ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ НА БАЗІ VPN »

Виконав: студент 6 курсу, групи БСДМ-62
Спеціальність: 125 Кібербезпека
освітньо-професійної програми
«Інформаційна та кібернетичка безпека»

Осадчий Максим Станіславович

Керівник Кожухівськи А.Д.
Рецензент
Нормоконтролер Чумак Н.С.

КИЇВ – 2023

РЕФЕРАТ

Текстова частина бакалаврської роботи: 63 сторінки, 8 таблиць, 18 джерел.

Об'єкт дослідження - забезпечення безпеки користування інформаційними систем на базі VPN.

Предметом дослідження є обґрунтування рекомендацій та можливості застосування VPN для захисту інформаційних систем організації для віддалених користувачів.

Мета роботи - розглянути сучасний стан сервісів VPN, можливості його застосування в сучасний умовах для захисту інформаційних систем, сформувати рекомендації вибору та впровадження відповідних технологій.

Методи дослідження - полягає в розробці обґрунтованих рекомендацій щодо вибору та застосування VPN на підприємствах для віддалених користувачів.

В роботі проведено аналіз проблеми застосування віддаленими користувачами доступу до інформаційних систем за допомогою VPN та визначена мета та завдання вибору корпоративної бізнес-VPN для ефективного захисту інформаційних систем підприємств різного розміру та різного рівня доступу віддалених користувачів. Проаналізовано існуючі технології та провайдери VPN.

Досліджено методи та підходи до вибору певних провайдерів VPN в залежності від розмірів підприємства, його фінансового стану та можливостей підтримки відповідних технологій, а також технічних можливостей доступу до інформаційних ресурсів користувачів, зокрема віддалених. Визначено призначення, основні функції, переваги та недоліки основних сучасний провайдерів VPN.

На основі дослідження проведених в роботі розроблено технологію вибору провайдеру VPN в залежності від вимог підприємства, фінансових факторів, форм-мажорів, кількості віддалених співробітників, геополітичних умов тощо.

Галузь використання – захист інформаційної системи на підприємстві за допомогою VPN.

ІНФОРМАЦІЯ, ЗАХІИСТ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, VPN, ВІДДАЛЕНИЙ ДОСТУП, ІНФОРМАЦІЙНІ СИСТМЕМИ, ВІДДАЛЕНИЙ КОРСИТУВАЧ

ABSTRACT

Master’s thesis: 63 pages, 8 tables, 18 sources.

Object of research – ensuring the security of using VPN-based information systems.

Subject of research is the substantiation of recommendations and the possibility of using VPN to protect the organization's information systems for remote users.

The aim of research – consider the current state of VPN services, the possibilities of its application in modern conditions for the protection of information systems, form recommendations for the selection and implementation of appropriate technologies.

Research methods – is to develop sound recommendations for choosing and deploying enterprise VPNs for remote users.

The work analyzes the problem of using access to information systems by remote users using VPN and defines the purpose and task of choosing a corporate business VPN for effective protection of information systems of enterprises of different sizes and different access levels of remote users. Existing technologies and VPN providers are analyzed.

The methods and approaches to the selection of certain VPN providers depending on the size of the enterprise, its financial condition and the ability to support relevant technologies, as well as the technical capabilities of accessing users' information resources, in particular remote ones, were studied. The purpose, main functions, advantages and disadvantages of the main modern VPN providers are defined.

Based on the research carried out in the work, the technology for choosing a VPN provider was developed depending on the requirements of the enterprise, financial factors, form-majors, the number of remote employees, geopolitical conditions, etc.

Field of use – protection of the information system at the enterprise using VPN.

INFORMATION, INFORMATION PROTECTION, CYBER SECURITY, VPN, REMOTE ACCESS, INFORMATION SYSTEMS, REMOTE USER

ЗМІСТ

РОЗДІЛ 1. Інформаційні системи та їх захист 11
1.1. Захист інформаційних систем 11
1.2. Концепція технології VPN 17
1.2. Переваги технології VPN 18
1.3. Приватність та VPN 19
1.4. Мобільні пристрої та VPN 20
1.5. Законність використання VPN 21
РОЗДІЛ 2. Технології та програмне забезпечення 22
для захисту інформаційних систем користувачів на базі VPN 22
2.1. Захист за допомогою VPN 22
2.1.1. Тунелювання 23
2.1.2. Шифрування 23
2.2. Типи VPN 24
2.3. Протоколи VPN 25
2.3.1. Lightway 26
2.3.2. OpenVPN 27
2.3.3. WireGuard 28
2.3.4. Layer2 Tunnel Protocol 29
2.3.5. Secure Socket Tunneling Protocol 30
2.3.6. Internet Key Exchange Version 2 31
2.3.7. Point-to-Point Tunneling Protocol 32
2.4. Переваги та недоліки використання VPN для захисту інформаційних систем 33
РОЗДІЛ 3. Технологія застосовування VPN 37
3.1. VPN та захист інформаційних систем 37
3.2. Постачальники VPN та особливості технологій, що застосовуються 38
3.2.1. Perimeter 81 38
3.2.2 NordLayer 40

3.2.3 Twingate 41
3.2.4 GoodAccess 42
3.2.5 CyberGhost 43
3.2.6 IPVanish 44
3.2.7 ExpressVPN 45
3.3 Пошук найкращих VPN для бізнесу: методологія 47
3.4 Загальна технологія вибору VPN 48
3.5. Технології вибору VPN для підприємств 51
3.6 Бізнес-альтернативи VPN 52
3.7. Мережі VPN, яких слід уникати 52
3.8. Рекомендації щодо вибору VPN 53
3.9. Обмеження VPN 55
ВИСНОВКИ 58
ПЕРЕЛІК ПОСИЛАНЬ 60
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN - Virtual Private Network

eVPN - Ethernet Virtual Private Network

Wi-Fi - Wireless Fidelity

IP - Internet Protocol

ISP - Internet Service Provider

IAM - Identity and Access Management

TCP Transmission Control Protocol

UDP - User Datagram Protocol

IPsec - Internet Protocol Security

SSL - Secure Sockets Layer

SSH - Secure SHell

TLS - Transport Layer Security

ACL - Access Control List

RBAC -Role Based Access Control

AES - Advanced Encryption Standard

NAT - Network Address Translation

L2TP - Layer2 Tunnel Protocol

PPTP -Point-to-Point Tunneling Protocol

AES-CBC - Advanced Encryption Standard- Cipher Block Chaining

AES-GCM - Advanced Encryption Standard-Galois/Counter Mode

SSTP - Secure Socket Tunneling Protocol

IKE - Internet Key Exchange

RDP - Remote Desktop Protocol

VNC - Virtual Network Computing

SASE - Secure access service edge

HMAC - hash-based message authentication code

SHA - Secure Hash Algorithm

DNS - Domain Name System

IPv6 - Internet Protocol version 6

WebRTC - Web Real Time Communications

MPLS - Multiprotocol Label Switching

ZTNA - Zero Trust Network Access

SD-WAN - Software-Defined Networking in a Wide Area Network

WAF - Web Application Firewall

IPS - Image Packaging System

ВСТУП

Актуальність дослідження. Тенденція до віддаленої роботи пропонує низку переваг для бізнесу, таких як гнучкість співробітників, зменшення витрат на офісні приміщення тощо. Однак це пов'язано з певними проблемами. Зокрема, організаціям необхідно визначити, як вони можуть найкраще захистити свої мережі та конфіденційні дані, коли значний відсоток їхніх співробітників виконує роботу з персональних пристроїв і в публічних мережах.

Без належного захисту віддалені працівники, підключені до корпоративної інформаційної мережі з віддаленого робочого місця, можуть наражати корпоративну інформацію на небезпеку. Це пояснюється тим, що доступ до Інтернету через повністю публічну мережу, тобто через звичайного постачальника послуг Інтернету (ISP), наражає пристрої та онлайн-активність зловмисників. Це не означає, що кожного разу, коли працівник виконує роботу з віддаленого місця, він піддає ризику інформацію з якою працює інформаційна система підприємства. Без будь-яких заходів захисту, це полегшує роботу тих, хто має намір перехопити інформацію.

Для багатьох користувачів вирішення цієї проблеми – це корпоративна мережа VPN. Ця технологія може фактично з'єднати цілі філії з центральним офісом, дозволяючи командам у територіально розподілених організаціях працювати разом, обмінюватися важливою інформацією та залишатися в одному додатку або інформаційному просторі.

Також, з огляду на те, що більшість кібератак спрямовано на малий і середній бізнес, захист онлайн-активності є надзвичайно важливим, ніж будь-коли. Дистанційна робота та віддалена робота стають все більш популярними, тому співробітники піклуються про бізнес майже з усіх куточків світу — і найчастіше покладаються в цьому процесі на незахищені загальнодоступні мережі.

Робота з будь-якого місця стала синонімом сучасної роботи, однак це може коштувати величезних витрат. Але є способи зменшити цей ризик. VPN дозволяє користувачам отримувати віддалений доступ до мереж, тож працівники можуть працювати поза фізичним офісом і все ще безпечно отримувати доступ до

мережевих ресурсів — це лише одна з багатьох причин, чому ця технологія широко використовується в бізнес-середовищі.

VPN використовують шифрування для створення безпечного з'єднання через незахищену інфраструктуру Інтернету. VPN є одним із способів захисту корпоративних даних і керування доступом користувачів до цих даних. VPN захищають дані, коли користувачі взаємодіють із програмами та веб-ресурсами через Інтернет, і вони можуть приховувати певні ресурси. Вони зазвичай використовуються для контролю доступу, однак інші рішення для керування ідентифікацією та доступом (IAM) також можуть допомогти з керуванням доступу користувачів.

Шифрування – це спосіб кодування даних, щоб лише авторизовані сторони могли зрозуміти інформацію. Ефект цього шифрування полягає в тому, що з'єднання VPN залишаються приватними, навіть якщо вони передаються через загальнодоступну інфраструктуру Інтернету.

Багато компаній використовують VPN для контролю доступу — іншими словами, щоб контролювати, які користувачі мають доступ до ресурсів. Компанія може встановити кілька різних VPN, і кожна VPN відповідає за захист різних внутрішніх ресурсів. Одні й ті самі користувачі цих VPN можуть мати різні рівні доступу до даних.

Контроль і керування доступом має вирішальне значення для захисту корпоративних даних. Без контролю доступу неавторизовані користувачі можуть переглядати або змінювати конфіденційні дані, що призведе до витоку даних.

Донедавна найпоширенішими типами випадків використання VPN були віддалений доступ і Site-to-Site. VPN віддаленого доступу є більш популярною версією, оскільки вони надають і контролюють доступ до сервера VPN, розміщеного в приватній мережі, і користувачі безпечно підключаються до мережі за допомогою клієнтських програм VPN, встановлених на пристроях.

Як випливає з назви, остання технологія VPN нового покоління, Cloud VPN, спеціально розроблена для хмари; локальне обладнання не потрібне. Це важлива

подія, оскільки кількість компаній, які обирають хмарні, а не власні центри обробки даних, швидко зростає.

Об'єкт дослідження - забезпечення безпеки користування інформаційними систем на базі VPN.

Предметом дослідження є обґрунтування рекомендацій та можливості застосування VPN для захисту інформаційних систем організації для віддалених користувачів.

Мета роботи - розглянути сучасний стан сервісів VPN, можливості його застосування в сучасний умовах для захисту інформаційних систем, сформувати рекомендації вибору та впровадження відповідних технологій.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту корпоративних інформаційних систем;

встановити сутність завдань захисту інформаційних систем та віддалених користувачі на базі VPN;

проаналізувати існуючі технології захисту інформаційних систем на базі VPN;

проаналізувати методи та засоби забезпечення роботи віддалених користувачів з інформаційними системами на базі VPN;

проаналізувати основні принципи реалізації захисту інформаційних системам з використанням VPN.

Методи дослідження - полягає в розробці обґрунтованих рекомендацій щодо вибору та застосування VPN на підприємствах для віддалених користувачів.

Методи дослідження – опрацювання літератури за даною темою, аналіз стандартів та їх порівняння, побудова технології захисту інформаційної системи організації віддалених користувачів на базі VPN.

