Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

23-24 листопада 2023 р.

Миколаїв ■ НУК ■ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

МАТЕРІАЛИ

XI Всеукраїнської науково-технічної конференції з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2023

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2023. – 223 с.

У збірнику подано матеріали XI Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, системи Інтернет речей (IoT), моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

3. Обфускація і захист програмних продуктів [Електронний ресурс]. – Режим доступу : http://www.citforum.ru/security/articles/obfus/

УДК 004.056.5:004.738.5

ІНФОРМАЦІЙНА БЕЗПЕКА ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ МЕРЕЖ

Автори: *Трибулькевич С.Л., ст. викладач; Трибулькевич В.В., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Мета роботи полягає у вивченні, аналізі та розробці стратегій та методів забезпечення захищеності корпоративних мереж під час віддаленого доступу. Основними завданнями є ідентифікація потенційних загроз та вразливостей, визначення ефективних заходів безпеки, розробка та впровадження політик безпеки, а також навчання персоналу щодо кращих практик забезпечення безпеки віддаленого доступу.

Віддалений доступ до корпоративних мереж став необхідною складовою сучасного бізнесу, особливо в умовах зростаючої мобільності та вимог до флексібільності робочого процесу. Із розвитком технологій зв'язку та інформаційних систем, багато компаній надають своїм співробітникам можливість працювати з будь-якого місця, використовуючи віддалений доступ до корпоративних ресурсів.

Проте разом із зручністю віддаленого доступу приходять і нові виклики щодо безпеки інформації. Забезпечення конфіденційності, цілісності та доступності даних стає основною турботою для багатьох організацій, які використовують віддалені технології.

У цьому контексті робота з інформаційною безпекою віддаленого доступу до корпоративних мереж набуває особливого значення. Вона спрямована на вивчення та аналіз потенційних загроз безпеці, розробку та впровадження ефективних стратегій захисту, а також навчання персоналу щодо кращих практик безпеки віддаленого доступу.

Зловмисники активно використовують різноманітні методи та техніки для атак на системи віддаленого доступу з метою отримання

несанкціонованого доступу до конфіденційної інформації, розповсюдження шкідливого програмного забезпечення або нанесення шкоди бізнесу:

1. Перехоплення даних: зловмисники можуть використовувати методи перехоплення трафіку мережі для зламування віддалених сесій та отримання конфіденційної інформації, такої як паролі, дані корпоративних проектів тощо.

2. Brute Force атаки: зловмисники можуть використовувати програми для автоматичного перебору паролів, намагаючись відгадати пароль доступу до віддаленого облікового запису.

3. Фішинг: атаки фішингу можуть спрямовуватися на користувачів, які використовують віддалений доступ, з метою отримання їхніх облікових даних шляхом підманювання їх до натискання на шкідливі посилання або завантаження шкідливих вкладень.

4. Використання слабкостей програмного забезпечення: зловмисники можуть використовувати відомі або невідомі вразливості в програмному забезпеченні, що використовується для віддаленого доступу, для отримання несанкціонованого доступу до системи.

5. Перехоплення сесії (Session Hijacking): зловмисники можуть намагатися використовувати вразливості в мережевих протоколах або програмах для перехоплення сесії віддаленого доступу та отримання контролю над ним.

6. Атаки з використанням вразливостей в програмному забезпеченні: зловмисники можуть експлуатувати вразливості в програмному забезпеченні VPN клієнтів або серверів для отримання несанкціонованого доступу.

На сьогоднішній день найбільш популярні протоколи VPN наступні:

1. OpenVPN - відкритий протокол, який широко використовується для своєї надійності та безпеки. Він працює на основі SSL/TLS і підтримує різні типи шифрування.

2. L2TP/IPsec (Layer 2 Tunneling Protocol over IPsec) комбінує переваги IPsec для забезпечення безпеки та L2TP для створення тунелю. Цей протокол часто використовується на мобільних пристроях.

3. WireGuard вважається одним з найшвидших та найпростіших у використанні протоколів VPN. Він має менше коду порівняно з іншими протоколами, що сприяє зменшенню можливостей для вразливостей.

4. SSTP (Secure Socket Tunneling Protocol) - це інший протокол VPN, який забезпечує безпеку при передачі даних через віддалені з'єднання. Він розроблений компанією Microsoft і використовує SSL для шифрування трафіку між клієнтом і сервером

Якщо порівнювати OpenVPN з іншими протоколами VPN, то можна виділити наступне:

1. Безпека. OpenVPN забезпечує високий рівень безпеки завдяки шифруванню трафіку за допомогою сильних алгоритмів ідентифікації та шифрування. Він використовує SSL/TLS для аутентифікації і обміну ключами, що робить його дуже відповідним для захисту конфіденційності даних під час передачі через незахищені мережі.

2. Гнучкість. OpenVPN може працювати на різних портах і протоколах, що дозволяє йому обходити обмеження мережі та брандмауери. Він також підтримує різні методи аутентифікації, включаючи пароль, сертифікати та двофакторну аутентифікацію.

