УДК 004.056.55:004.72.056 DOI: 10.31673/2409-7292.2026.022814

Матійко Олександра Андріївна
доктор філософії, доцент кафедри кіберзахисту та безпеки спеціального зв'язку
Національний технічний університет "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0000-0002-6947-5958
E-mail: alexm1710@ukr.net

Братасюк Роман Вікторович
курсант Інституту спеціального зв'язку та захисту інформації
Національний технічний університет "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0009-0004-2241-3022
E-mail: romabratasuk@gmail.com

Конотопець Микола Миколайович
кандидат технічних наук, доцент, доцент кафедри кіберзахисту та безпеки спеціального зв'язку
Національний технічний університет "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0000-0002-6963-1877
E-mail: nikolyalux@gmail.com

Туровський Олександр Леонідович
доктор технічних наук, професор, завідувач кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4961-0876
E-mail: s19641011@ukr.net

ОЦІНКА ЗАХИЩЕНОСТІ ТА ЕФЕКТИВНОСТІ VPN-РІШЕНЬ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Технології віртуальних приватних мереж є одним із базових засобів забезпечення захищеної передачі даних у сучасних інформаційно-комунікаційних системах. Вони дозволяють реалізувати конфіденційність, цілісність та автентичність інформації при передачі через відкриті мережі. Разом із тим, різноманіття VPN-протоколів та підходів до їх реалізації ускладнює вибір оптимального рішення з урахуванням вимог до рівня захищеності та продуктивності системи. Проведені дослідження свідчать, що забезпечення високого рівня криптографічного захисту часто супроводжується зростанням обчислювальних витрат і зниженням швидкодії, що є критичним для багатьох прикладних задач. Сьогодні питання комплексного оцінювання VPN-протоколів з урахуванням одночасного впливу показників безпеки та ефективності залишається недостатньо дослідженим. У статті запропоновано підхід до оцінювання VPN-рішень, що базується на використанні системи узагальнених критеріїв, які враховують як показники захищеності, так і ефективності функціонування. Такий підхід дозволяє формалізувати процес вибору VPN-протоколу залежно від умов експлуатації інформаційної системи та пріоритетності окремих параметрів. Зокрема, розглянуто особливості функціонування та характеристики сучасних VPN-протоколів, проведено їх порівняльний аналіз за ключовими показниками, включаючи рівень криптографічного захисту, пропускну здатність, затримку та навантаження на обчислювальні ресурси. Отримані результати свідчать про наявність компромісу між рівнем захищеності та ефективністю, що обумовлює необхідність застосування інтегральних критеріїв оцінювання. Наведено рекомендації щодо вибору VPN-протоколів залежно від вимог до інформаційної безпеки та продуктивності системи, що дозволяє підвищити ефективність побудови захищених каналів передачі даних.

Ключові слова: VPN-протоколи, захищена передача даних, криптографічний захист, інформаційна безпека.

Вступ та формулювання проблеми

У сучасних умовах масштабного переходу на дистанційні форми роботи та стрімкого зростання кіберзагроз, забезпечення захищеної передачі даних у відкритих мережах набуває критичного значення. Технологія віртуальних приватних мереж (VPN) залишається одним із ключових інструментів захисту корпоративних і державних комунікацій, оскільки дозволяє забезпечити конфіденційність, цілісність та автентичність інформації під час її передачі через

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

публічну інфраструктуру. Разом із тим широкий спектр існуючих VPN-протоколів суттєво відрізняється за рівнем криптографічної стійкості, продуктивністю, складністю реалізації та особливостями застосування. Вибір конкретного протоколу ускладнюється необхідністю одночасного врахування вимог до безпеки та ефективності функціонування. Підвищення рівня захисту зазвичай супроводжується збільшенням обчислювальних витрат і затримок у передачі даних, що може негативно впливати на якість сервісів. Водночас рішення з низькими накладними витратами часто мають недостатній рівень захищеності та можуть бути вразливими до сучасних методів атак.

Таким чином, актуальною науково-практичною задачею є розробка формалізованого підходу до комплексного оцінювання VPN-рішень, який дозволяє кількісно враховувати сукупність показників захищеності та ефективності для обґрунтованого вибору оптимального протоколу залежно від конкретних умов функціонування та пріоритетів інформаційної системи.

Аналіз останніх досліджень і публікацій

Проблематика забезпечення захищеної передачі даних із використанням VPN-технологій активно досліджується у сучасній науковій літературі. Так, у [1] наведено узагальнений огляд практики застосування VPN, проаналізовано основні протоколи та розглянуто типові вразливості, що підкреслює необхідність обґрунтованого підходу до вибору VPN-рішення з урахуванням актуальних загроз.

Значна увага у сучасних дослідженнях приділяється порівняльному аналізу продуктивності VPN-протоколів у різних середовищах. У роботі [2] проведено порівняння сучасних протоколів, зокрема WireGuard та OpenVPN, за результатами якого встановлено, що нові рішення демонструють вищу ефективність та менші накладні витрати порівняно з традиційними підходами. Подібні висновки отримано і в [3], де досліджено вплив різних мережевих конфігурацій на продуктивність VPN-протоколів; показано, що оптимізація архітектури дозволяє суттєво підвищити швидкодію та зменшити затримки.

Окремий напрям досліджень пов’язаний з аналізом вразливостей та можливостей ідентифікації VPN-трафіку. У роботі [4] показано, що з’єднання OpenVPN можуть бути виявлені за характерними мережевими ознаками, що створює передумови для їх блокування або аналізу. Суміжну задачу розглянуто у [5], де продемонстровано можливість класифікації зашифрованого трафіку на основі характеристик мережевого потоку, що свідчить про обмеженість анонімності VPN у сучасних умовах.

Важливим напрямом у сучасних дослідженнях є розробка нових архітектурних підходів до побудови захищених каналів зв'язку. Так, у роботі [6] запропоновано метод мультирівневого VPN-тунелювання, який створює додаткові шари захисту та забезпечує надійний віддалений доступ до ресурсів корпоративної екстранет-мережі, мінімізуючи ризики компрометації окремих вузлів або каналів. Водночас у дослідженні [7] проаналізовано застосування віртуальних мереж у критичних умовах: зафіксовано зростання попиту на VPN-рішення в Україні на 609% після початку повномасштабного вторгнення та досліджено здатність протоколів WireGuard, OpenVPN та IKEv2 підтримувати стабільні з'єднання і обходити інструменти мережевого цензурування на тимчасово окупованих територіях.

Таким чином, аналіз сучасних досліджень свідчить про значну увагу до питань підвищення ефективності та захищеності VPN-технологій. Водночас більшість робіт зосереджується на дослідженні окремих протоколів або їх характеристик, тоді як питання комплексного оцінювання VPN-рішень з урахуванням сукупності показників захищеності та ефективності залишаються недостатньо розробленими, що й визначає актуальність даного дослідження.

Мета статті полягає у розробці комплексного підходу до кількісного оцінювання VPN-протоколів на основі системи критеріїв захищеності та ефективності з використанням

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

варіативного коефіцієнта пріоритетності, що забезпечує обґрунтований вибір оптимального рішення залежно від вимог конкретного інформаційного середовища.