РОЗДІЛ 1. Інформаційні системи та їх захист

Комп’ютери та інші цифрові пристрої стали важливими для підприємств, вони дедалі частіше стають об’єктами атак. Для того, щоб компанія чи окрема особа могли впевнено використовувати комп’ютерний пристрій, вони спочатку повинні бути впевнені, що пристрій захищений та що всі комунікації будуть безпечними.

Захищаючи інформацію, необхідно мати можливість обмеження доступ для тих, кому дозволено її переглядати; всім іншим має бути заборонено дізнаватися що-небудь про його зміст. Це суть конфіденційності.

Цілісність — це впевненість у тому, що інформація, до якої здійснюється доступ, не була змінена та справді відповідає призначенню. Інформація може втратити свою цілісність через зловмисний намір, наприклад, коли неавторизована особа вносить зміни, щоб навмисно спотворити наявні данні. Цілісність також може бути втрачена ненавмисно, наприклад, коли стрибок напруги комп’ютера пошкоджує файл або хтось, уповноважений вносити зміни, випадково видаляє файл або вводить неправильну інформацію.

Доступність означає, що будь-хто, уповноважений на це, може отримати доступ до інформації та змінити її у відповідний проміжок часу.

Таким чином інформаційна безпека базується на трьох засадах: конфіденційність, цілісність та доступність.

1.1. Захист інформаційних систем

Щоб забезпечити конфіденційність, цілісність і доступність інформації, організації можуть використовувати наступні інструменти:

- Автентифікація;
- Управління доступом;
- Шифрування;
- Безпека пароля;
- Резервні копії;
- Брандмауери;

- Система виявлення вторгнень;
- Віртуальні приватні мережі (VPN);
- Фізична безпека;
- Політика безпеки;
- Мобільна безпека;
- Юзабіліті;
- Безпека особистої інформації.

Автентифікація. Автентифікація – це підтвердження того, ким є користувач на вході. Це проходження перевірки автентичності. Авторизація – це те, що користувачу дозволяється робити після входу. Це надання і перевірка прав на вчинення будь-яких дій в системі.

Найпоширенішою формою автентифікації сьогодні є ідентифікатор (логін) користувача та пароль. У цьому випадку автентифікація виконується шляхом підтвердження того, що користувач знає свій ідентифікатор та пароль. Але цю форму автентифікації легко обійти, і іноді потрібні більш надійні форми автентифікації. Якщо ідентифікаційний маркер втрачено або викрадено, ідентифікаційну інформацію можна легко вкрасти. Тому кращим ідентифікатором користувача є його фізичні характеристик, такі як сканування ока або відбиток пальця. Більш безпечний спосіб автентифікації користувача — багатофакторна автентифікація. Поєднуючи два чи більше факторів стає набагато важче представити потрапити сторонній особі у систему.

Після автентифікації користувача наступним кроком є переконатися, що він може отримати доступ лише до відповідних інформаційних ресурсів. Це робиться за допомогою контролю доступу. Контроль доступу визначає, хто з користувачів має право читати, змінювати, додавати та/або видаляти інформацію. Існує кілька різних моделей контролю доступу. Розглянемо наступні:

- список керування доступом (ACL)
- контроль доступу на основі ролей (RBAC).

Для кожного інформаційного ресурсу, яким організація хоче керувати, можна створити список користувачів, які мають можливість виконувати певні дії. Це список керування доступом або ACL. Для кожного користувача призначаються певні можливості, такі як читання, запис, видалення або додавання. Лише користувачі з такими можливостями можуть виконувати ці функції. Якщо користувача немає в списку, він не має можливості навіть знати про існування інформаційного ресурсу.

ACL прості для розуміння та обслуговування. Однак вони мають кілька недоліків. Основним недоліком є те, що кожний інформаційний ресурс управляється окремо, тому, якщо адміністратор безпеки захоче додати або видалити користувача до більшого набору інформаційних ресурсів, це буде досить важко. І зі збільшенням кількості користувачів і ресурсів, ACL стає важче підтримувати.

Це призвело до вдосконаленого методу контролю доступу, який називається контроль доступу на основі ролей або RBAC. За допомогою RBAC замість надання певним користувачам прав доступу до інформаційного ресурсу користувачам призначаються ролі, а потім цим ролям призначається доступ. Це дозволяє адміністраторам окремо керувати користувачами та ролями, спрощуючи адміністрування та, як наслідок, покращуючи безпеку.

Шифрування. Організаціям потрібно передавати інформацію через Інтернет або переносити її на зовнішні носії. У цих випадках навіть за належної автентифікації та контролю доступу неавторизована особа може отримати доступ до даних. Шифрування – це процес кодування даних під час їх передачі або зберігання, щоб лише авторизовані особи могли їх прочитати. Це кодування виконується комп’ютерною програмою, яка кодує звичайний текст, який потрібно передати; потім одержувач отримує зашифрований текст і декодує його (дешифрування). Щоб це працювало, відправник і одержувач повинні домовитися про метод кодування, щоб обидві сторони могли правильно спілкуватися. Обидві сторони мають спільний ключ шифрування, що дозволяє їм кодувати та декодувати повідомлення один одного. Це називається шифруванням із симетричним ключем.

Цей тип шифрування є проблематичним, оскільки ключ доступний у двох різних місцях.

Альтернативою шифруванню з симетричним ключем є шифрування з відкритим ключем. У шифруванні з відкритим ключем використовуються два ключі: відкритий і закритий. Щоб надіслати зашифроване повідомлення, ви отримуєте відкритий ключ, кодуєте повідомлення та надсилаєте його. Потім одержувач використовує закритий ключ для його декодування. Відкритий ключ можна надати кожному, хто бажає надіслати одержувачу повідомлення. Кожному користувачеві просто потрібен один приватний ключ і один відкритий ключ, щоб захистити повідомлення. Приватний ключ необхідний, щоб розшифрувати щось, надіслане з відкритим ключем.

Із збільшенням використання інформаційних систем та цифрових платформ для роботи, важливих транзакцій існує висока потреб захисту даних від кіберзлочинців. І одним із таких способів запобігти захопленню даних інформаційних систем є використання VPN.

Одним із таких інструментів захисту є технологія VPN - ця технологія може фактично з’єднати цілі філії з центральним офісом, дозволяючи командам у територіально розкиданих організаціях працювати разом, обмінюватися важливою інформацією. VPN дозволяє користувачеві, який знаходиться за межами корпоративної мережі, обійти брандмауер і отримати доступ до внутрішньої мережі ззовні. Завдяки поєднанню програмного забезпечення та заходів безпеки це дозволяє організації дозволити обмежений доступ до своїх мереж, водночас забезпечуючи загальну безпеку.

Безпека пароля. На підприємстві необхідно запровадити правильнуполітику паролів, щоб гарантувати, що паролі не можуть бути викрадені. Для цього слід виставати спіробітникам наступні прості, але досить ефективні критерії для створення паролів:

- Складний пароль;
- Регулярна зміна пароля;
- Нерозголошення паролів.

Резервні копії. Іншим важливим інструментом інформаційної безпеки є комплексний план резервного копіювання для всієї організації. Слід створювати резервні копії не лише даних на корпоративних серверах, але й окремих комп'ютерів, які використовуються в організації. Хороший резервний план повинен складатися з кількох компонентів.

Брандмауери. Брандмауер може існувати у вигляді апаратного чи програмного забезпечення (або обох). Апаратний брандмауер – це пристрій, підключений до мережі та фільтруючий пакети на основі набору правил. Програмний брандмауер працює в операційній системі та перехоплює пакети, щойно вони надходять на комп'ютер. Брандмауер захищає всі сервери та комп'ютери компанії, зупиняючи пакети ззовні мережі організації, які не відповідають суворому набору критеріїв. Брандмауер також може бути налаштований для обмеження потоку пакетів, що залишають організацію. Це може бути зроблено, щоб виключити можливість перегляду відео YouTube або використання Facebook із комп'ютера компанії.

Деякі організації можуть запровадити кілька брандмауерів як частину конфігурації безпеки мережі, створивши одну або кілька частково захищених частин своєї мережі. Цей сегмент мережі називають DMZ, запозичивши термін демілітаризована зона у військових, і це місце, де організація може розміщувати ресурси, які потребують більш широкого доступу, але все ще потребують безпеки.

Система виявлення вторгнень. Іншим пристроєм, який можна розмістити в мережі з метою безпеки, є система виявлення вторгнень або IDS. IDS не додає додаткової безпеки; натомість він надає функціональні можливості для виявлення атаки на мережу. IDS можна налаштувати для спостереження за певними типами дій, а потім сповіщення персоналу служби безпеки, якщо така діяльність відбувається. IDS також може реєструвати різні типи трафіку в мережі для подальшого аналізу. IDS є важливою частиною будь-якої надійної системи безпеки.

Віртуальні приватні мережі (VPN). Використовуючи брандмауери та інші технології безпеки, організації можуть ефективно захистити багато своїх інформаційних ресурсів, зробивши їх невидимими для зовнішнього світу. Але

інколи працівнику, який працює вдома (віддалений користува), потрібен доступ до деяких із цих ресурсів? У цих випадках використовують віртуальну приватну мережу (VPN).

VPN дозволяє користувачеві, який знаходиться за межами корпоративної мережі, обійти брандмауер і отримати доступ до внутрішньої мережі ззовні. Завдяки поєднанню програмного забезпечення та заходів безпеки це дозволяє організації дозволити обмежений доступ до своїх мереж, водночас забезпечуючи загальну безпеку.

Фізична безпека. Організація може запровадити найкращу у світі схему автентифікації, розробити найкращий контроль доступу та встановити брандмауери та засоби запобігання вторгненням, але її безпека не може бути повною без впровадження фізичної безпеки. Фізична безпека — це захист фактичного обладнання та мережевих компонентів, які зберігають і передають інформаційні ресурси. Щоб запровадити фізичну безпеку, організація повинна ідентифікувати всі вразливі ресурси та вжити заходів, щоб гарантувати, що ці ресурси неможливо фізично підробити або вкрасти.

Політика безпеки. Окрім перелічених вище технічних засобів контролю, організаціям також необхідно запровадити політику безпеки як форму адміністративного контролю. Насправді ці політики повинні бути відправною точкою в розробці загального плану безпеки. Хороша політика інформаційної безпеки містить вказівки щодо використання працівниками інформаційних ресурсів компанії та забезпечує компанію регресом у випадку, якщо працівник порушує політику.

Мобільна безпека. Оскільки використання мобільних пристроїв, таких як смартфони та планшети, поширюється, організації повинні бути готові вирішувати проблеми безпеки, пов’язані з використанням цих пристроїв. Одне з перших питань, яке повинна розглянути організація, це чи дозволяти мобільні пристрої на робочому місці взагалі. Створення політики BYOD («Візьміть свій власний пристрій») дозволяє співробітникам повніше інтегрувати себе у свою роботу та може принести працівникам більше задоволення та продуктивності. У багатьох

випадках може бути практично неможливо заборонити співробітникам мати власні смартфони чи iPad на робочому місці. Мобільні пристрої можуть створювати багато проблем безпеки для організації. Однією з найбільших проблем є крадіжка інтелекуальної власності.

Організаціям слід розглянути можливість розробки політики щодо мобільних пристроїв, яка стосується таких питань: використання камери, використання запису голосу, придбання програм, шифрування в стані спокою, налаштування автоматичного з'єднання Wi-Fi, налаштування Bluetooth, використання VPN (Virtual Private Network), налаштування пароля, звіт про втрачений або викрадений пристрій і резервне копіювання.

Юзабіліті. Прагнучи захистити інформаційні ресурси, організації повинні збалансувати потребу в безпеці з потребою користувачів ефективно отримувати доступ до цих ресурсів і використовувати їх. Якщо заходи безпеки системи ускладнюють її використання, користувачі знайдуть способи обійти безпеку, що може зробити систему більш вразливою, ніж це було б без заходів безпеки. Наприклад, розглянемо політику паролів. Якщо в організації потрібен надзвичайно довгий пароль із кількома спеціальними символами, працівник може записати його та покласти в ящик, оскільки запам'ятати його буде неможливо.