3. Швидкодія. Зазвичай OpenVPN забезпечує хорошу швидкодію, але в порівнянні з деякими іншими протоколами, такими як WireGuard, він може мати трохи більший наклад через складніші механізми шифрування.

4. Підтримка. OpenVPN підтримується на багатьох платформах, включаючи Windows, macOS, Linux, Android та iOS. Це робить його дуже універсальним і зручним для використання на різних пристроях та операційних системах.

Отже, якщо врахувати вищезазначені переваги, OpenVPN може бути вважаний одним із найбільш захищених та універсальних протоколів VPN, здатний забезпечити безпеку та приватність під час віддаленого доступу до корпоративних мереж.

Структурна схема системи віддаленого доступу наведена на рис. 1.

Вихід в інтернет здійснюється через головний маршрутизатор з білою IP адресою. Функції обробки запитів та безпеки покладено на OpevVPN сервер, який працює по протоколу UDP за допомогою тунельного (TUN) драйверу. На головному маршрутизаторі UDP порт 1194 (стандартний порт OpenVPN, для безпеки або приховування та маскування трафіку може бути змінений на будь-який інший, наприклад,

443) прокинуто у внутрішню мережу до сервера віддаленого доступу, на якому налаштовано маршрутизацію трафіку. Віддалені користувачі, у залежності від задач, можуть підключатися до віддаленого робочого столу до своїх власних робочих комп’ютерів або до термінальних серверів. При даній реалізації трафік проходить через тунель з шифруванням та відсутнє програмне забезпечення сторонніх розробників із закритим кодом, а також відсутній протокол RDP із прямим виходом у глобальну мережу.

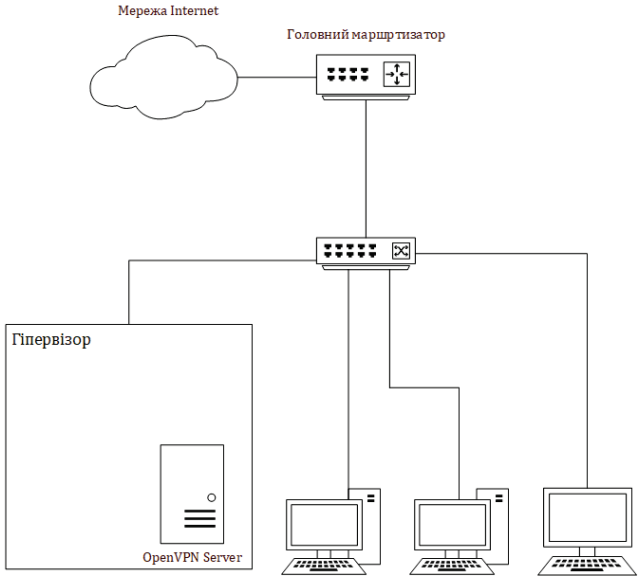

Рисунок 2.1 – Структурна схема системи

Висновки. Досліджено та проаналізовано питання безпеки під час використання віддаленого доступу до корпоративних мереж. Визначено основні загрози та ризики, пов'язані з цим процесом, а також розглянуто методи та стратегії захисту. Обрано OpenVPN як протокол VPN для забезпечення безпеки віддаленого доступу. OpenVPN відомий своєю надійністю, гнучкістю та високим рівнем шифрування, що робить його відмінним вибором для організацій, які прагнуть захистити свої корпоративні мережі під час віддаленої роботи.

Враховуючи усі аспекти слід зазначити, що ефективна інформаційна безпека віддаленого доступу до корпоративних мереж є важливою складовою для забезпечення безпеки та захисту конфіденційної інформації. Використання правильних інструментів та стратегій захисту, таких як OpenVPN, може допомогти організаціям забезпечити безпеку своїх даних у віддаленому режимі роботи.

Список літератури:

1. Александр Харкер. "OpenVPN Cookbook". Packt Publishing, 2017.
2. Майк Черчілло. "Mastering OpenVPN". Packt Publishing, 2015.
3. Майк МакКінлі. "OpenVPN: Building and Integrating Virtual Private Networks". O'Reilly Media, 2006.
4. Ерік Форті. "Virtual Private Networks, Second Edition". O'Reilly Media, 2005
5. Джон Вілкс. "SSL and TLS: Theory and Practice". Addison-Wesley Professional, 2009.
6. Найден Хібберт. "The Official (ISC)2 Guide to the CISSP CBK Reference, Fifth Edition". Sybex, 2019.
7. Хільбрукс Д.М., Сілва Л.М. "Кібербезпека: підручник". Видавництво КНЕУ, 2019.
8. Артем Остапець. "Безпека інформаційних технологій". Видавництво Національного університету "Львівська політехніка", 2018.
9. Дуглас Е. Комер. "Криптографія і безпека комп'ютерних мереж". Видавництво "ТОРСІНГ Плюс", 2019.
10. Б. Шнайдер. "SSL/TLS Essentials: Securing the Web". O'Reilly Media, 2000.