Для досягнення поставленої мети необхідно виконати наступні **завдання**:

1. Визначити ключові показники оцінювання VPN-протоколів (захищеності та ефективності);
2. Розробити систему критеріїв комплексного оцінювання VPN-протоколів;
3. Провести порівняльне оцінювання VPN-протоколів за запропонованим підходом та надати рекомендації щодо вибору VPN-рішень залежно від умов експлуатації.

Виклад основного матеріалу дослідження

Для кількісного аналізу захищеності VPN-протоколів вводиться інтегральний показник S_{VPN}, який розраховується як сума добутків індивідуальних оцінок за п'ятьма критеріями ($S_1 - S_5$) та їхніх вагових коефіцієнтів (w_i), які визначають значущість кожного параметра:

$$S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i, \quad (1)$$

де S_i – оцінка за конкретним критерієм, $S_i \in [0,1]$; w_i – відповідний ваговий коефіцієнт, $\sum_{i=1}^{5} w_i = 1$.

Для переведення якісних характеристик протоколів у числові значення застосовується диференційована шкала оцінювання (табл. 1).

Таблиця 1

Шкала оцінювання захищеності VPN-технологій

Діапазон балів	Рівень реалізації	Характеристика механізмів безпеки та рекомендації
0,9-1	Оптимальний	Забезпечується практично максимальний рівень безпеки, обмежений лише неминучими факторами реальної реалізації. Протокол відповідає кращим сучасним практикам та стандартам. Значення 1.00 є ідеальним еталоном.
0,76-0,89	Високий	Протокол реалізує сучасні криптографічні алгоритми, надійні механізми автентифікації та захисту від типових атак. Недоліки мають переважно експлуатаційний характер. Рішення придатне для використання в корпоративних та державних ІКС.
0,6-0,75	Середній	Механізми безпеки відповідають сучасним вимогам і стандартам. Забезпечується захист від основних атак за умови коректного налаштування. Можливі окремі компроміси між безпекою, продуктивністю та зручністю адміністрування.
0,4-0,59	Базовий	Забезпечується рівень безпеки, достатній для обмежених або некритичних систем. Протокол підтримує стандартні механізми, проте має відомі обмеження або підвищену складність конфігурації. Не рекомендовано для середовищ з високими вимогами.
0,2-0,39	Низький	Механізм присутній, однак не відповідає сучасним вимогам безпеки. Можливе використання слабких алгоритмів, відсутність захисту від типових атак або залежність від небезпечних налаштувань. Захист носить фрагментарний характер.
0-0,19	Критичний	Відповідний механізм безпеки відсутній або реалізований формально. Протокол не забезпечує захист від базових загроз або використовує зламані чи застарілі механізми. Використання в реальних ІКС є неприйнятним.

Опис критеріїв захищеності та визначені для них вагові значення:

– S_1 – криптографічна стійкість ($w_1 = 0,3$) – оцінює надійність алгоритмів, симетричного шифрування, стійкість механізмів обміну ключами та використання сучасних хеш-функцій для контролю цілісності. Даний критерій має найвищу вагу, оскільки стійкість криптографічного базису є першочерговою умовою забезпечення конфіденційності;

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

– S_2 – автентифікація ($w_2 = 0,2$) – визначає здатність протоколу забезпечувати надійну перевірку справжності вузлів. Аналізується підтримка методів від попередньо спільних ключів (PSK) до цифрових сертифікатів стандарту X.509 та розширюваних протоколів автентифікації (EAP);

– S_3 – захист від атак ($w_3 = 0,2$) – відображає наявність вбудованих механізмів протидії загрозам, таким як перехоплення та модифікація трафіку (Man-in-the-Middle), повторне відтворення пакетів (Replay attacks) та примусове зниження рівня шифрування (Downgrade attacks);

– S_4 – управління ключами ($w_4 = 0,15$) – оцінюється безпека життєвого циклу ключового матеріалу. Основними показниками є функції Perfect Forward Secrecy (PFS), автоматизація процесів ротації та періодичного переустановлення ключів;

– S_5 – зрілість та аудит ($w_5 = 0,15$) – визначає рівень довіри до протоколу на основі тривалості його експлуатації, наявності незалежних публічних аудитів безпеки та оперативності усунення виявлених вразливостей.

Також вводиться інтегральний показник ефективності E_{VPN}, який розраховується як сума добутків індивідуальних оцінок за п'ятьма технічними критеріями ($E_1 - E_5$) та їхніх вагових коефіцієнтів (v_i), що визначають вплив кожного параметра на загальну продуктивність системи:

$$E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i, \tag{2}$$

де E_i – оцінка за конкретним критерієм, $E_i \in [0,1]$; а v_i – відповідний ваговий коефіцієнт, $\sum_{i=1}^{5} v_i = 1$.

Рівень ефективності протоколу зазначається за допомогою відповідної шкали оцінювання (табл. 2).

Таблиця 2

Шкала оцінювання ефективності VPN-технологій

Діапазон балів	Рівень ефективності	Технічні наслідки та продуктивність
0,9-1	Оптимальний	Характеристики максимально наближені до фізичного каналу; 1,00 – ідеальний еталон.
0,76-0,89	Високий	Раціональне використання ресурсів та висока швидкість обробки даних.
0,6-0,75	Середній	Відповідає стандартам для більшості корпоративних сценаріїв.
0,4-0,59	Базовий	Стабільна робота при суттєвих обмеженнях швидкості або затримок.
0,2-0,39	Низький	Значні затримки або високе споживання апаратних ресурсів.
0-0,19	Критичний	Надмірні накладні витрати; впровадження технології недоцільне.

Опис критеріїв ефективності та визначені для них вагові значення:

– E_1 – пропускна здатність ($v_1 = 0,3$) – оцінює швидкість передавання корисних даних через тунель після вирахування накладних витрат на інкапсуляцію та криптографічну обробку трафіку. Даний показник є пріоритетним, оскільки визначає здатність протоколу працювати у сучасних високошвидкісних мережах;

– E_2 – затримка ($v_2 = 0,2$) – визначає додатковий час обробки пакетів (latency), зумовлений операціями шифрування та обміном службовою інформацією, що є критичним для сервісів реального часу;

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

– E_3 – навантаження на ресурси ($v_3 = 0,2$) – відображає вимогливість протоколу до обчислювальних потужностей центрального процесора та оперативної пам'яті пристрою, що визначає можливість його використання на апаратно обмежених платформах;

– E_4 – масштабованість ($v_4 = 0,15$) – оцінює здатність протоколу зберігати стабільність та продуктивність при зростанні кількості одночасних з'єднань та складності мережевої топології;

– E_5 – складність налаштування та автоматизації ($v_5 = 0,15$) – визначає трудомісткість процесу конфігурування, поріг входу для технічного персоналу та сумісність із сучасними інструментами автоматизації мереж.