1.2. Концепція технології VPN

VPN (Virtual Private Network) розшифровується як віртуальна приватна мережа . Інтернет є загальнодоступною мережею, де файли можна передавати з одного комп'ютера на інший. Офісна мережа має фізичне підключення. Якщо, наприклад, компанія має десять комп'ютерів, які під'єднані через комутатор мережі, а не до Інтернету, це буде приватна мережа.

Спочатку віртуальні приватні мережі VPN створювалися як спосіб віддаленого доступу компаній до інших машин. По суті, віддалена машина «вважає», що вона в тій самій фізичній мережі. Тепер, коли VPN розвинулися для комерційного використання, їх можна використовувати для інших цілей. Підключення до

віддаленого сервера, який надсилає дані від вашого імені, наприклад проксі. Різниця між VPN і проксі полягає в тому, що VPN забезпечують більший захист завдяки шифруванню та вживає різних заходів на віддаленому сервері, щоб гарантувати анонімність користувача [1].

Отже VPN-тунель (також відомий як VPN - від англ. Virtual private network, віртуальна приватна мережа) - це зашифроване з'єднання між комп'ютером або мобільним пристроєм і Інтернетом. Так як це з'єднання зашифровано, то трафік, що по ньому проходить не можна перехопити, відстежити або змінити.

1.2. Переваги технології VPN

Технологія VPN має помітний ефект застосування, який перевершує інші мережеві технології під час її фактичного застосування в управлінні інформацією в інформаційних системах великих компаній. Технологія VPN широко використовувалася під час побудовb численних інформаційних систем для різних предметних областей.

Технологія VPN має ряд переваг:

1) Вартість використання технології VPN низька, що не впливає на мережеві витрати утримання мережі підприємства і певною мірою знижує вхідні витрати організації. З використанням технології VPN немає необхідності передавати інформацію через приватний інтернет канал та використовувати іншу мережеву систему через інший режим зв’язку з нижчими експлуатаційними ресурсами або створювати власну мережеву систему.

2) Під час використання технології VPN безпека та стабільність передачі інформаційних даних гарантована. Під час цього процесу застосовуються різні засоби безпеки таких як, перевірку особи користувачів, шифрування протоколу тунелювання та каналу тощо. Слід зазначити, що мережева адреса під час застосування технології VPN є різновидом криптографічної URL-адреси, тому вся

інформація про дані буде конфіденційною, що робить мережу VPN конфіденційною.

1.3. Приватність та VPN

Ступінь, до якого VPN робить користувач інформаційної системи захищеною, обмежена. З одного боку, VPN ускладнюють для інтернет-провайдера відстеження активності співробітника, наприклад спостереження за історією веб-перегляду. З іншого боку, все ще існують цифрові маркери, які можуть видати діяльність користувача веб-сайтам або інтернет-провайдеру.

У той час як корпорації все частіше звертаються до VPN, щоб надати своїм віддаленим працівникам і окремим філіям безпечний доступ до власної внутрішньої мережі, окремі користувачі також починають покладатися на послуги VPN. Точна мотивація використання VPN у кожної людини різна, але цей варіант став популярним для тих, хто хоче захистити свою онлайн-діяльність від перевірки, зокрема від стеження з боку державних організацій, зловмисників або провайдерів, які намагаються продати їх особисту інформацію.

За відсутності VPN, інтернет-провайдер може відстежувати активність співробітника в Інтернеті. Використовуючи VPN, дані користувача стають зашифрованими, а це означає, що особливості діяльності будуть незрозумілими навіть для тих, хто зможе їх переглянути. VPN працює між пристроєм (комп'ютер, ноутбук, телефон тощо) та Інтернетом, і тому третій особі важко побачити, які веб-сайти відвідують співробітники або що саме завантажують.

Зважаючи на це, співробітник не є повністю анонімними під час використання VPN, і деякі форми відстеження все ще можливі. Хоча оригінальна IP-адреса буде прихована замість неї VPN призначить нову IP-адресу, але все одно оригінальна IP-адреса підключається до VPN, перш ніж користувач спробує вийти в Інтернет.

Відповідно, додатковий рівень безпеки, який забезпечують VPN, слід розглядати як частину загальної стратегії кібербезпеки, а не як універсальне

рішення. Наприклад, незважаючи на те, що дані інформаційної системи будуть захищені за допомогою VPN, і стороннім особам буде важче бачити, що відбувається, все одно знадобиться брандмауер для захисту даних на фактичному пристрої.

1.4. Мобільні пристрої та VPN

Все більше віддалених працівників ведуть справи за допомогою своїх телефонів. Від надсилання робочих електронних листів, до доступу та обміну конфіденційними документами та інформацією, компанії повинні переконатися, що їхні співробітники мають безпечний спосіб використовувати свої мобільні пристрої.

Функціональність VPN не сильно відрізняється між комп'ютерами та мобільними пристроями. Співробітник усе одно підключатиметься до сервера VPN зі свого пристрою, покладатиметься на VPN для шифрування даних і налаштування віртуального тунелю та матиме доступ до приватних мереж на іншому кінці з'єднання. У цій ситуації кінцева точка, яка розшифровує дані, працює на телефоні, а не на комп'ютері.

Щоб працівники могли підключатися до VPN зі своїх телефонів, IT-команда повинна розробити спеціальний набір інструкцій для доступу до нього. Хоча низка додатків доступна від приватних компаній, які керують власними VPN-серверами, компанії, зрозуміло, віддають перевагу підключенню співробітників до VPN власної розробки. Для цього працівники можуть отримати доступ до елементів керування VPN на своїх мобільних пристроях і слідувати вказівкам IT-спеціалістів щодо того, як правильно все налаштувати.

Зважаючи на це, є деякі нюанси, які потрібно взяти до уваги для VPN, що працюють з телефону. Наприклад, будь-хто, хто регулярно підключається до Wi-Fi зі свого мобільного пристрою, знає, що іноді з'єднання не стабільне. Якщо телефон перемикається з стільникової мережі передачі даних на мережу Wi-Fi під час підключення до VPN, це захищене з'єднання може бути розірвано, і співробітники будуть наражатися на небезпеку.

1.5. Законність використання VPN

У більшості країн, включаючи Сполучені Штати та Велику Британію, використання VPN є абсолютно законним. Однак це не скрізь так. Наприклад, деякі країни обмежують доступ до VPN з ряду політичних, соціальних і релігійних причин, включаючи Росію, Туреччину та Китай. У більш суворих країнах, таких як Іран і Північна Корея, доступ до VPN заборонено.

Декому відносна анонімність і безпека, які надають VPN, може здатися запрошенням до незаконної діяльності. У цьому випадку будь-яка незаконна діяльність, яка здійснюється через VPN, все ще є незаконною. Торрент-захист матеріалів, захищених авторським правом, таких як фільми та музика, все ще суперечить закону, навіть якщо владі важко сказати, що це робить конкретна особа.

Більше того, державні органи все ще можуть вимагати від постачальників VPN інформацію користувачів, що означає, що ніхто не буде повністю виключений з мережі лише тому, що вони мають доступ до Інтернету через VPN. Хоча деякі служби VPN стверджують, що не реєструють діяльність тих, хто використовує їхні сервери, багато хто це робить, і будь-хто, хто вчиняє незаконні дії за VPN, усе ще несе відповідальність за будь-які завдані збитки.

РОЗДІЛ 2. Технології та програмне забезпечення для захисту інформаційних систем користувачів на базі VPN

VPN - ця технологія може фактично з’єднати цілі філії з центральним офісом, дозволяючи командам у територіально розкиданих організаціях працювати разом, обмінюватися важливою інформацією.

Із збільшенням використання інформаційних систем та цифрових платформ для роботи, важливих транзакцій існує висока потреб захисту даних від кіберзлочинців. І одним із таких способів запобігти захопленню даних інформаційних систем є використання VPN.

VPN-тунель - це зашифроване з'єднання між комп'ютером або мобільним пристроєм і Інтернетом. Так як це з'єднання зашифровано, то трафік, що по ньому проходить не можна перехопити, відстежити або змінити.

2.1. Захист за допомогою VPN

Введення у браузер URL-адреси ініціює запит на веб-сервер. Сервер отримує запит, а потім надсилає назад дані для цього веб-сайту, який, у свою чергу, завантажує їх у веб-браузер користувача.

Це відбувається за лічені мілісекунди, тому кінцевий користувач цього не помічає. Коли надсилається цей запит, постачальник послуг Інтернету (ISP) реєструє URL-адресу, до якої намагаються отримати доступ та IP-адресу.

У випадку, якщо користувач виконує заборонені дії провайдер має це зафіксувати. Інтернет-провайдер може записувати всі дані веб-перегляду, це є серйозною проблемою щодо конфіденційності [1][2].

Існує два рівні захисту, які VPN використовує для захисту від такого роду стеження.

— Тунелювання;

— Шифрування.

2.1.1. Тунелювання

Тунелювання — це віртуальний тунель, через який дані переміщуються, щоб Інтернет-провайдер чи інші користувачі не бачили їх. Усі дані, що надсилаються на кінцеву машину та з неї, надсилаються в пакетах даних. Пакети містять запит, який надсилається, протокол і IP-адресу відправника.

VPN розміщує пакет даних всередині іншого пакета даних. Процес відомий як інкапсуляція, і це перший рівень безпеки, який використовує VPN, щоб зберегти анонімність користувача.

Проста і широко вживана метафора для інкапсуляції полягає в тому, щоб сприймати її як пошту. Нехай пакет даних буде листом. Щоб приховати вміст листа від листоноші, потрібно використовувати конверт. У цьому випадку конверт — це другий пакет, який VPN використовує для захисту першого.

VPN використовує сервер віддаленого доступу, до якого підключаєтеся користувач під час використання VPN. Комп'ютер користувача надає необхідні облікові дані для входу на цей сервер та має відповідне клієнтське програмне забезпечення, яке використовується для встановлення цього тунельного з'єднання. Коли це буде зроблено, усі дії браузера виглядатимуть так, ніби вони надходять із віддаленого сервера, а не з комп'ютера користувача.

Тунелювання — це перший рівень безпеки та основна функція VPN. Однак існують додаткові заходи захисту.

2.1.2. Шифрування

VPN шифрують пакети даних, які надсилаються на віддалений сервер, щоб додати додаткову форму безпеки та анонімності. Дані шифруються локально, надсилаються на віддалений сервер через тунель, а потім розшифровуються.

Найкращі провайдери VPN, використовують 256-бітне шифрування AES. Це галузевий стандартний метод шифрування, який практично неможливо зламати. 256-бітний ключ може створити 1,1 x 1077 можливих комбінацій.

Лише дані, які надсилаються на сервер, зашифровані, оскільки він має відповідний декодер, щоб зробити дані доступними. Коли дані надсилаються з

віддаленого сервера на веб-сайт, до якого користувач або інформаційна система намагаєтеся отримати доступ, вони не будуть зашифровані, оскільки веб-сайт-одержувач не має ключа для розшифровки цих даних. До цього моменту IP-адреса та дані користувача повністю приховані.

2.2. Типи VPN

В основному існує два типи категорій VPN:

1. **Remote Access VPN (VPN віддаленого доступу)**: VPN віддаленого доступу надає користувачам можливість підключати свій пристрій до приватної мережі та віддалено отримувати доступ до всіх служб/ресурсів. Ці пристрої називаються кінцевими точками і можуть бути ноутбуками, настільними комп'ютерами або смартфонами. Захищене та приватне з'єднання між користувачем і приватною мережею встановлюється через Інтернет. Працівник компанії у відрядженні може використовувати VPN для підключення до приватної мережі своєї компанії та віддаленого доступу до файлів і ресурсів у приватній мережі.
2. **Site-to-Site VPN**: великі компанії та транснаціональні корпорації з офісами в різних місцях використовують Site-to-Site VPN, оскільки відстань унеможливлює пряме мережеве з'єднання між офісами. Таким чином, вони з'єднують мережу одного офісу з мережею іншого офісу.
    - **Intranet-based VPN:** VPN на основі інтрамережі: коли кілька офісів однієї компанії підключено за допомогою VPN типу "сайт-сайт", щоб ви могли обмінюватися інформацією та ресурсами між собою, це називається VPN на основі інтрамережі.
    - **Extranet-based VPN**: VPN на основі Extranet: коли компанії підключаються до офісу головної компанії, але без можливості прямого доступу однієї до іншої, це називається VPN на основі Extranet.

