

[1] RFC Editor. [Online]. Available: www.rfc-editor.org. Accessed on: Sept.14, 2017.
[2] V.V. Maiorov, "Modern VPN-networks". *Scientific works KSTU*, № 13, pp. 121-128, 2016.
[3] I.I. Parhomenko, O.O. Kvachuk, A.O. Voskobojnikov, and G.V. Popov, "Tunneling as a way to protect corporate information", *Ukrainian Information Security Research Journal*, Vol. 14, № 1, pp. 36-39, 2012.
doi: 10.18372/2410-7840.14.2059.
[4] M.M. Brailovskyy, T.V. Pogrebna, and O.V. Ptashok, "VPN networks and problems of their defence", *Telecommunications and Information Technologies*, № 1, pp. 76-80, 2014.
[5] Cisco. [Online]. Available: www.cisco.com. Accessed on: Sept.10, 2017.
[6] Hewlett Packard Enterprise. [Online]. Available: https://www.hpe.com. Accessed on: Sept.10, 2017.
[7] D-Link. [Online]. Available: http://www.dlink.ua. Accessed on: Sept.10, 2017.
[8] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, "RFC 2637 Point-to-Point Tunneling Protocol (PPTP)". [Online]. Available: https://tools.ietf.org/html/rfc2637. Accessed on: Sept.10, 2017.

[9] G. Pall, and G. Zorn, “RFC 3078 Microsoft Point-To-Point Encryption (MPPE) Protocol”. March 2001. [Online]. Available: https://tools.ietf.org/html/rfc3078. Accessed on: Sept.10, 2017.
[10] S. Kent, and K. Seo, “RFC 4301 Security Architecture for the Internet Protocol”. [Online]. Available: https://tools.ietf.org/html/rfc4301. Accessed on: Sept.10, 2017.
[11] B. Patel, B. Aboba, W. Dixon, G. Zorn, and S. Booth, “RFC 3193 Securing L2TP using IPsec”. [Online]. Available: https://tools.ietf.org/html/rfc3193. Accessed on: Sept.10, 2017.
[12] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter. “RFC 2661 Layer Two Tunneling Protocol ”L2TP”. [Online]. Available: https://tools.ietf.org/html/rfc2661. Accessed on: Sept.10, 2017.
[13] T. Dierks, and E. Rescorla. “RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2”. [Online]. Available: https://tools.ietf.org/html/rfc5246. Accessed on: Sept.10, 2017.

АРТЕМ ЖИЛИН
СЕРГЕЙ ВАЛОВОЙ
ДМИТРИЙ МАРИНИН

ОСОБЕННОСТИ ПОСТРОЕНИЯ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ПРОТОКОЛОВ ВИРТУАЛЬНЫХ ЗАЩИЩЕННЫХ СЕТЕЙ

В статье проведен анализ основных протоколов построения виртуальных защищенных сетей, которые широко используются при построении защищенных соединений в сетях общего назначения. Отмечены возможные виды реализаций виртуальных защищенных сетей и приведены примеры современной телекоммуникационной аппаратуры, использующей виртуальные защищенные соединения для защиты информации, которая передается открытыми каналами связи. В то же время определенно, что все ведущие телекоммуникационные компании имеют оборудование для построения защищенных виртуальных сетей. Приведены характеристики таких основных протоколов как IPSec, PPTP, L2TP и TLS. Рассмотрено и проанализировано их строение, приведены рисунки логического построения каждого протокола, а также их преимущества и недостатки. Приведен перечень криптографических алгоритмов, которые используются в этих протоколах. Проанализированные протоколы работают на разных уровнях модели взаимодействия открытых систем, но имеют общие черты построения и криптографические алгоритмы, которые используются. Да, каждый из проанализированных протоколов имеет подпротоколы, которые отвечают за туннелирование, аутентификацию, шифрование и обеспечение целостности данных. Однако, каждый из них содержит свои возможные реализации криптографических алгоритмов. Определенно, что перспективным вариантом развития технологий виртуальных частных сетей для защиты информации, которая является собственностью государства при ее передаче открытыми каналами связи, являются использования в реализации виртуальных частных сетей протоколов криптографических алгоритмов, которые прошли Государственную экспертизу. Это могут быть алгоритм блочного шифрования ГСТУ 7624:2014, алгоритм хеширования ГСТУ 7564:2014 и алгоритм электронной цифровой подписи ГСТУ 4145: 2002.

Ключевые слова: виртуальные защищенные сети, криптопротокол, IPSec, PPTP, L2TP, TLS, туннелирование, аутентификация, шифрование.

ARTEM ZHYLIN
SERHII VALOVYI
DMYTRII MARYNIN

THE VIRTUAL PRIVATE NETWORKS PROTOCOLS: FEATURES OF CREATION AND PERSPECTIVE OF DEVELOPMENT

In this article, the analysis of the main protocols of the creation of the virtual private networks which are widely used in case of creation of the protected connections on networks of general purpose

is carried out. Possible types of implementations of the virtual private networks are marked and examples of the modern telecommunication equipment which uses the virtual protected connections for information security which is transferred by open channels of communication are given. At the same time, it is certain that all leading telecommunication companies have the equipment for the creation of the protected virtual area networks. Characteristics of such main protocols as IPSec, by PPTP, L2TP and TLS are provided. Their structure is considered and analyzed, figures of the logical creation of each protocol and also their advantage and shortcomings are given. The list of cryptographic algorithms which are used in these protocols is provided. The analyzed protocols work at different levels of the open system interconnection model but have common features of creation and cryptographic algorithms which are used. Yes, each of the analyzed protocols has subprotocols which are responsible for tunneling, authentication, encryption, and support of the integrity of data. However, each of them contains the possible implementations of cryptographic algorithms. It is certain that perspective option of development the virtual private area networks technologies for information security which is the property of the state during its transfer over open channels of communication are used in an implementation of the virtual private area networks of cryptographic algorithms which are passed a State expertise. It can be an algorithm of block encryption of GSTU 7624: 2014, hashing algorithm GSTU 7564: 2014 and algorithm of the digital signature of GSTU 4145: 2002.

Keywords: virtual private networks, the crypto protocol, IPSec, PPTP, L2TP, TLS, tunneling, authentication, encryption.

Артем Вікторович Жилін, кандидат технічних наук, доцент кафедри захисту державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: zhylinartem@gmail.com

Сергій Олександрович Валовий, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: serg.val@ukr.net

Дмитро Олегович Маринін, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: dima.marinin95@ukr.net

Артем Викторович Жилин, кандидат технических наук, доцент кафедры Защиты государственных информационных ресурсов, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Сергей Александрович Валовой, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Дмитрий Олегович Маринин, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Artem Zhylin, candidate of technical sciences, associate professor of state information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Serhii Valovyi, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Dmytro Marynin, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.