Для отримання остаточного результату, який дозволяє порівнювати різні протоколи з урахуванням специфіки конкретних завдань, розраховується підсумковий показник $Rating_{VPN}$. Він базується на зваженому поєднанні інтегральних оцінок захищеності S_{VPN} (1) та ефективності E_{VPN} (2):

$$Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN},$$

де α – коефіцієнт пріоритету безпеки, що набуває значень від 0 до 1.

Вибір значення α дозволяє адаптувати вищезазначений підхід під наступні сценарії використання:

1. Збалансований сценарій ($\alpha = 0,5$) передбачає рівнозначну важливість показників безпеки та швидкодії. Застосовується для загальних бізнес-задач та стандартного корпоративного трафіку;

2. Сценарії підвищеної безпеки ($\alpha = 0,7$), де пріоритет надається захищеності протоколу. Використовується в системах, де ризики компрометації даних переважають над вимогами до швидкості (наприклад, державний сектор або фінансові операції);

3. Сценарії високої продуктивності ($\alpha = 0,3$), де пріоритет зміщується в бік ефективності передачі даних. Актуально для сервісів реального часу (VoIP, відеоконференції), де мінімальна затримка є критичною.

Підсумковий результат дозволяє зрозуміти, наскільки протокол підходить для роботи, згідно з наведеною шкалою (табл. 3).

Таблиця 3

Інтерпретація підсумкового рейтингу VPN-технологій

Діапазон балів	**Рівень якості**	**Характеристика придатності**
0,9-1	Оптимальний	Відмінне поєднання безпеки та швидкості; найкращий вибір;1,00 – ідеальний еталон.
0,76-0,89	Високий	Надійне рішення, повністю готове до використання в серйозних системах.
0,6-0,75	Середній	Хороший рівень, підходить для більшості стандартних завдань.
0,4-0,59	Базовий	Достатній рівень, але має обмеження в захисті або швидкодії.
0,2-0,39	Низький	Слабкий рівень, використовувати такий VPN-протокол не рекомендується.
0-0,19	Критичний	Протокол не забезпечує прийнятного рівня ні безпеки, ні швидкодії.

Таким чином, було розроблено та обґрунтовано комплексний підхід кількісного оцінювання VPN-протоколів, який базується на математичному моделюванні взаємозв'язку між захищеністю та ефективністю. Сформована система критеріїв охоплює десять параметрів, що дозволяють детально проаналізувати як криптографічну стійкість та механізми автентифікації, так і пропускну здатність разом із навантаженням на апаратні ресурси. Запропонований математичний апарат для розрахунку показників S_{VPN} та E_{VPN} у поєднанні з коефіцієнтом пріоритету α забезпечує високу гнучкість оцінювання залежно від специфіки

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

інформаційного середовища. Створена шкала верифікації результатів дозволяє об'єктивно інтерпретувати отримані числові дані та приймати обґрунтовані рішення щодо доцільності впровадження конкретних VPN-технологій, що створює необхідний методологічний базис для проведення подальшого порівняльного аналізу.

Практичне застосування розробленого підходу дозволяє кількісно оцінити сильні та слабкі сторони VPN-протоколів. Кожне рішення оцінюється за десятьма визначеними параметрами, що дає змогу вивести об'єктивний рейтинг захищеності (S_{VPN}) та ефективності (E_{VPN}). Використання варіативного коефіцієнта α допомагає визначити оптимальну сферу застосування для кожної технології.

Практичну частину дослідження доцільно розпочати з аналізу PPTP, який у даному порівнянні виступає як базовий еталон застарілих технологій. Його оцінювання дозволить продемонструвати, як використання слабких криптографічних примітивів та механізмів автентифікації впливає на інтегральний показник захищеності, попри високу швидкість обробки даних на канальному рівні.

Аналіз захищеності протоколу PPTP (S_{VPN}):

− PPTP використовує застаріле шифрування MPPE (Microsoft Point-to-Point Encryption), яке базується на потоковому шифрі RC4. Протокол підтримує ключі довжиною 40, 56 або 128 біт, проте через архітектурні вразливості RC4 та відносно коротку довжину ключів, шифрування не забезпечує надійного захисту від сучасних методів криптоаналізу [8]. Тому $S_1 = 0,2; w_1 = 0,3$;

− PPTP забезпечує автентифікацію на основі методів PAP (передача у відкритому вигляді), CHAP та MS-CHAP v2. Найбільш вживаний MS-CHAP v2 є вразливим до атак типу "словниковий підбір" та перехоплення хешів паролів, що дозволяє зловмисникам відносно швидко отримати несанкціонований доступ [8]. Тому $S_2 = 0,3; w_2 = 0,2$;

− PPTP реалізує лише базовий захист від атак. У протоколі відсутні механізми перевірки автентичності кожного окремого пакета, що робить сесію вразливою до атак типу Man-in-the-Middle, ін'єкцій даних та перехоплення тунелю. Захист суттєво поступається сучасним стандартам безпеки [8]. Тому $S_3 = 0,2; w_3 = 0,2$;

− PPTP не підтримує Perfect Forward Secrecy (PFS). Управління ключами інтегроване в процес автентифікації, тому компрометація головного ключа дозволяє розшифрувати весь перехоплений раніше трафік. Автоматична ротація ключів реалізована слабко [8]. $S_4 = 0,2; w_4 = 0,15$;

− PPTP є застарілим протоколом, який офіційно не рекомендується до використання багатьма розробниками (зокрема Microsoft). Попри повну стандартизацію, він регулярно провалює аудити безпеки, а більшість сучасних операційних систем поступово обмежують його підтримку [8]. Тому $S_5 = 0,25; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,2 + 0,2 \cdot 0,3 + 0,2 \cdot 0,2 + 0,15 \cdot 0,2 + 0,15 \cdot 0,25 = 0,23$.

Аналіз ефективності PPTP (E_{VPN}):

− PPTP забезпечує високий рівень пропускної здатності за рахунок використання простих алгоритмів шифрування RC4, які створюють мінімальні накладні витрати на обробку даних. У стандартних мережевих середовищах протокол здатен працювати майже на швидкості фізичного каналу, оскільки не потребує великих обчислювальних потужностей. Тому $E_1 = 0,9; v_1 = 0,3$;

− Затримки в PPTP є мінімальними завдяки швидкому процесу інкапсуляції пакетів та відсутності складних процедур узгодження ключів. Протокол є прийнятним для додатків реального часу (VoIP, відео), проте його стабільність може знижуватися в мережах із високим

рівнем втрат пакетів через особливості роботи над протоколом GRE [8]. Тому $E_2 = 0,9; v_2 = 0,2$;

− PPTP є одним із найменш ресурсномістких протоколів. Завдяки програмній реалізації, яка не потребує спеціалізованого апаратного прискорення, він спостерігає мінімальне навантаження на CPU навіть на застарілих пристроях або мобільних платформах з обмеженою потужністю. Тому $E_3 = 0,95; v_3 = 0,2$;

− PPTP має середню масштабованість. Він широко підтримується клієнтськими ОС, проте часто виникають складнощі при проходженні через міжмережеві екрани та NAT (через використання порту TCP 1723 та протоколу GRE), що вимагає специфічних налаштувань мережевого обладнання [8]. Тому $E_4 = 0,65; v_4 = 0,15$;

− Налаштування PPTP є максимально простим і не вимагає глибоких технічних знань. Більшість параметрів встановлюються автоматично, а підтримка вбудована безпосередньо в інтерфейси користувача багатьох ОС. Загальний поріг входу є найнижчим серед усіх розглянутих технологій. Тому $E_5 = 0,95; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,9 + 0,2 \cdot 0,9 + 0,2 \cdot 0,95 + 0,15 \cdot 0,65 + 0,15 \cdot 0,95 = 0,88$.