2.3. Протоколи VPN

Віртуальна приватна мережа захищає та анонімізує підключення до Інтернету, підключаючи користувача до віддаленого сервера перед запуском веб-сайтів. З’єднання з цим сервером також зашифроване, тобто жоден із веб-запитів не може побачити зовнішній світ.

Тип і рівень шифрування визначається протоколом безпеки. Залежно від протоколу, який використовуєте підприємство, корсиувач підключатиметеся до VPN через різні порти та з різними рівнями безпеки.

Хоча тип шифрування є основною відмінністю між протоколами, він також впливає на інші аспекти використання VPN. Наприклад, складніший рівень шифрування краще захистить з’єднання, але він не буде таким швидким, як протокол, який використовує менш надійне шифрування.

На практичному рівні вибір протоколу зводиться до того, як потрібно збалансувати безпеку та швидкість. Протоколи VPN є формою мережевого протоколу, тобто вони об’єднують вимоги для встановлення з’єднання між двома пристроями. Це включає безпеку та швидкість.

На жаль, це не так просто. Підтримка платформи важлива, а також те, де і коли відбувається шифрування в ланцюгу зв’язку. Через ці відмінності найкращі постачальники VPN включають кілька варіантів протоколу.

Також актуальним питання є захист мережі та віддаленого доступу до неї, що є актуальним для захисту інформаційних систем.

Віддалений доступ дозволяє користувачам отримувати доступ до корпоративних систем якщо немає можливості працювати в ній безпосередньо. Користувачі можуть отримати доступом до віддаленої системам через системи телекомунікації або Інтернет-з'єднання.

Віддалений доступ дозволяє найняти фахівців в своїй області, незалежно від їх місця розташування, щоб створювати робочі команди не прив’язуючись до офісу.

Відомо, що VPN передає дані за допомогою тунелювання. Перед передачею пакету вони інкапсулюються (загортаються) у новий пакет із новим заголовком.

Цей заголовок надає інформацію про маршрутизацію, щоб вона могла пройти загальнодоступну мережу, перш ніж досягти своєї кінцевої точки тунелю. Цей логічний шлях, по якому проходять інкапсульовані пакети, називається тунелем. Коли кожен пакет досягає кінцевої точки тунелю, він "деінкапсулюється" і пересилається до кінцевого пункту призначення.

Весь трафік проходить через VPN-тунель, що забезпечує йому повний захист від сторонніх очей. Це убезпечує всі онлайн-дії, листування і будь-який інший трафік як від інтернет-провайдерів, уряду або хакерів, які можуть відстежувати дії підключившись до публічних точок доступу Wi-Fi.

VPN-тунель не тільки захищає дані від перехоплення, але і приховує IP-адресу, за допомогою якого можна ідентифікувати робітника під час роботи в Інтернеті[3].

Наведемо типи протоколів VPN-тунелювання:

— Lightway;

— OpenVPN;

— WireGuard;

— IKEv2;

— L2TP/IPsec;

— PPTP;

— SSTP.

2.3.1. Lightway

Lightway — це новий протокол із відкритим кодом, розроблений спеціально для збільшення швидкості та надійності VPN-з’єднання. З офіційним запуском ExpressVPN зробив його доступним на всіх платформах, включаючи Android, iOS, Windows, Mac, Linux.

Замість того, щоб будувати Lightway на основі існуючого протоколу, ExpressVPN створив його з нуля за допомогою бібліотеки шифрування wolfSSL. Це дозволило ExpressVPN створити неймовірно легкий протокол. Протокол містить близько 2000 рядків коду, що менше, ніж будь-який інший протокол на ринку.

Полегшений код означає, що він потребує менше процесорної потужності, що, у свою чергу, означає кращу продуктивність. OpenVPN має, як відомо, велику кодову базу, через що початкове підключення сповільнюється. Lightway завантажується майже миттєво, і легко побачити, як менший код підвищує продуктивність.

Lightway — це останнє доповнення до масиву протоколів VPN ExpressVPN. Незважаючи на те, що новий власний протокол все ще знаходиться на початковій стадії, він покращив продуктивність ExpressVPN, перевершивши старіші протоколи, такі як OpenVPN. Протокол вийшов зі стадії бета-тестування і тепер доступний для всіх користувачів ExpressVPN.

Lightway працює зі стандартами шифрування AES і ChaCha20 і підтримує тунелювання через TCP і UDP. Незалежно від того, надається пріоритет швидкості чи безпеці, можна обрати відповідну комбінацію шифрування відповідно до потреб. Крім того, його природа з відкритим вихідним кодом означає, що будь-хто може перевірити код на наявність будь-чого підозрілого.

2.3.2. OpenVPN

OpenVPN є популярним протоколом для використання, оскільки він є відкритим і безкоштовним. Деякі провайдери, наприклад AirVPN та e-VPN, побудували свої послуги навколо цього. Їй майже 20 років, і навколо них є спільнота, яка постійно сканує вихідні файли на наявність вразливостей у безпеці, що робить його одним із найбезпечніших доступних варіантів.

Він може використовувати два транспортних протоколи: TCP або UDP. Протокол керування передачею є найпоширенішим. Комп’ютер корисувача надсилає пакет, потім очікує підтвердження, перш ніж надсилати інший, створюючи надійніше з’єднання. Це сприяє надійності, але не швидкості. Оскільки кожен пакет має чекати підтвердження, використання TCP додає додаткові витрати на мережеве з’єднання. Ось тут і з’являється протокол дейтаграм користувача. Він продовжує надсилати пакети без підтвердження, створюючи швидше, хоча й менш надійне з’єднання.

Що стосується шифрування, OpenVPN є першокласним. Він використовує бібліотеку OpenSSL, тобто має доступ до всіх шифрів. Він також використовує спеціальний протокол безпеки на основі SSL/TLS, який забезпечує до 256-бітного шифрування.

Однак 256-бітне шифрування не потрібне. Використання меншого розміру ключа зазвичай забезпечує швидше з'єднання, але це відбувається за рахунок безпеки. Тим не менш, навіть найшвидші провайдери VPN використовують 256-бітний ключ, що показує, чому OpenVPN такий популярний. Крім багатьох інших причин, чому провайдер пропонує це, OpenVPN має найкращий баланс безпеки та швидкості.

Через свою природу з відкритим вихідним кодом він також відображається в спеціальних протоколах деяких постачальників VPN. Протокол Chameleon від VyprVPN шифрує пакети OpenVPN, а StealthVPN від Astrill робить здебільшого те саме. VyprVPN і Astrill розробили свої протоколи для обходу цензури в Китаї. OpenVPN, хоч і дуже безпечний, не робить нічого особливого, щоб приховати від глибокої перевірки пакетів. VyprVPN увійшов до списку найкращих послуг VPN для Китаю, оскільки його протокол Chameleon може шифрувати пакети OpenVPN, що надсилаються.

Ще одна перевага OpenVPN полягає в тому, що його можна адаптувати майже до будь-якої платформи. ExpressVPN, наприклад, дозволяє використовувати OpenVPN на вашому маршрутизаторі, як ви можете побачити в нашому огляді ExpressVPN. Він використовує спеціальну мікропрограму, яка включає попередньо налаштовану версію OpenVPN, що дозволяє захищати трафік.

2.3.3. WireGuard

WireGuard новий інструмент. На відміну від більшості інших протоколів, код WireGuard неймовірно компактний. Це забезпечує швидше з'єднання з набагато меншими проблемами. Проте є певні сумніви щодо конфіденційності WireGuard. Це безкоштовний протокол тунелювання з відкритим кодом, заснований на ChaCha20 замість AES-256, як OpenVPN. Різниця між двома шифрами мінімальна,

коли мова йде про безпеку. Стандарт TLS 1.3 навіть використовує ChaCha20 як резервний шифр, а також спосіб шифрування з'єднань на пристроях без апаратного прискорення AES.

WireGuard здатний досягати таких високих швидкостей із належним шифруванням завдяки коду та процесу підключення. Процес подібний до встановлення з'єднання SSH - сервер потребує статичної IP-адреси та повинен зберігати локальну IP-адресу для автентифікації.

Очевидно, це проблема для конфіденційності. Однак численні служби VPN розробили системи для вирішення проблеми конфіденційності. NordVPN вирішує проблему за допомогою подвійного NAT, який може призначати кожному користувачеві динамічну IP-адресу, тоді як Mullvad постійно скидає IP-адреси, що зберігаються в пам'яті сервера.

Окрім переваг у швидкості, спрощена кодова база WireGuard також забезпечує переваги безпеки. Для довідки, OpenVPN містить приблизно півмільйона рядків коду, а WireGuard – менше 10 000. Набагато менше шансів, що рядок коду стане вразливим місцем безпеки.

Дослідникам безпеки також набагато простіше перевіряти код, і це можливо, оскільки він є відкритим кодом. WireGuard —ймовірно, майбутнє VPN, хоча зараз його підтримують лише кілька служб.

2.3.4. Layer2 Tunnel Protocol

Layer2 Tunnel Protocol (L2TP) — це протокол тунелювання, який дозволяє переміщувати дані з однієї мережі в іншу. На відміну від OpenVPN, L2TP є суто протоколом тунелювання. Він сам по собі не забезпечує шифрування. Через це L2TP часто поєднується з протоколом шифрування для забезпечення безпеки.

Він був створений у 1999 році і базується на двох старих протоколах тунелювання під назвою L2F і PPTP. Нову версію протоколу, відому як L2TPv3, було представлено в 2005 році для додавання функцій безпеки, L2TP здебільшого залишився незмінним.

L2TP використовує два типи пакетів: контрольні пакети та пакети даних. Пакети керування встановлюють з'єднання та відкривають тунель між користувачем та сервером, до якого є доступ. Оскільки це основна функція протоколу тунелювання, L2TP має функції надійності, такі як підтвердження пакетів, пов'язані з контрольними пакетами.

Пакети даних не мають таких функцій. L2TP надсилає пакети в дейтаграмі UDP, тобто вони не перевіряються під час надсилання. Це забезпечує швидше, але менш надійне з'єднання.

Проблема самого L2TP полягає в тому, що пакети, які надсилаються, не зашифровані. Вони інкапсульовані, але немає криптографічного алгоритму для приховування даних. Через це, швидше за все, L2TP буде у парі з IPSec у клієнті VPN, що використовується.

IPSec забезпечує шифрування, інкапсулюючи вже інкапсульований пакет, коли він проходить через тунель L2TP. Це означає, що IP-адреси джерела та призначення зашифровані в пакеті IPSec, створюючи безпечне VPN-з'єднання.

Що стосується шифрування, IPSec пропонує кілька варіантів, включаючи HMAC з відповідним алгоритмом хешування, TripleDES-CBC, AES-CBC і AES-GCM. Деякі постачальники VPN, як-от TorGuard, дозволяють змінювати використовуваний шифр, але здебільшого це буде L2TP/IPSec, захищений 128-бітним або 256-бітним AES.

L2TP/IPSec вважається безпечним, але деякі експерти з безпеки сумніваються, оскільки IPSec був розроблений, зокрема, Агентством національної безпеки США. Незважаючи на це, зазвичай це гірший вибір, ніж OpenVPN. Порт, який використовує L2TP, легко блокується брандмауерам, тому буде важко обійти перевірку, якщо використовується VPN, який підтримує переадресацію портів.

2.3.5. Secure Socket Tunneling Protocol

Secure Socket Tunneling Protocol (SSTP)— це власна технологія Microsoft, розроблена для Windows Vista. Хоча це протокол, розроблений Microsoft, SSTP

також можна використовувати в Linux. Тим не менш, він не підтримується в macOS і, ймовірно, ніколи не підтримуватиметься.

Як і OpenVPN, SSTP дозволяє трафіку «точка-точка» проходити через канал SSL/TLS . Через це вона має однакові плюси та мінуси використання такої системи. Наприклад, він використовує SSL/TLS через TCP-порт 443, що робить його чудовим для проходження через більшість брандмауерів, оскільки трафік здається нормальним.

Проблема його використання така сама як і з використанням TCP на OpenVPN, і полягає в тому, що він вразливий до збою TCP. TCP має дочекатися підтвердження, перш ніж відправити пакет назад. Він має вбудовані функції для виявлення та спроби вирішення проблем, якщо пакет не було підтверджено.

У такому випадку TCP-пакет на одному рівні може спробувати вирішити проблему, викликаючи надмірну компенсацію пакета на рівні вище. Коли це трапляється, продуктивність TCP-з'єднання значно падає. Цього можна уникнути за допомогою OpenVPN, використовуючи натомість UDP. З SSTP проблема неминуча.

Хоча SSTP доступний у деяких програмах VPN, він рідко використовується. Він краще обходить брандмауери, ніж L2TP, але OpenVPN також це робить на достатньому рівні. Проблема SSTP полягає в тому, що він не так налаштовується, як OpenVPN, тому він більш сприйнятливий до проблем, таких як збій TCP. OpenVPN забезпечує всі переваги SSTP без недоліків.

2.3.6. Internet Key Exchange Version 2

Internet Key Exchange (IKE) — це протокол, розроблений Microsoft і Cisco у 1998 році. Технічно це не протокол VPN. IKE використовується для встановлення асоціації безпеки в наборі протоколів IPSec. Асоціація безпеки включає такі атрибути, як шифр і ключ шифрування трафіку.

Незважаючи на це, його часто розглядають як протокол VPN, який називається IKEv2, який є просто другою версією IKE або IKEv2/IPSec. На відміну

від L2TP/IPSec, який використовує IPSec лише для шифрування, IKE використовує IPSec для передачі даних.

Що стосується безпеки, якість захисту так, як L2TP або SSTP, якщо є довіра Microsoft. Він може підтримувати кілька версій AES, і він буде працювати в в парі зі 128-бітним або 256-бітним ключем у своєму VPN.

Однак це не просто інший варіант. IKEv2 зазвичай є найшвидшим протоколом, який пропонують VPN.

IKE використовує пакети UDP і починає створювати асоціацію безпеки після надсилання перших кількох пакетів. Потім асоціація безпеки передається в стек IPSec, який змушує його починати перехоплювати відповідні IP-пакети та шифрувати або дешифрувати їх відповідно.

Через це IKE добре підключається після розриву з'єднання. Під час дротового або Wi-Fi з'єднання. Однак для мобільних пристроїв IKE набагато краще адаптований.

Мережі 3G і 4G LTE постійно змінюються разом з версіями телефонів або планшетім. Корисувач можете перейти з 4G LTE на 3G або тимчасово втратити з'єднання. Оскільки IKE швидко підключається, це найкращий вибір для мобільних пристроїв. IKEv2 навіть вбудовано в пристрої BlackBerry.

2.3.7. Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP, протокол тунелювання «точка-точка» — це застарілий і незахищений протокол тунелювання, який не слід використовувати, якщо в найвищому пріоритеті безпека. Незважаючи на це, деякі провайдери VPN все ще включають його у свої програми. Для більшості користувачів його слід просто ігнорувати.

Найкращим варіантом використання PPTP є зовнішній доступ до внутрішньої мережі корпоративної будівлі, тому в першу чергу були розроблені VPN. PPTP не визначає шифрування. Скоріше він покладається на протокол «точка-точка» для реалізації функцій безпеки.

Через нижчу форму шифрування PPTP є швидким. Це майже така сама швидкість, як звичайне підключення до Інтернету. У випадку особистого використання це також безпечно, як і звичайне підключення до Інтернету. PPTP рекомендовано використовувати, лише якщо користувач робите щось, що не можете зробити без VPN, наприклад, отримує доступ до зовнішньої мережі.

Однак не слід очікувати, що це з'єднання буде безпечним. Існує багато інструментів для злому тунелів PPTP, деякі з яких можуть просто отримати ключ із методу автентифікації, а інші можуть знайти ключ протягом кількох годин за допомогою атаки.

Крім того, відомо, що АНБ активно шпигує за мережами PPTP через слабку безпеку. Якщо немає конкретної причини використовувати його, бажано уникати PPTP, навіть якщо він доступний у вашій програмі VPN.

Для більшості користувачів OpenVPN є найкращим варіантом, оскільки він забезпечує безпеку найвищого рівня та можливість конфігурації з коробки. Крім того, його природа з відкритим вихідним кодом дозволяє завантажувати файли конфігурації та додатково налаштовувати їх на свій смак [4].

Інші варіанти мають свої сильні сторони, але вони також мають і слабкі. SSTP вирішує проблему брандмауера, але може стати жертвою збою TCP. L2TP швидкий і стабільний, але його легко заблокувати. Єдиним винятком буде IKEv2, який, хоч і поступається OpenVPN, але має багато переваг для мобільних користувачів.

2.4. Переваги та недоліки використання VPN для захисту інформаційних систем

Основна мета VPN — надати користувачам приватну мережу в межах публічної. Простими словами, це дозволяє користувачам створювати віртуальну мережу в іншій мережі. У таблиці 2.1 наведено переваги та недоліку використання VPN для захисту інформації віддалених користувачів.

Таблиця 2.1.

Переваги та недоліки використання VPN

Переваги	Недоліки
• **Анонімність** : великою перевагою VPN є те, що вони забезпечують конфіденційність, якої користувач ніколи не мав під час серфінгу в Інтернеті. Навіть інтернет-провайдер не може бачити онлайн-активність користувача, коли він підключений до VPN. • **Геопереміщення** : підключившись до сервера іншої країни, користувач можете обійти державну цензуру та обмеження веб-сайтів (Netflix Canada замість Netflix US). • **Розділене тунелювання** : якщо користувачу потрібен доступ до приватної мережі під час використання загальнодоступної Wi-Fi, мережі VPN із розділеним тунелюванням дозволять вам зробити те й інше одночасно одним натисканням кнопки.	• **Нижча швидкість веб -** перегляду. Незалежно від VPN усі VPN певною мірою сповільнюють швидкість доступу до Інтернету користувача, оскільки дані мають проходити через зашифрований тунель, а не підключатися безпосередньо до маршрутизатора. • **Заблоковані сервери** : хоча деякі мережі VPN дозволяють доступ до Netflix, Netflix стає розумнішим і блокує багато серверів VPN, тому це ніколи не є гарантією. • **Вартість** : незважаючи на те, що мережі VPN не дорогі, і ціни починаються лише від декількох доларів на місяць з деякими довгостроковими планами, вони є додатковими витратами, і залежно від того, для чого вони потрібні або як довго вони потрібні, вони можуть не бути варто того. Як альтернативу VPN можна використовувати проксі-

	сервера, оскільки вони зазвичай безкоштовні.

Отже, VPN вважається безпечним, якщо він відповідає таким критеріям:

Шифрування: шифрування гарантує, що жодна третя сторона не зможе прочитати дані під час передавання. Тому будь-яка спроба злому буде невдалою.

Автентифікація: автентифікація гарантує, що користувач є тим, за кого себе видає. Іншими словами, він перевіряє, чи належить особа, яка отримує доступ до веб-сайту, до групи авторизованих користувачів.

Цілісність даних: цілісність даних гарантує, що отримані в кінці дані точно збігаються з даними, надісланими відправником.

Конфіденційність: конфіденційність гарантує, що ніхто інший не може отримати доступ до даних, крім передбачуваного одержувача.

Роль VPN у кібербезпеці дуже важлива. Основні ситуації, які можуть виникати для захисту віддалених користувачів.

- **Захист особистості.** Якщо користувач має бізнес-акаунт на веб-сайтах соціальних мереж, таких як Facebook, Twitter, Instagram тощо, йому потрібно захистити свою особистість. Якщо хтось зламав обліковий запис, він може змінити зображення вашого профілю, опублікувати неприйнятні повідомлення, видалити публікації тощо. Сервіс VPN, захищає цю інформацію. Для захисту слід створити надійний пароль і ввімкнути двофакторну автентифікацію. Потрібно переконатися, що ніхто не має доступу до облікових даних користувача для входу. Крім того, потрібно відстежувати всі дії, які виконуються через обліковий запис уористувача.
- **Захист онлайн-транзакцій.** Можливо, користувач має намір купити щось онлайн за допомогою власної кредитної картки. Якщо є сумніви щодо безпеку своєї транзакції, слід розглянути можливість використання служби VPN. Коли користувач підключаєтеся до VPN-сервера, він діє як проксі-сервер. Отже, коли при перегляді веб-

сторінки, трафік проходить через сервер VPN, а не безпосередньо на веб-сайт. Тому з'єднання стає зашифрованим. В результаті ваша особиста інформація залишається в безпеці.

- **Запобігання DDoS-атакам.** DDoS-атаки проводяться, щоб порушити нормальну роботу веб-сайту. Зловмисник надсилає величезну кількість запитів на цільовий веб-сайт. Ці запити споживають пропускну здатність, VPN сповільнює цей процес, отже ресурси цілі, а інформація залишається в безпеці.

З огляду на ці фактори, слід дотримуватися відповідних правил при виборі VPN. Вони дозволять уникнути зайвих проблем і спростять захист інформаційних систем.

РОЗДІЛ 3. Технологія застосовування VPN

Великі корпорації зазвичай керують власними службами VPN. Але малим і середнім підприємствам не вистачає IT-ресурсів для налаштування та підтримки безпечної та приватної VPN.

Є низка компаній які пропонують послуги VPN для захисту інформаційних систем малого та середнього бізнесу. Звичайний користувач VPN може працювати з таким ресурсом теж, але компаніям часто потрібен безпечний доступ до сервера, на якому вони можуть розміщувати документи, програми та інші офісні ресурси для віддаленого доступу персоналу.

3.1. VPN та захист інформаційних систем

VPN — найкращий спосіб захистити дані під час передачі. Скорочено від Virtual Private Network, VPN шифрує та захищає весь інтернет-трафік, що протікає між ноутбуком або смартфоном і сервером VPN. Через це допитливим хакерам дуже важко проникнути в конфіденційні дані. З огляду на те, що середня вартість витоку бізнес-даних у Microsoft склала близько 4-х мільйонів доларів, а п’ята частина малих підприємств постраждала від злому, вірусу чи витоку даних, безпека є великою проблемою.

Наведемо основних постачальників VPN та технології, що використовуються з для захисту інформаційних систем віддалених користувачів.

Найкращі VPN для бізнесу:

1. **Perimeter 81** вибір VPN №1 для бізнесу. Сервери здатні встановлювати швидкі та стабільні з’єднання, які можуть обробляти всі види мережевого трафіку, включаючи SSH, RDP, VNC і Telnet. Дозволяє налаштувати між сайтові VPN.
2. **NordLayer Specialist Business** VPN, популярний серед малих і середніх організацій.
3. **Twingate Business** VPN, обслуговує віддалені команди з підтримкою SSO, розділеним тунелюванням, доступом із нульовою довірою та приватними шлюзами.

4. **GoodAccess Scalable business** VPN, цей інноваційний постачальник послуг пропонує безкоштовний рівень і плани, які переходять аж до нульового довіреного доступу до мережі за допомогою середовища єдиного входу.
5. **Windscribe Business** VPN із найвищими функціями безпеки, простими у використанні та опцією централізованого виставлення рахунків. Має гарну документація, але не має цілодобової підтримки. Є бюджетним варіантом.
6. **CyberGhost** - послуга з безпечними додатками, які легко встановити та почати використовувати.
7. **IPVanish** – має швидкі сервери з безпечними та надійними з'єднаннями. Зручні додатки. Має цілодобову підтримку.
8. **ExpressVPN** - має розгалужену мережу швидких серверів, іисокоякісне шифрування і навіть чудово працює в Китаї та ОАЕ. Не найдешевший варіант у цьому переліку.

3.2. Постачальники VPN та особливості технологій, що застосовуються

Оцінити VPN для бізнесу можна за такими факторами:

- Пропонує послуги, призначені спеціально для підприємств
- Швидкість і стабільність
- Висока безпека
- Кількість одночасних підключень
- Програми для Android, iOS, Windows, MacOS, Linux, Chrome.

Розглянемо особливості і переваги деяких з них.