Підсумкова оцінка для PPTP при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,23 + 0,7 \cdot 0,88 = 0,68$ (середній рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,23 + 0,5 \cdot 0,88 = 0,56$ (базовий рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,23 + 0,3 \cdot 0,88 = 0,43$ (базовий рівень).

Переходячи до більш захищених рішень, розглянемо комбінацію L2TP/IPsec. Для цього протоколу критичним фактором оцінювання є архітектурна надлишковість, спричинена подвійною інкапсуляцією. Це дозволяє дослідити, наскільки суттєво підвищення рівня безпеки (за рахунок стеку IPsec) знижує ефективність передачі даних (E_{VPN}) через додаткові накладні витрати на заголовки.

Аналіз захищеності L2TP/IPsec (S_{VPN}):

− L2TP/IPsec використовує надійні криптографічні алгоритми шифрування AES-128/256 та хешування SHA-2 для перевірки цілісності даних. Проте протокол допускає використання застарілих наборів, таких як 3DES або SHA-1, для забезпечення сумісності зі старим обладнанням, що може бути активовано через помилки в конфігурації [9]. Тому $S_1 = 0,85; w_1 = 0,3$;

− Протокол підтримує автентифікацію на основі цифрових сертифікатів X.509, попередньо спільних ключів (PSK) та методів EAP. Проте використання PSK створює ризик компрометації всієї мережі у разі викрадення ключа з одного клієнтського пристрою, а дворівнева структура автентифікації підвищує складність контролю доступу [9]. Тому $S_2 = 0,8; w_2 = 0,2$;

− L2TP/IPsec реалізує захист від атак типу Man-in-the-Middle та Replay-атак за допомогою механізмів інкапсуляції IPsec. Проте використання фіксованих портів (UDP 500, 1701, 4500) дозволяє легко ідентифікувати протокол засобами аналізу трафіку, що робить його вразливим до цілеспрямованих атак на відмову в обслуговуванні або блокування [9]. Тому $S_3 = 0,8; w_3 = 0,2$;

− Протокол підтримує Perfect Forward Secrecy (PFS), автоматичну ротацію ключів та перевстановлення тунелів. Проте реалізація захисту на базі IKEv1 має менш стійкий механізм

узгодження параметрів безпеки порівняно з оновленим стандартом IKEv2, що знижує загальну стійкість сесії до спроб примусового зниження рівня захисту [9]. Тому $S_4 = 0,85; w_4 = 0,15$;

− L2TP/IPsec є повністю стандартизованим та стабільним рішенням, яке інтегроване в більшість сучасних операційних систем. Проте архітектурна складність стеку через велику кількість компонентів ускладнює проведення повного аудиту безпеки всієї системи одночасно [9]. Тому $S_5 = 0,85; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,85 + 0,2 \cdot 0,8 + 0,2 \cdot 0,8 + 0,15 \cdot 0,85 + 0,15 \cdot 0,85 = 0,83 \cdot$

Аналіз ефективності L2TP/IPsec (E_{VPN}):

− Пропускна здатність обмежена через архітектурну особливість “подвійної інкапсуляції”, де дані обгортаються спочатку заголовком L2TP, а потім IPsec. Проте такий підхід створює значні накладні витрати на кожен пакет, що призводить до помітного зниження корисної швидкості передачі даних [9]. Тому $E_1 = 0,65; v_1 = 0,3$;

− Показники затримки в L2TP/IPsec є вищими за середні через багатоетапний процес встановлення та підтримки з’єднання. Проте необхідність обробки великої кількості службових пакетів для кожного тунелю робить його менш ефективним для сервісів, чутливих до часових інтервалів [9]. Тому $E_2 = 0,6; v_2 = 0,2$;

− Протокол створює високе навантаження на ресурси системи через необхідність подвійної обробки заголовків. Інтенсивне використання процесора для криптографічних операцій без спеціалізованого апаратного прискорення робить його ресурсоємним для малопотужних мережевих пристроїв [9]. Тому $E_3 = 0,6; v_3 = 0,2$;

– Масштабованість протоколу забезпечується його широкою підтримкою, проте виникають складнощі при роботі в мережах із багатьма рівнями NAT. Це зумовлено тим, що використання протоколу ESP та фіксованих портів часто спричиняє конфлікти при спробі встановити кілька одночасних з’єднань з однієї зовнішньої IP-адреси [9]. Тому $E_4 = 0,7; v_4 = 0,15$;

− Налаштування L2TP/IPsec інтегроване в інтерфейси більшості ОС, що спрощує роботу для кінцевого користувача. Проте велика кількість параметрів шифрування та тунелювання на стороні сервера створює високий поріг входу для адміністратора та підвищує ризик виникнення помилок при конфігурації [9]. Тому $E_5 = 0,6; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,65 + 0,2 \cdot 0,6 + 0,2 \cdot 0,6 + 0,15 \cdot 0,7 + 0,15 \cdot 0,6 = 0,63 \cdot$

Підсумкова оцінка для L2TP/IPsec при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,83 + 0,7 \cdot 0,63 = 0,69$ (середній рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,83 + 0,5 \cdot 0,63 = 0,73$ (середній рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,83 + 0,3 \cdot 0,63 = 0,77$ (високий рівень).

Наступним об'єктом аналізу є IPsec із механізмом IKEv2. Порівняння цього протоколу з попереднім дозволить кількісно оцінити переваги відмови від тунелювання L2 на користь роботи безпосередньо на мережевому рівні. Очікується, що оптимізація процесу обміну ключами та відсутність подвійної інкапсуляції забезпечать вищий баланс між захищеністю та швидкодією.

Аналіз захищеності IPsec(IKEv2) (S_{VPN}):

− IPsec (IKEv2) підтримує найсучасніші криптографічні алгоритми шифрування (AES-128/256, ChaCha20), надійні методи хешування (SHA-2) та стійкі механізми обміну ключами

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

(Diffie-Hellman, ECDH). Проте протокол все ще допускає активацію застарілих криптографічних наборів (3DES, SHA-1), які можуть бути увімкнені внаслідок некоректної конфігурації для забезпечення зворотної сумісності [9]. Тому $S_1 = 0,9; w_1 = 0,3$;

− Протокол забезпечує гнучку автентифікацію на основі попередньо спільних ключів (PSK), цифрових сертифікатів X.509 та сучасних EAP-методів, що дозволяє використовувати його у великих корпоративних мережах із підтримкою двофакторної перевірки. Проте використання PSK залишається потенційно вразливим місцем у разі компрометації ключа на одному з вузлів, а розгортання сертифікатів вимагає складної інфраструктури [10]. Тому $S_2 = 0,85; w_2 = 0,2$;

− IPsec (IKEv2) реалізує високий ступінь захисту від атак типу Man-in-the-Middle, replay та downgrade за рахунок використання криптографічно захищеного встановлення сеансу, нумерації пакетів та перевірки цілісності. Проте протокол залишається чутливим до атак на виснаження ресурсів (DoS) на етапі ініціалізації з'єднання, а реальна стійкість залежить від коректності налаштування параметрів Security Associations [10]. Тому $S_3 = 0,85; w_3 = 0,2$;

− Протокол нативно підтримує Perfect Forward Secrecy (PFS), регулярну ротацію ключів та автоматичне переустановлення тунелів (технологія MOBIKE), що суттєво підвищує рівень безпеки при зміні мережевих адрес. Проте в деяких спрощених реалізаціях PFS може бути вимкнено за замовчуванням, що потребує додаткового контролю з боку адміністратора [9]. Тому $S_4 = 0,9; w_4 = 0,15$;

− IPsec (IKEv2) є стандартизованим та стабільним протоколом із багаторічною історією експлуатації, який регулярно проходить незалежні аудити безпеки та підтримується всіма провідними виробниками обладнання. Проте складність самого стандарту іноді призводить до проблем сумісності між різними програмними стеками, що може створювати неочевидні вектори для атак [10]. Тому $S_5 = 0,85; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,9 + 0,2 \cdot 0,85 + 0,2 \cdot 0,85 + 0,15 \cdot 0,9 + 0,15 \cdot 0,85 = 0,87$.

Аналіз ефективності IPsec (IKEv2) (E_{VPN}):

− Пропускна здатність IKEv2 є дуже високою, оскільки протокол працює безпосередньо над IP-рівнем і не має надлишковості у вигляді подвійної інкапсуляції. Проте шифрування та додавання заголовків ESP все одно створюють певні накладні витрати, що дещо знижує корисну швидкість у порівнянні з передачею відкритих даних [10]. Тому $E_1 = 0,9; v_1 = 0,3$;

− Затримки в протоколі є мінімальними завдяки оптимізованому процесу встановлення з'єднання, який потребує меншої кількості пакетів для "рукостискання". Проте при активному використанні функції MOBIKE під час перемикання між різними типами мереж (наприклад, з Wi-Fi на 4G) можливі короткочасні мікрозатримки [10]. Тому $E_2 = 0,85; v_2 = 0,2$;

− Навантаження на ресурси системи є помірним, особливо за наявності апаратної підтримки алгоритмів AES у сучасних процесорах. Проте на мобільних пристроях постійна підтримка активних криптографічних сесій може призводити до підвищеного споживання енергії акумулятора [10]. Тому $E_3 = 0,8; v_3 = 0,2$;

− Масштабованість протоколу є високою, він ідеально підходить для мобільних клієнтів завдяки здатності утримувати тунель при зміні IP-адреси. Проте робота через UDP-порти 500/4500 робить його вразливим до блокування суворими міжмережевими екранами, що обмежує його застосування в деяких мережах [10]. Тому $E_4 = 0,85; v_4 = 0,15$;

− Налаштування клієнтської частини в сучасних операційних системах є досить простим і зручним для користувача. Проте конфігурація серверної частини вимагає високої кваліфікації через велику кількість параметрів узгодження фаз шифрування, що часто стає причиною помилок при розгортанні [10]. Тому $E_5 = 0,75; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,9 + 0,2 \cdot 0,85 + 0,2 \cdot 0,8 + 0,15 \cdot 0,85 + 0,15 \cdot 0,75 = 0,84$.

Підсумкова оцінка для IPsec (IKEv2) при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,87 + 0,7 \cdot 0,84 = 0,85$ (високий рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,87 + 0,5 \cdot 0,84 = 0,86$ (високий рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,87 + 0,3 \cdot 0,84 = 0,86$ (високий рівень).

Окремої уваги заслуговує протокол OpenVPN, який, на відміну від попередніх рішень, функціонує в просторі користувача (User Space). Важливо оцінити, як саме використання бібліотек OpenSSL та передача даних через контекстні перемикання впливає на критерії ефективності, та чи компенсується це гнучкістю налаштувань безпеки.

Аналіз захищеності OpenVPN (S_{VPN}):

− OpenVPN підтримує надзвичайно широкий спектр криптографічних алгоритмів завдяки використанню бібліотеки OpenSSL, включаючи AES-256, Camellia та ChaCha20. Проте через велику кількість підтримуваних конфігурацій існує ризик випадкового використання застарілих шифрів (наприклад, Blowfish), якщо адміністратор не налаштував параметри безпеки належним чином [11]. Тому $S_1 = 0,9; w_1 = 0,3$;

− Протокол забезпечує багаторівневу автентифікацію на основі цифрових сертифікатів X.509, логінів/паролів та статичних ключів. Проте складність керування інфраструктурою відкритих ключів (PKI) та сертифікатами для великої кількості клієнтів створює додаткові адміністративні ризики та вимагає суворого контролю за термінами дії сертифікатів [11]. Тому $S_2 = 0,85; w_2 = 0,2$;

− В протоколі реалізовано високий рівень захисту від атак типу Man-in-the-Middle та DoS завдяки використанню додаткового рівня TLS-автентифікації (HMAC-підпис). Проте робота в просторі користувача та великий обсяг програмного коду (Monolithic code) потенційно збільшують поверхню атаки порівняно з більш компактними протоколами, такими як WireGuard [11]. Тому $S_3 = 0,8; w_3 = 0,2$;

− Протокол нативно підтримує Perfect Forward Secrecy (PFS) та дозволяє гнучко налаштовувати частоту зміни ключів сесії. Проте за замовчуванням процес перегенерації ключів може бути інтенсивним для ресурсів, а некоректне налаштування параметрів Renegotiation може призводити до тимчасових розривів з'єднання у навантажених мережах [11]. Тому $S_4 = 0,85; w_4 = 0,15$;

− OpenVPN є одним із найбільш перевірених рішень із відкритим кодом, яке пройшло численні незалежні аудити безпеки. Проте зрілість протоколу також означає наявність великої кількості застарілих функцій для сумісності, що іноді ускладнює проведення швидкого аудиту нових версій системи [11]. Тому $S_5 = 0,9; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,9 + 0,2 \cdot 0,85 + 0,2 \cdot 0,8 + 0,15 \cdot 0,85 + 0,15 \cdot 0,9 = 0,86$.