3.2.1. Perimeter 81

Perimeter 81 — це спеціалізована бізнес-VPN. Дозволяє компаніям розгортати приватні сервери VPN, до яких персонал може безпечно підключатися з будь-якої точки світу. Дозволяє легко керувати мережевою діяльністю всього персоналу, не маючи диплому IT, за допомогою онлайн-панелі. Це дозволяє співробітникам безпечно отримувати доступ до файлів, програм та інших ресурсів із віддалених місць. Має наступні ключові риси:

- Призначений для розподіленого бізнесу
- Включає аплікаційні огорожі
- Може реалізувати SASE
- Захист хмарних облікових записів
- Контролює права доступу.

Perimeter 81 обслуговує підприємства завдяки унікальним функціям безпеки, таким як сегментація мережі, щоб ізолювати конфіденційні дані від зламів. Якщо підприємство має офіси в різних місцях, можна налаштувати VPN між сайтами для з'єднання двох мереж. Хмарні VPN забезпечують віддалений доступ і можуть бути легко збільшені за потреби.

Усі дані зашифровано за допомогою 256-бітного AES. Якщо підприємство не розгортаєте власну VPN, можна обирати з 700 публічних серверів у 36 місцях по всьому світу. Компанії можуть контролювати доступ до VPN, реєструючи та перевіряючи весь трафік, який проходить через нього.

Таблиця 3.1.

Переваги та недоліки використання VPN Perimeter 81

Переваги	Недоліки
• Спеціально для підприємств • Дозволяє розгорнути власний сервер або обрати із публічних • Підтримує міжсайтові VPN • Підтримує розміщення програм та файли на сервері VPN • Надійне шифрування • Підтримує сегментацію мережі	• Не найдешевший варіант

«Advanced Cloud VPN» — це спеціальна функція, що має ця VPN та створена спеціально для використання в бізнесі. Має велику мережу швидких серверів, які можна надзвичайно динамічно налаштувати. Підходить для більшості бізнес-цілей

і дозволяє 5 одночасних підключень. Включає 30-денну гарантію повернення грошей.

3.2.2 NordLayer

NordLayer — це бізнес-сервіс NordVPN для малого та середнього бізнесу. Дозволяє легко налаштувати безпечний віддалений доступ як до офісної мережі, так і до Інтернету. Кожним обліковим записом користувача можна керувати з єдиної централізованої панелі керування. Дозволяє тунелювати з'єднання з робочих пристроїв через 33 різні країни. Додавати користувачів легко й не ускладнюватиме виставлення рахунків.

Має наступні ключові риси:

- Шифрування AES-256
- Опція виділеного IP
- Віддалений доступ і сайт-сайт
- Сканування безпеки пристрою

Стороння автентифікація працює з GSuite, OneLogin, Okta та Azure. Програми доступні для Windows, MacOS, iOS, Android і Linux. Надійне шифрування забезпечують постійний захист даних організації. Підтримка користувачів від моменту звернення не перевищує трьох годин.

Таблиця 3.2.

Переваги та недоліки використання VPN NordLayer

Переваги	Недоліки
• Швидкі та надійні з'єднання • 256-бітове шифрування військового класу для надійної конфіденційності • Сувора політика заборони реєстрації	• До настільного додатка може знадобитися деякий час, щоб звикнути

• Необмежена пропускна здатність і відсутність обмежень щодо даних • Програми для Windows, MacOS, iOS, Linux і Android	

Справжній конкурент у всіх категоріях, має потужні функції безпеки, високу швидкість і просте виставлення рахунків для компаній.

3.2.3 Twingate

Twingate — це новий бізнес-VPN з деякими цікавими функціями, які відрізняють його від інших. Twingate — це хмарна служба, яка відрізняється від традиційних рішень VPN завдяки контролю доступу з нульовою довірою та робить шлюзи невидимими для Інтернету. Twingate можна розгортати без зміни мережевої інфраструктури та легко масштабувати.

Має наступні ключові риси:

- Контроль доступу до програм;
- Єдиний вхід;
- Групи доступу на основі ролей.

Twingate підтримує єдиний вхід (SSO), щоб персонал міг отримати доступ лише до тих ресурсів, які їм надають IT-адміністратори. Це включає в себе хмарні та локальні програми та віддалені мережі. Розділене тунелювання дозволяє трафіку проходити через мережу лише за необхідності, тоді як дії, що потребують більше пропускної здатності, як-от відеодзвінки, здійснюються через пряме з’єднання.

Таблиця 3.3.

Переваги та недоліки використання VPN Twingate

Переваги	Недоліки
• Контроль доступу з нульовою довірою	• Формально, це не VPN

• Підтримує більшість основних постачальників єдиного входу (SSO). • Легко розгортається • Розділене тунелювання	

Twingate — надійне рішення для віддалених команд, які використовують систему єдиного входу.

3.2.4 GoodAccess

GoodAccess пропонує програми для Windows, macOS і Linux, а також захист мобільних пристроїв для iOS, Android і Chrome OS. Цей провайдер пропонує просте рішення VPN для бізнесу, яке включає безкоштовний доступ до 35 шлюзів. Вищі тарифні плани надають складніші послуги захисту бізнес-мережі, такі як посилання «сайт-сайт» і «нульовий доступ довіри».

Має наступні ключові риси:

- Хмарний брандмауер;
- Нульовий довірчий доступ до програми;
- Середовище єдиного входу.

Спрощує доступ користувачів до певних програм, представивши кожному користувачеві середовище із механізмами єдиного входу. Дозволяє покращити безпеку доступу, вимагаючи багатофакторну автентифікації, обрати захист окремих пристроїв, у тому числі пристроїв роумінгу, або цілих сайтів. Роздільне тунелювання також пропонується як стратегічний варіант.

Таблиця 3.4.

Переваги та недоліки використання VPN GoodAccess

Переваги	Недоліки
• Безкоштовний план • 35 локацій шлюзів	• Кількість шлюзів не така велика, як у інших провайдерів

• Доступ без довіри та єдиний вхід із коштовними тарифними планами • Варіанти захисту між сайтами	

GoodAccess пропонує передові рішення для доступу без довіри, а також стандартну послугу VPN, стартовий план безкоштовний.

Доступ без довіри це означає повну відсутність довіри кому-небудь – навіть користувачам всередині периметра. Модель передбачає, що кожен користувач або пристрій повинні підтверджувати свої дані кожного разу, коли вони запитують доступ до якогось ресурсу всередині або за межами мережі.

3.2.5 CyberGhost

У CyberGhost немає спеціальної опції VPN для бізнесу. Але як виявляється, це найкращий VPN для бізнесу завдяки доступності та кількості одночасних підключень у платних облікових записах.

Має наступні ключові риси:

- Шифрування AES-256;
- Опція виділеного IP;
- Додатковий антивірусний пакет.

Цей провайдер додає нові сервери з шаленою швидкістю. Наразі існує понад 9000 серверів у 91 країні, і очикується, що в середньостроковій перспективі цей показник може ще зростати. Додаткова перевага для компаній полягає в тому, що внутрішня політика не зберігає журнали даних, тому вміст комунікацій має залишатися прихованим навіть від системних адміністраторів компанії. Існують програми як для Android, так і для iOS, а також підтримують настільні комп’ютери для Windows, MacOS і Linux. Один обліковий запис дозволяє одночасно встановити сім підключень.

Ця служба VPN за замовчуванням використовує 256-бітове шифрування AES на протоколі OpenVPN разом із 2048-бітними ключами RSA та автентифікацією MD5

HMAC. Існує також перемикач блокування Інтернету, який означає, що веб-трафік буде припинено, якщо з’єднання несподівано впаде.

До одного облікового запису можна одночасно підключити сім пристроїв.

Таблиця 3.5.

Переваги та недоліки використання VPN CyberGhost

Переваги	Недоліки
• Має найшвидші сервери • Не зберігайте журнали даних • Додатки прості в установці та використанні	• Немає специфічних для бізнесу послуг • Не підходить для тих, кому потрібен контроль розширених функцій

Найкращий вибір для початківці. CyberGhost простий у використанні . Відмінна конфіденційність із нульовим журналюванням і захистом від витоків DNS. Розблоковує популярні потокові платформи та обмежені служби. Має 45-денну гарантія повернення грошей.

3.2.6 IPVanish

IPVanish продовжує дотримуватись політики нульового журналювання. Він поєднує це з жорсткими протоколами шифрування та зосередженістю на високій швидкості для забезпечення надійності в цілому.

Має наступні ключові риси:

- Необмежена кількість одночасних підключень;
- Дуже високі швидкості;
- Захист Wi-Fi.

На даний момент існує понад 2000 серверів по всьому світу з гідним вибором на кожному континенті. Стандарти шифрування також вражають. IPVanish за замовчуванням використовує 256-бітне шифрування за протоколом OpenVPN, аутентифікацію SHA512 і 2048-бітний обмін ключами DHE-RSA з ідеальною конфіденційністю. Перемикач блокування Інтернету доступний у всіх клієнтах.

Є програми як для iOS, так і для Android, а також настільні програми для Windows і MacOS. Немає обмежень щодо кількості пристроїв, які можна підключити до сервісу одночасно за допомогою одного облікового запису.

Таблиця 3.6.

Переваги та недоліки використання VPN IPVanish

Переваги	Недоліки
• Вражаюча швидкість і надійне підключення • Повну базу знань можна знайти на веб-сайті компанії • Вбудований захист від витоків DNS і IPv6	• Немає специфічних для бізнесу послуг • Не підходить для використання програми в Китаї • Не пропонує жодних розширень для браузера

Швидкий і надійний IPVanish має велику мережу серверів. Неперевантажена мережа забезпечує хорошу швидкість. Сильні функції безпеки та конфіденційності. Має гарну підтримку клієнтів. 30-денна гарантія повернення грошей.

3.2.7 ExpressVPN

ExpressVPN має тисячі серверів у 94 країнах, що означає, що це гарний вибір для співробітників, яким, можливо, доведеться часто подорожувати або працювати віддалено. Найбільший вибір у Європі, Північній Америці та Азіатсько-Тихоокеанському регіоні з меншою кількістю в Африці та на Близькому Сході.
Має наступні ключові риси:

- Надійне шифрування;
- Менеджер паролів;
- Приватний DNS.

Служба VPN є фаворитом користувачів, оскільки вона пропонує високу швидкість у поєднанні з шифруванням військового рівня. Користувачі, які піклуються про конфіденційність, знають, що ExpressVPN не зберігає жодних журналів трафіку. Єдина крихітна частина збереження метаданих стосується дати

(не часу) підключення, вибору розташування сервера та загальної використаної пропускної здатності.

Перевага і те, що штаб-квартира ExpressVPN знаходиться на Британських Віргінських островах, тому вона не зобов'язана дотримуватися жодних обов'язкових законів про збереження даних. Це означає, що це також поза юрисдикцією західних урядових установ.

Стандарти шифрування суворі. Постачальник використовує 256-бітний AES-CBC як протокол шифрування за замовчуванням, а також як автентифікацію HMAC, так і ідеальну пряму секретність. У комплект входить перемикач блокування Інтернету, який компанія називає «блокуванням мережі». Одночасне підключення в одному тарифному плані дозволено максимум п'ятьом пристроям.

Програми доступні як для iOS, так і для Android, а також програмне забезпечення для ПК для Windows, MacOS і Linux.

Таблиця 3.7.

Переваги та недоліки використання VPN ExpressVPN

Переваги	Недоліки
• Висока швидкість для завантаження та потокового відео • Надійна конфіденційність і безпека • Чудові можливості для розблокування геозаблокованого контенту	• Немає специфічних для бізнесу послуг • Трохи дорожче, ніж деякі інші варіанти • Досвідчені користувачі можуть знайти обмежені додаткові параметри

Універсальний ExpressVPN швидкий і надійний вибір, який впевнено розблокує більшість обмежених сайтів. Чудові функції конфіденційності та відсутність журналів. Одна з небагатьох VPN, яка працює в Китаї та ОАЕ. 30-денна гарантія повернення грошей.

3.3 Пошук найкращих VPN для бізнесу: методологія

На ринку надають послуги багато VPN, але багато з них просто не підходять для малого та середнього бізнесу.

Методологія пошуку найкращих VPN для конкретного бізнесу передбачає пошук, що забезпечують наступне:

Орієнтація на бізнес: більшість VPN на ринку обслуговують окремих осіб, а не компанії. Потрібно шукати ті, що пропонують послуги спеціально для конкретного за розмірами бізнесу.