Аналіз ефективності OpenVPN (E_{VPN}):

− Пропускна здатність OpenVPN оцінюється як середня через роботу протоколу в просторі користувача (User Space), що вимагає постійного копіювання даних між ядром та додатком. Проте використання стиснення трафіку та протоколу UDP дозволяє частково компенсувати ці витрати, хоча швидкість все одно поступається рішенням, інтегрованим у ядро ОС [11]. Тому $E_1 = 0,7; v_1 = 0,3$;

− Показники затримки можуть бути значними, особливо при використанні TCP як транспортного протоколу (явище TCP Meltdown). Проте навіть при роботі через UDP затримка залишається вищою за аналогічні показники IPsec через складніший процес інкапсуляції та обробки пакетів бібліотекою OpenSSL [11]. Тому $E_2 = 0,65; v_2 = 0,2$;

− Навантаження на ресурси системи є високим, оскільки шифрування та перемикання контексту між ядром і User Space вимагають значних потужностей процесора. Проте на сучасному обладнанні це стає критичним лише при обробці гігабітних каналів, тоді як для звичайних користувачів навантаження залишається в межах норми [11]. Тому $E_3 = 0,6; v_3 = 0,2$;

− Масштабованість та прохідність є найкращими серед усіх протоколів, оскільки OpenVPN може працювати на будь-якому порту (наприклад, TCP 443) і легко маскуватися під звичайний HTTPS-трафік. Проте централізована модель керування сертифікатами може стати вузьким місцем при спробі швидкого масштабування мережі на тисячі пристроїв [11]. Тому $E_4 = 0,9; v_4 = 0,15$;

− Налаштування серверної частини є досить складним і вимагає розуміння принципів роботи PKI та мережевої інкапсуляції. Проте наявність великої кількості готових конфігураційних файлів та графічних клієнтів для всіх ОС робить використання протоколу кінцевими користувачами максимально зручним [11]. Тому $E_5 = 0,75; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,7 + 0,2 \cdot 0,65 + 0,2 \cdot 0,6 + 0,15 \cdot 0,9 + 0,15 \cdot 0,75 = 0,71$.

Підсумкова оцінка для OpenVPN при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,86 + 0,7 \cdot 0,71 = 0,76$ (високий рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,86 + 0,5 \cdot 0,71 = 0,79$ (високий рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,86 + 0,3 \cdot 0,71 = 0,82$ (високий рівень).

Для аналізу сценаріїв обходу мережевих обмежень розглядається SSTP. Ключовим аспектом оцінювання тут є вплив інкапсуляції в HTTPS-канал на продуктивність. Необхідно визначити, наскільки використання TCP як транспортного протоколу знижує оцінку за критерієм затримок (E_2) порівняно з UDP-аналогами.

Аналіз захищеності SSTP (S_{VPN}):

− SSTP забезпечує високий рівень конфіденційності, оскільки використовує шифрування AES-256 через захищений SSL/TLS канал. Проте криптографічна стійкість напряму залежить від версії протоколу TLS, що використовується на сервері, і за наявності підтримки застарілих версій (наприклад, TLS 1.0/1.1) захист може бути вразливим до відомих атак на веб-протоколи [9]. Тому $S_1 = 0,85; w_1 = 0,3$;

− Протокол підтримує автентифікацію на основі цифрових сертифікатів X.509 для сервера та методів MS-CHAP v2 або EAP для користувачів. Проте використання сертифікатів вимагає надійної інфраструктури ключів, а вразливість MS-CHAP v2 до атак перебором паролів залишається слабким місцем, якщо не застосовуються додаткові методи захисту [8]. Тому $S_2 = 0,75; w_2 = 0,2$;

− В протоколі реалізовано надійний захист від атак типу Man-in-the-Middle завдяки перевірці автентичності сервера через сертифікати. Проте протокол є вразливим до специфічних атак на TCP-з'єднання (наприклад, TCP DoS), а закритий вихідний код реалізації від Microsoft не дозволяє провести незалежний повний аудит на наявність прихованих вразливостей [8]. Тому $S_3 = 0,8; w_3 = 0,2$;

− SSTP підтримує механізми управління ключами в рамках TLS-сесії, що забезпечує стабільність з'єднання. Проте протокол не завжди гарантує Perfect Forward Secrecy (PFS) за замовчуванням, оскільки це залежить від налаштувань наборів шифрів (Cipher Suites) на стороні Windows-сервера [9]. Тому $S_4 = 0,75; w_4 = 0,15$;

− Протокол є стандартизованим рішенням, яке пройшло тривалий період експлуатації в корпоративних середовищах Windows. Проте через закриту архітектуру та обмежену підтримку на інших платформах (Linux, macOS), ступінь глобальної довіри та зрілості оцінюється нижче, ніж у відкритих стандартів на кшталт IPsec [8]. Тому $S_5 = 0,8; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,85 + 0,2 \cdot 0,75 + 0,2 \cdot 0,8 + 0,15 \cdot 0,75 + 0,15 \cdot 0,8 = 0,8$.

Аналіз ефективності SSTP (E_{VPN}):

− Пропускна здатність SSTP є відносно низькою через значні накладні витрати на багаторівневу інкапсуляцію (PPP всередині HTTP поверх TLS/TCP). Проте використання TCP як транспортного протоколу створює додаткові затримки при повторних передачах пакетів, що суттєво обмежує реальну швидкість у порівнянні з UDP-протоколами [9]. Тому $E_1 = 0,6; v_1 = 0,3$;

− Показники затримки є вищими за середні, особливо в мережах із нестабільним зв'язком, де виникає конфлікт механізмів контролю потоку (TCP Meltdown). Проте для стабільних каналів затримка залишається прийнятною для офісної роботи, хоча вона значно перевищує показники IKEv2 або WireGuard [9]. Тому $E_2 = 0,55; v_2 = 0,2$;

− Навантаження на ресурси системи є помітним через складну обробку SSL-трафіку та роботу з TCP-стеком. Проте завдяки глибокій інтеграції в ядро Windows, протокол працює стабільніше за OpenVPN, хоча все одно вимагає значних потужностей процесора для шифрування [1]. Тому $E_3 = 0,65; v_3 = 0,2$;

− Масштабованість та прохідність є головними перевагами протоколу, оскільки він використовує стандартний TCP-порт 443 та легко проходить через будь-які міжмережеві екрани та NAT, оскільки його трафік не відрізняється від звичайного HTTPS-з'єднання з веб-сайтом [1]. Тому $E_4 = 0,95; v_4 = 0,15$;

− Налаштування SSTP на стороні клієнта Windows є максимально простим, оскільки він не потребує встановлення додаткового ПЗ. Проте на стороні сервера процедура конфігурації є складною, оскільки вимагає правильного налаштування сертифікатів та служб маршрутизації, що часто стає причиною помилок при розгортанні [1]. Тому $E_5 = 0,7; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,6 + 0,2 \cdot 0,55 + 0,2 \cdot 0,65 + 0,15 \cdot 0,95 + 0,15 \cdot 0,7 = 0,67$.

Підсумкова оцінка для SSTP при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,8 + 0,7 \cdot 0,67 = 0,71$ (середній рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,8 + 0,5 \cdot 0,67 = 0,74$ (середній рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,8 + 0,3 \cdot 0,67 = 0,76$ (високий рівень).

Завершує порівняльний аналіз протокол WireGuard, який представляє сучасний підхід до побудови VPN. Його оцінювання дозволить перевірити гіпотезу про те, що відмова від застарілих криптографічних наборів та оптимізація коду ядра здатні забезпечити максимальні бали одночасно як за критеріями захищеності (S_i), так і ефективності (E_i).

Аналіз захищеності WireGuard (S_{VPN}):

− WireGuard використовує жорстко визначений набір сучасних криптографічних примітивів: потоковий шифр ChaCha20, алгоритм автентифікації Poly1305, протокол обміну ключами Curve25519 та хеш-функцію BLAKE2s. Недоліком такого підходу є відсутність криптографічної гнучкості (Cryptographic Agility): протокол не дозволяє замінити ці алгоритми (наприклад, на AES) без зміни версії самого протоколу, що робить систему залежною від стійкості конкретно цього набору шифрів [12]. Тому $S_1 = 0,95; w_1 = 0,3$;

− Протокол забезпечує автентифікацію на основі обміну публічними ключами за аналогією з SSH, що значно надійніше за використання паролів. Проте відсутність вбудованої підтримки динамічного розподілу ключів та складність інтеграції з традиційними корпоративними методами (наприклад, RADIUS чи LDAP) без додаткових програмних надбудов ускладнює його впровадження у великих організаціях [12]. Тому $S_2 = 0,85; w_2 = 0,2$;

− Протокол забезпечує захист від сканування мережі, оскільки просто відкидає некоректні пакети і не надсилає жодних відповідей, поводячись так, ніби сервер вимкнений. Проте сервер зберігає у пам’яті IP-адреси клієнтів та час останнього з’єднання, що створює ризик розкриття особи користувачів, якщо зловмисники отримають фізичний доступ до обладнання [12]. Тому $S_3 = 0,9; w_3 = 0,2$;

− Протокол нативно підтримує Perfect Forward Secrecy (PFS) для кожного окремого сеансу та реалізує дуже швидку ротацію ключів за допомогою протоколу Noise. Проте через відсутність фази узгодження параметрів (Handshake відбувається миттєво), адміністратор має менше можливостей для тонкого контролю над життєвим циклом ключів у реальному часі [12]. Тому $S_4 = 0,95; w_4 = 0,15$;

− WireGuard є стандартизованим протоколом, який вже інтегрований безпосередньо в ядро Linux, що підтверджує високий рівень довіри розробників. Проте порівняно з IPsec чи OpenVPN, він є відносно новим рішенням, яке ще не пройшло такої ж кількості випробувань у реальних умовах експлуатації [12]. Тому $S_5 = 0,85; w_5 = 0,15$.

Тоді $S_{VPN} = \sum_{i=1}^{5} w_i \cdot S_i = 0,3 \cdot 0,95 + 0,2 \cdot 0,85 + 0,2 \cdot 0,9 + 0,15 \cdot 0,95 + 0,15 \cdot 0,85 = 0,91$.

Аналіз ефективності WireGuard (E_{VPN}):

− Пропускна здатність WireGuard є найвищою серед усіх розглянутих протоколів завдяки роботі в просторі ядра та використанню швидких алгоритмів ChaCha20. Проте на гігабітних каналах він демонструє мінімальні втрати швидкості, практично не поступаючись передачі даних без шифрування [12]. Тому $E_1 = 0,95; v_1 = 0,3$;

− Показники затримки є рекордно низькими, оскільки протокол перебуває в стані очікування і не підтримує постійний обмін службовими пакетами за відсутності корисного трафіку. Проте миттєве встановлення з’єднання дозволяє уникнути затримок, характерних для тривалого “рукостискання” в OpenVPN чи IPsec [12]. Тому $E_2 = 0,95; v_2 = 0,2$;

− Навантаження на ресурси системи є мінімальним, оскільки компактний код протоколу та оптимізовані алгоритми потребують значно менше циклів процесора. Завдяки ефективній багатопотоковій обробці він однаково добре працює як на потужних серверах, так і на малопотужних вбудованих системах чи смартфонах. [12]. Тому $E_3 = 0,95; v_3 = 0,2$;

− Масштабованість протоколу є високою для невеликих мереж, проте відсутність вбудованого механізму динамічного призначення IP-адрес (DHCP-like) вимагає ручного керування конфігураціями. Також використання стандартних UDP-портів може призводити до блокування в корпоративних мережах, що вимагає використання додаткових інструментів для маскування трафіку [12]. Тому $E_4 = 0,8; v_4 = 0,15$;

– Налаштування є вкрай простим: конфігурація зводиться до генерації пари ключів та вказання адрес кінцевих точок. Проте незвична логіка роботи (відсутність статусу з'єднання "connected/disconnected") може викликати певні труднощі у користувачів, звиклих до традиційних VPN-клієнтів [12]. Тому $E_5 = 0,9; v_5 = 0,15$.

Тоді $E_{VPN} = \sum_{i=1}^{5} v_i \cdot E_i = 0,3 \cdot 0,95 + 0,2 \cdot 0,95 + 0,2 \cdot 0,95 + 0,15 \cdot 0,8 + 0,15 \cdot 0,9 = 0,92$.

Підсумкова оцінка для WireGuard при різних коефіцієнтах пріоритету безпеки:

1) при $\alpha = 0,3$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,3 \cdot 0,91 + 0,7 \cdot 0,92 = 0,92$ (оптимальний рівень);

2) при $\alpha = 0,5$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,5 \cdot 0,91 + 0,5 \cdot 0,92 = 0,92$ (оптимальний рівень);

3) при $\alpha = 0,7$, $Rating_{VPN} = \alpha \cdot S_{VPN} + (1-\alpha) \cdot E_{VPN} = 0,7 \cdot 0,91 + 0,3 \cdot 0,92 = 0,91$ (оптимальний рівень).

На основі проведених розрахунків для кожного з досліджуваних протоколів, зведемо отримані підсумкові значення коефіцієнтів захищеності (S_{VPN}) та ефективності (E_{VPN}) у загальну табл. 4. Також занесемо до неї результати обчислення інтегрального рейтингу ($Rating_{VPN}$) для трьох сценаріїв пріоритетності (α): збалансованого ($\alpha = 0,5$), з акцентом на безпеку ($\alpha = 0,7$) та з акцентом на швидкодію ($\alpha = 0,3$).

Таблиця 4

Зведені показники захищеності, ефективності та інтегрального рейтингу VPN-протоколів

VPN-протокол	S_{VPN}	E_{VPN}	$Rating_{VPN}$		
			$\alpha = 0,3$	$\alpha = 0,5$	$\alpha = 0,7$
PPTP	0,23	0,88	0,68	0,56	0,43
L2TP/IPsec	0,83	0,63	0,69	0,73	0,77
IPsec(IKEv2)	0,87	0,84	0,85	0,86	0,86
OpenVPN	0,86	0,71	0,76	0,79	0,82
SSTP	0,8	0,67	0,71	0,74	0,76
WireGuard	0,91	0,92	0,92	0,92	0,91

Таким чином, проведений аналіз показав, що найкращим вибором за всіма показниками є WireGuard, який поєднує максимальну швидкість із сучасним захистом. Протокол IPsec (IKEv2) залишається "надійним високим" стандартом для бізнесу, тоді як OpenVPN, SSTP та L2TP/IPsec працюють помітно повільніше через застарілу архітектуру та велике навантаження на процесор. Розрахунки також підтвердили, що використовувати PPTP сьогодні не можна: попри високу швидкість, його захист є критично недостатнім та не відповідає сучасним вимогам інформаційної безпеки. Запропонований підхід з коефіцієнтом α дає можливість чітко обрати протокол під конкретну задачу.