Швидкість: час – це гроші, тому швидкість VPN стає ще важливішою. Тестуючи кожну корпоративну VPN, потрібно визначити її рівень продуктивності. Слід звертати увагу на найшвидші VPN та мають необмежену пропускну здатність. Це забезпечує швидшу передачу файлів і підключення до віддалених серверів компанії.

Розблокування: на жаль, в Інтернеті існує багато географічних обмежень. Це включає в себе популярні веб-сайти новин і онлайн-банкінгові послуги. Якщо потрібен доступ співробітників до такого типу інформації, потрібен VPN із сильною можливістю розблокування та для обходу цих обмежень.

Безпека: віруси та витоки даних – це лише деякі із загроз безпеці, з якими щодня стикається бізнес. Кожна VPN, повинна мати як мінімум високоякісне шифрування та захист від витоку. Однак багато найкращих VPN для бізнесу пропонують набагато більше, ніж така вимога.

Конфіденційність: VPN, яку використовується підприємстовм, має діяти без реєстрації. Це буде означати, що він не зберігає ідентифікаційні журнали користувачів, захищаючи конфіденційність не лише вашої компанії, а й усього персоналу, який ним користується. Однак не кожному VPN можна довіряти.

Простота використання: від першого налаштування VPN до додавання або видалення користувачів, процес повинен бути простим. Найкращі VPN для бізнесу пропонують програми, зручні для початківців, і цілодобову підтримку через чат і електронну пошту. Крім того, не бракує посібників із налаштування та усунення помилок у налаштуваннях.

Співвідношення ціни та якості: хороша новина полягає в тому, що найкращі VPN для бізнесу пропонують різноманітні варіанти для будь-якого бюджету. Компанія може спробувати майже будь-яку VPN без ризику, оскільки кожна із них включає гарантію повернення грошей.

3.4 Загальна технологія вибору VPN

Вибір VPN залежить від потреб. Найкращі VPN повинні захищати інтернет-з'єднання за допомогою шифрування, з'єднувати користувача з серверами VPN із найкращими протоколами та бути зручні у користуванні.

Розташування серверів: відстань від сервера може вплинути на швидкість VPN, тому необхідно переглянути список розташувань серверів VPN, щоб переконатися, що можна працювати з максимально можливою швидкістю.

Швидкість: до тестів на швидкість, слід ставитися з недовірою, тому що швидкість залежить від багатьох факторів, крім самої VPN. Наприклад від моделі комп'ютера чи телефону, року його випуску, операційної системи. Для перевірки VPN зазвичай використовують VPN з безкоштовними пробними періодами, підписками чи гарантією повернення грошей.

Тести DNS/WebRTC: В інтернеті є прості інструменти, щоб перевірити сервер доменних імен або DNS, тобто веб-сайти, на які заходить користувач, а також IP-адреси, коли браузер за замовчуванням використовує WebRTC.

Шифрування: Метою захисту користувача є те, щоб увесь веб-трафік і приватні IP-адреси були зашифровані, щоб навіть якщо хтось зламав VPN, він фактично не міг побачити дані користувача. Зазвичай вибирають VPN із шифруванням OpenVPN або AES-256.

Політика конфіденційності: Необхідно уважно ознайомлюватися з угодою про політику конфіденційності, оскільки необхідно знати яку інформацію про користувача зберігає відповідна VPN.

Головний офіс: Слід звертати увагу де розташована компанія. Якщо штаб-квартира компанії розташована в країні, яка є членом Five Eyes, Nine Eyes або 14 Eyes, це може означати, що вони можуть бути змушені передавати дані клієнтів

уряду. Такі країни, як Сполучені Штати та Велика Британія, є членами, тому слід віддавати перевагу VPN, розташованим у країнах, що не є членами, наприклад Панама чи Румунія. Це особливо важливо, якщо конфіденційність є основним питанням.

Сумісність пристроїв: слід переконатися, що VPN працюватиме на тих пристроях, на яких повинен чи хоче використовувати працівник; зазвичай це не є проблемою для таких пристроїв, як iOS, MacOS, Android або Windows, але якщо у вас є пристрій від менш популярного виробника, необхідно перевірити сумісність.

Kill switch: якщо VPN, що використовується не працює (наприклад, збій), слід звернути увагу на наявність перемикача, який автоматично вимикає всі веб-браузери в разі такої ситуації. Такий перемикач називають функціями блокування мережі.

Завантаження торрентів: якщо необхідно завантажувати торрент-файли, переконайтеся, що ваш VPN це дозволяє, оскільки не всі це роблять.

IP-адреси: слід віддавати перевагу мережам VPN із динамічними IP-адресами, тобто вони надають нову IP-адресу кожного разу, коли відбувається підключення, а іноді навіть частіше. Це краще, ніж статична IP-адреса, яка щоразу залишається незмінною, її набагато легше відстежити. Однак, якщо IP-адреса статична, це нормально, при умові, що вона використовується кількома користувачами.

Інтернет-протоколи: Інтернет-протоколи точно визначають, як VPN передає наші дані з нашого пристрою в приватну мережу. Індивідуальні досвід стосуються певним чином на вибір, але зазвичай віддають перевагу таким протоколам, як TCP або UDP, обидва зазвичай використовуються з VPN.

Підписки: Вартість завжди важливі для будь-якої служби VPN. Хоча є деякі мережі VPN, які пропонують безкоштовні послуги, зазвичай вони обмежені або обсягом даних, які можна використати під час використання VPN, або кількістю днів, які надаються для безкоштовного підключення. Швидше за все, вам доведеться скористатися тарифним планом VPN за гроші, тому важливо не переплачувати.

Тривалість дії тарифного плану: щоб отримати максимальну економію, необхідно оформити тарифний план на найдовший термін. Однак, якщо є невпевненість щодо VPN або вона потрібно лише ненадовго, слід оформити щомісячний тарифний план, це буде коштувати дорожче, але якщо виникнуть або виявляться проблеми з функціонуванням VPN, її можна буде змінити, без додаткових витрат.

Одночасне підключення: Якщо VPN планується для користуванням певної кількості людей, слід переконатися, що підписка дозволяє достатню кількість одночасних з'єднань. Деякі VPN дозволяють необмежену кількість підключень одночасно, хоча це може значно сповільнити підключення до Інтернету.

Перемикання серверів: деякі мережі VPN мають обмеження на кількість серверів, до яких можна підключитися, тому, якщо віддалений користувач мандрує, слід переконатися, що обраний сервер передбачає достатню кількість перемикань серверів.

Загальна кількість пристроїв: те саме стосується загальної кількості пристроїв, які можна підключити до VPN, незалежно від того, одночасно чи ні. Багато підписок на VPN застосовуються лише до обмеженої кількості пристроїв, тому про це також слід пам'ятати.

Знижки: Деякі VPN пропонують знижки, незалежно від того, чи є вони сезонними чи для студентів, тож іноді це дозволить заощадити.

Безкоштовні VPN: деякі VPN є безкоштовні або мають безкоштовний тарифний план. Зазвичай вони обмежені обсягом переданих даних або періодом часу, протягом якого їх можна використовувати.

Підтримка клієнтів: підтримка клієнтів у більшості VPN не розвинута. Деякі VPN пропонують різні способи зв'язку зі службою підтримки клієнтів (наприклад, електронна пошта, чатом або телефоном, онлайн-довідковий центр).

Додаток: слід переглянути рейтинги додатків VPN у магазині Apple або Google Play, деякі додатки VPN працюють надто погано або зовсім не працюють.

3.5. Технології вибору VPN для підприємств

По-перше, слід використовувати VPN, призначений спеціально для використання в бізнесі. Це забезпечить необхідну функціональність і безпеку, а також відповідність нормативним стандартам.

Компанії повинні враховувати кілька факторів, зважуючи різні варіанти VPN:

Хмара чи саморозміщення: Більшість VPN, працюють у хмарі. Це значно полегшує їх налаштування, керування та масштабування. Можна розміщувати файли та програми на хмарному сервері VPN, до якого співробітники можуть отримати віддалений доступ за допомогою програм VPN. Крім того, можна розмістити власний сервер VPN у хмарі або на місці, але для цього знадобляться додаткові IT-ресурси та досвід.

Зручна панель налаштувань. Добре розроблена інформаційна панель для керування обліковими записами VPN і привілеями доступу значною мірою допоможе підтримати зв’язок і захист співробітників.

Site-to-site: працівники не єдині, хто може використовувати VPN. Можна створити безпечний тунель між двома мережами за допомогою VPN. Це називається VPN типу Site-to-site («сайт-сайт»), і він корисний, наприклад, для підприємств із кількома офісами.

Масштабованість: якщо планується активно наймати працівників, необхідно переконайтеся, що VPN може виконувати такі функції: додавання та видалення доступу до облікових записів та сервера VPN. Такі дії мають бути простим.

Безпека: Надійне шифрування, запобігання витокам, автентифікацію та політику відсутності журналів від постачальника VPN це те нащо треба звертати увагу при виборі VPN для великих підприємств. Слідкуйте потрібно за наявністю таких функцій, як двофакторна автентифікація, ідеальна конфіденційність і сучасні протоколи VPN з відкритим кодом.

Сегментація: Розділивши мережу підприємства на менші частини, є можливість краще захистити важливі дані. На такі питання слід звертати увагу також системному адміністратору.

Підтримка: Обов'язково вибір VPN повинен бути із компетентною та оперативною підтримкою клієнтів. Деяка підтримка обмежена робочими годинами країни, у якій розташовано VPN.

3.6 Бізнес-альтернативи VPN

Для корпоративних середовищ VPN можуть бути не найкращим рішенням. Для з'єднань «сайт-сайт» між географічно віддаленими офісами та центрами обробки даних існує кілька більш сучасних альтернатив:

- **Multiprotocol Label Switching (MPLS)**, направляє дані за допомогою міток замість публічних IP-адрес. Він робить можливим вибір пріоритету у трафіку, є менш вразливим до незахищених IP-пошуків і, як правило, страждають від меншої затримки, ніж «сайт-сайт» VPN.
- **Zero Trust Network Access** (ZTNA). Рішення Zero Trust Network Access працюють на прикладному рівні та, на відміну від VPN, не залежать від мережі. Натомість користувачі підключаються безпосередньо до програм на основі перевірки користувача та положення пристрою. Програми приховані від Інтернету, що зменшує площу атаки. Це схема, яку використовує Twingate.
- **Хмарний VPN**. Налаштувавши за допомогою SD-WAN, хмарні VPN можуть бути швидшими, безпечнішими та вимагати менше обслуговування, ніж традиційні VPN. Хмарні VPN-сервіси SD-WAN найкраще реалізовувати за допомогою SASE або периферії служби безпечного доступу, яка дає організації єдине централізоване уявлення про всю мережу.
- **Орендовані канали зв'язку**, також відомі як орендовані лінії, є постійними та приватними з'єднаннями між двома або більше місцями. Орендовані канали дорогі і застосовні лише для дуже великих підприємств.

3.7. Мережі VPN, яких слід уникати

Коли обирається бізнес-VPN, є надія, що постачальник зробить усе можливе, щоб захистити дані та захистити компанію від зовнішніх загроз. Провайдери VPN несуть моральну відповідальність за виконання своєї сторони угоди. Але не всі

компанії цінують цей принцип. Наведемо перелік провайдерів VPN від послуг яких слід утриматися.

1. **HolaVPN.** Ізраїльська компанія Hola, яка керує безкоштовним одноранговим розширенням VPN для Chrome, колись мала базу користувачів майже в 50 мільйонів. На жаль, частина індивідуальної пропускної здатності користувачів Hola використовувалася для участі в таких речах, як DDoS-атаки, просування піратського вмісту та розповсюдження порнографії. І це без будь-якої згоди користувача.

2. **Betternet.** Було виявлено, що він містить зловмисне програмне забезпечення, порушує власну політику конфіденційності та перенаправляє користувачів на веб-сторінки, де має прибуток. Він записував інформацію про користувачів, щоб показувати їм рекламу від третіх осіб.

Крім того, швидкість низька, а сервери ненадійні. Betternet може дуже мало запропонувати споживачам і ще менше для бізнесу.