Висновки

1. Розроблено підхід до комплексного оцінювання VPN-рішень, який базується на системі кількісних критеріїв, розподілених на показники захищеності та ефективності. Запропонована математична модель розрахунку інтегрального рейтингу, на відміну від існуючих підходів, використовує варіативний коефіцієнт пріоритетності, що забезпечує гнучкість процесу прийняття рішень та дозволяє адаптувати вибір технології до конкретних умов експлуатації.

2. Здійснено порівняльний аналіз сучасних VPN-протоколів, за результатами якого встановлено, що найбільш збалансованим рішенням є WireGuard, який поєднує високу продуктивність та сучасні криптографічні механізми. Протокол IPsec (IKEv2) підтвердив свою ефективність як надійний стандарт для корпоративних мереж.

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

3. Виявлено суттєві архітектурні обмеження протоколів OpenVPN, SSTP та L2TP/IPsec, ефективність яких знижується через значні накладні витрати обчислювальних ресурсів, що впливає на їх продуктивність у сучасних умовах.

4. Встановлено критичну вразливість протоколу PPTP, яка обумовлена використанням застарілих криптографічних механізмів, що робить його непридатним для використання у сучасних інформаційно-комунікаційних системах, незважаючи на високу швидкодію.

5. Практична цінність отриманих результатів полягає у створенні формалізованого інструментарію для обґрунтованого вибору VPN-технологій, що дозволяє системним адміністраторам мінімізувати ризики кіберзагроз та оптимізувати використання апаратних ресурсів відповідно до вимог конкретних задач.

Перелік посилань

1. Liu, Z. (2023). Application and Security Analysis of Virtual Private Network (VPN) in Network Communication. Academic Journal of Computing & Information Science, 6(11), 52–59. https://doi.org/ 10.25236/ AJCIS.2023.061108.

2. Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025). Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments under Simulated Network Conditions. Computers, 14(8), Article 326. https://doi.org/10.3390/computers14080326.

3. Demirdelen, T., & Kırmızı, S. (2025). Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations. Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 8(3), 1353–1369. https://doi.org/10.47495/okufbed.1660352.

4. Xue, D., Ramesh, R., Jain, A., Kallitsis, M., Halderman, J. A., Crandall, J. R., & Ensafi, R. (2022). OpenVPN is Open to VPN Fingerprinting. In Proceedings of the 31st USENIX Security Symposium (USENIX Security '22) (pp. 483–500). USENIX Association. https://www.usenix.org/conference/usenixsecurity22/presentation/xue.

5. Al-Fawa'reh, M., & Nashwan, S. (2022). VPN and Non-VPN Network Traffic Classification Using Time-Related Features. Computers, Materials & Continua, 72(2), 1939–1961. https://doi.org/10.32604/cmc.2022.025397.

6. Ткачов В. М., Чепурна І. С., Фесенко Т. Г. Метод мультирівневого VPN-тунелювання для забезпечення віддаленого доступу до вузлів екстранет-мережі. Вісник Херсонського національного технічного університету. 2024. № 3 (90). С. 299–308. https://doi.org/10.35546/kntu2078-4481.2024.3.37.

7. Лемешко А. В., Новіченко Є. О., Недавній А. В., Дурнєв Є. С., Стасюк А. В. Використання технології VPN під час воєнного стану в Україні. Зв'язок. 2022. № 5. С. 11–15. https://doi.org/10.31673/2412-9070.2022.051117.

8. Abbas, H., Balogun, A., Ugwu, C., Adewole, K., Usman, M. J., Shafi, I., Abayomi-Alli, A., Abdulkarim, M., & Bamgboye, O. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. ACM Computing Surveys, 55(13s), Article 273. https://doi.org/10.1145/3579162.

9. Barker, E., Souppaya, M., Barker, W., & Roginsky, A. (2020). Guide to IPsec VPNs (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-77r1.

10. Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296). IETF. https://www.rfc-editor.org/rfc/rfc7296.

11. OpenVPN Community. (2023). Reference manual for OpenVPN 2.6 [Електронний ресурс]. Режим доступу: https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/.

12. Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2017). Internet Society. https://www.ndss-symposium. org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/.

Oleksandra Matiyko
PhD, Associate Professor, Department of Cyber Defense and Security of Special Communications
National Technical University “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
ORCID: 0000-0002-6947-5958
E-mail: alexm1710@ukr.net

Roman Bratasyuk
cadet of the Institute of Special Communications and Information Protection
National Technical University “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
ORCID: 0009-0004-2241-3022
E-mail: romabratasuk@gmail.com

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814

Mykola Konotopets
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Cyber Defense and Security of Special Communications
National Technical University "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0000-0002-6963-1877
E-mail: nikolyalux@gmail.com

Oleksandr Turovskyi
Doctor of Technical Sciences, Professor, Head of the Department of Technical Systems of Cyber Defense
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4961-0876
E-mail: s19641011@ukr.net

ASSESSMENT OF SECURITY AND EFFICIENCY OF VPN SOLUTIONS IN INFORMATION AND COMMUNICATION SYSTEMS

Virtual private network technologies are one of the basic means of ensuring secure data transmission in modern information and communication systems. They allow to implement confidentiality, integrity and authenticity of information when transmitted over open networks. At the same time, the variety of VPN protocols and approaches to their implementation complicates the choice of the optimal solution taking into account the requirements for the level of security and system performance. Studies have shown that ensuring a high level of cryptographic protection is often accompanied by an increase in computational costs and a decrease in performance, which is critical for many applied tasks. Today, the issue of comprehensive evaluation of VPN protocols taking into account the simultaneous influence of security and efficiency indicators remains insufficiently studied. The article proposes an approach to evaluating VPN solutions based on the use of a system of generalized criteria that take into account both security indicators and operating efficiency. This approach allows to formalize the process of selecting a VPN protocol depending on the operating conditions of the information system and the priority of individual parameters. In particular, the features of the functioning and characteristics of modern VPN protocols are considered, their comparative analysis is carried out according to key indicators, including the level of cryptographic protection, bandwidth, latency and load on computing resources. The results obtained indicate the existence of a compromise between the level of security and efficiency, which necessitates the use of integral evaluation criteria. Recommendations are given for the selection of VPN protocols depending on the requirements for information security and system performance, which allows increasing the efficiency of building secure data transmission channels.

Keywords: VPN protocols, secure data transmission, cryptographic protection, information security.

Надійшла до редакції (Received): 06.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Матійко А.А., Братасюк Р.В., Конотопець М.М. Туровський О.Л. Оцінка захищеності та ефективності VPN-рішень в інформаційно-комунікаційних системах. Сучасний захист інформації, 2(66), 162–177. https://doi.org/10.31673/2409-7292.2026.022814