3.8. Рекомендації щодо вибору VPN

1. Вибір VPN на основі стандартів

VPN, які використовують загальноприйняті стандарти, такі як IKE/IPSec, як правило, менш ризиковані та безпечніші, ніж SSL/TLS VPN, які використовують спеціальний код для надсилання трафіку через TLS. Якщо VPN розроблено для використання спеціального тунелю SSL/TLS як резервного варіанту слід вимкнути цю функцію.

2. Використання VPN із надійною криптографією

Слід переконатися, що алгоритми шифрування, алгоритми автентифікації та протоколи, які використовує VPN, є надійними та перевіреними FIP. Налаштування всіх VPN повинно бути на використання багатофакторної автентифікації (MFA). Також слід замінити автентифікацію на основі пароля на автентифікацію клієнта за

допомогою цифрових сертифікатів (зберігаються на смарт-картках), якщо це можливо.

3. Керування вразливими місцями програмного забезпечення

Використання вразливостей VPN є поширеним вектором атак для кіберзлочинців. Слід обирати постачальника VPN із значним досвідом роботи та ті які ведуть перелік виправлень вразливостей.

Після розгортання VPN регулярно слід перевіряти наявність і негайно застосовувати оновлення програмного забезпечення. Слід дотримуватися вказівок постачальника щодо оновлення, наприклад, примусової зміни пароля для користувачів під час виправлення вразливості, яка, як відомо, активно використовується зловмисниками.

4. Обмеження доступ до VPN

VPN є звичайною мішенню для кіберзлочинців, які використовують скомпрометовані облікові дані для доступу до внутрішніх систем організації. Необхідно створити правила брандмауера, щоб дозволити роботу лише UDP-порту 500 і 4500 для IKE/IPsec VPN або TCP-порт 433 (або спеціальний порт) для SSL/TLS VPN.

Також доцільно обмежити доступ до кінцевої точки VPN на основі білого списку IP-адрес. Слід заблокувати доступ до інтерфейсів керування через VPN, щоб запобігти його використанню зі зламаними обліковими даними адміністратора, доступу до інтерфейсів керування та виконання привілейованих дій. Це має бути частиною нульової довіри до безпеки та політики сегментації мережі, яка обмежує доступ до та з VPN на основі принципу найменших привілеїв.

5. Захист трафіку VPN

VPN призначений для забезпечення зашифрованого каналу між двома місцями. Він не перевіряє безпеку та не фільтрує трафік, що проходить через цей тунель.

Весь трафік VPN повинен проходити через повний стек безпеки на шляху до корпоративної мережі та з неї, включаючи брандмауер веб-додатків (WAF) і систему запобігання вторгненням (IPS). Крім того, VPN має бути налаштовано з увімкненими всіма параметрами безпеки веб-додатків, такі як повторні атаки з використанням даних сеансу попередніх користувачів.

Нижче наведено кілька моментів, які потрібно враховувати при виборі VPN:

- Доцільно переконатися, що VPN має надійний механізм шифрування, щоб приховати IP-адресу від провайдера та інших третіх осіб.
- Перевірка покриття сервера .Слід перевірити, що провайдер VPN має покриття сервера VPN у більшості країн світу.
- Протоколи мають вирішальне значення для безпеки VPN. Слід обирати VPN, який забезпечує OpenVPN або WireGuard для кращого шифрування.
- Слід зупиняти вибір на VPN, який пропонує додатковий рівень захисту через спільні IP-адреси.
- Слід обирати VPN, яка має підтримку достатньої кількості пристроїв в одній підписці.
- Слід переконатися, що VPN має функцію «Kill Switch», яка вимикає Інтернет і завершує роботу програм, якщо служба VPN зупиняє роботу.
- Завжди слід перевіряти політику конфіденційності, перш ніж обрати VPN.
- Слід спочатку отримати безкоштовну пробну версію VPN, щоб дізнатися, чи вона все те, що потрібно підприємству та віддаленому співробітнику, а потім придбати VPN за повну вартість на тривалий термін.

3.9. Обмеження VPN

Хоча VPN можуть бути надзвичайно корисними для захисту даних в Інтернеті, вони мають свої обмеження, залежно від конкретного фірми розробника, а також від вибраного рівня підписки. Деякі речі, на які варто звернути увагу:

- **Порушення безпеки:** коли компанія зберігає дані клієнтів в Інтернеті, можливі порушення безпеки, навіть із зашифрованим хмарним сховищем і обмеженою політикою реєстрації.
- **Надійність:** не всі VPN є надійними, тому деякі з них можуть мати нестабільне обслуговування. Інколи виникають технічні труднощі під час спроби підключитися до наших найближчих серверів, але наступні спроби зазвичай дозволяють встановити з'єднання.
- **Доступність:** не кожен VPN працюватиме у користувача в кожній країні. Це залежить від розташування серверів VPN, тому слід переконатися, що зона користування ваших співробітників охоплена, перш ніж вибрати одну VPN замість іншої.
- **Використання даних:** деякі VPN обмежують використання даних залежно від вибраної підписки. TunnelBear, наприклад, має ліміт 500 МБ на безкоштовну підписку, але більшість платних підписок на VPN дозволяють використовувати необмежену кількість даних. Отже, слід на перед дізнатися, як мережі VPN використовують дані .
- **Перемикання серверів:** так само деякі підписки дозволяють лише обмежену кількість перемикань серверів, хоча більшість із них необмежені.
- **Загальна кількість пристроїв:** зазвичай підписки на VPN відрізняються залежно від загальної кількості пристроїв, які можна підключити до VPN.
- **Кількість одночасних з'єднань:** коли необхідно, щоб кілька пристроїв були підключені до VPN одночасно, слід переконатися, що тарифний план обраної VPN дозволяє це. Деякі мережі VPN дозволяють підключати необмежену кількість пристроїв одночасно, деякі дозволяють лише один, п'ять або 10.

Хоча VPN є чудовим інструментом, який допомагає відокремити місцезнаходження співробітника від його даних, він не приховує всього про вас. Якщо ви пишете коментар у Facebook або ставите лайк до публікації в Instagram, програма, якою ви користуєтеся під час підключення до мережі VPN, усе ще зможе використовувати поведінку користувача для адаптації оголошень і вмісту в

програмі. Вони можуть не знати, звідки він переглядає, але все одно знатиме, що він робить в їхніх програмах.

Подібним чином, якщо на вашому комп'ютері ввімкнено файли cookie, компанії можуть стежити за вами, поки корисувач перебуваєте на їхньому сайті — і після теж. Повні данні про користувача не є прихованими лише за допомогою VPN. Поєднання захисту VPN із Tor, інструментом з відкритим вихідним кодом, який дозволяє анонімно переглядати веб-сторінки, та інші заходи безпеки необхідні для повнішої безпеки.

VPN не є ідеальним інструментом. Як і будь-яка комп'ютерна програма, вона чутлива до зловмисного програмного забезпечення та онлайн-атак. У разі зараження переваги безпеки VPN зводяться нанівець.

Вірогідність атак і порушень безпеки підвищується завдяки використанню безкоштовного сервісу VPN. Щоб компенсувати свої бізнес-витрати, «безкоштовні» служби VPN можуть продавати дані користувачів або показувати рекламу, яка може бути заражена шкідливим програмним забезпеченням.

ВИСНОВКИ

VPN, або віртуальна приватна мережа, використовує загальнодоступну мережу для підключення різних сайтів і користувачів. VPN використовує «віртуальні» з'єднання в Інтернеті від приватної мережі підприємства до співробітника або віддаленого сайту.

Завдяки цьому сторонні особи, які намагаються перехоплює зашифровані дані, не зможуть їх інтерпретувати. У будь-якому випадку, це метод підвищення конфіденційності та безпеки як для приватних, так і для загальнодоступних мереж, таких як точки доступу WI-FI. За результатами дослідження зрозуміло, що VPN частіше використовуються компаніями, ніж фізичними особами для захисту даних.

Безліч веб-сайтів мають обмеження щодо того, які користувачі, що належать до певних країн або регіонів, можуть отримати до них доступ. Інший цього процесу — «геоблокування». Користувачі часто швидко залишають спроби отримати доступ до такого ресурсу, коли справа доходить до регіонального блокування.

За допомогою VPN можна досить легко отримати доступ до таких сайтів, оскільки VPN дозволяє обійти такі обмеження.

Віддалені співробітники, які працюють не з офісних приміщень, або які подорожують чи знаходяться у відрядженні, використовуючи VPN можуть полегшувати та мати захищений доступ до корпоративних інформаційних систем, тим самим не наражати на безпеку корпоративні дані. Таким чином, компанія може мати більш захищений робочий процес, незалежно від місця розташування співробітників.

Різні веб-сайти мають різний інтерфейс і відображають результати залежно від місцезнаходження користувача, що його відвідує. Таким чином, за допомогою VPN можна маніпулювати своєю адресою та вибирати потрібну інформацію з сайту. Прикладом цього можуть бути торгові сайти, які відстежують місцезнаходження та показують вміст лише для цього регіону.

Для публічних мереж, які не є захищеними, VPN може виконувати роботу щодо збереження конфіденційності інформації. Будь-який IT-фахівець може

виявити користувача та отримати особисті дані. Якщо співробітники використовують VPN, вони з меншою ймовірністю будуть передавати важливу інформацію іншим. Для більшості підприємств це є головним пріоритетом, оскільки ніхто не хоче, щоб їхні дані викрали.

Сьогодні онлайн-злочинність є досить поширеним явищем. Окрім встановлення відповідного програмного забезпечення, належного приховування паролів і виходу з облікових записів після сеансу, ще обирають, як додатковий ступінь захисту, VPN.

Якщо підприємство або організація мають загальнодоступним Wi-Fi, тоді VPN може захистити і клієнтів. Підприємства, що турбуються про безпеку клієнтів, налаштовують службу VPN для захисту свого маршрутизатора, а потім шифрують онлайн-активність клієнтів. Це можете надати можливість завоювати довіру серед своїх клієнтів, продемонструвавши, що безпека є пріоритетом.

Переваги VPN застосовуються не лише для особистого використання, а й для бізнес-корпорацій. Це забезпечує додатковий рівень безпеки, не дозволяючи іншим стежити за підприємством чи організацію. Отримання доступ до веб-сайтів, які блокують певні регіони, дозволить знайти кращі фінансові пропозиції або більш корисну чи актуальну інформацію.

VPN захищає від кіберзлочинності та можливого злому чи шпигунства, а також не лише співробітники можуть отримати вигоду, а й клієнти.

ПЕРЕЛІК ПОСИЛАНЬ

1. 7 common VPN security risks: the not-so-good, the bad, and the ugly– [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://www.imprivata.com/blog/vpn-problems/ – Загл. с экрана (переглянуто 20 листопада 2022).
2. How does VPN work?– [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://www.namecheap.com/vpn/how-does-vpn-virtual-private-network-work/ – Загл. с экрана (переглянуто 15 грудня 2022).
3. 10 Ways to Increase VPN Security– [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://blog.devolutions.net/2021/02/10-ways-to-increase-vpn-security/ – Загл. с экрана (переглянуто 16 грудня 2022).
4. VPN Protocols: Are You Using the Right One?– [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://www.g2.com/articles/vpn-protocols – Загл. с экрана (переглянуто 16 грудня 2022).
5. VPN security: How VPNs help secure data and control access– [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://www.cloudflare.com/learning/access-management/vpn-security/ – Загл. с экрана (переглянуто 26 грудня 2022).
6. Understanding VPN Protocols: A Guide To The Best Protocols – [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://www.trustradius.com/buyer-blog/vpn-protocols – Загл. с экрана (переглянуто 26 грудня 2022).
7. How a VPN Helps with Network Security - [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://openvpn.net/blog/vpns-and-network-security/ – Загл. с экрана (переглянуто 5 січня 2023).
8. 10 Best VPN Services (January 2023) – [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL https://www.forbes.com/advisor/business/software/best-vpn/ – Загл. с экрана (переглянуто 10 січня 2023).

9. Mobile Device Management Software – [Електронний ресурс] / MDM – Режим доступа: World Wide Web. – URL: https://financesonline.com/mobile-device-management/ – Загл. с экрана (переглянуто 10 січня 2023).
10. 119 Impressive Cybersecurity Statistics: 2020/2021 Data & Market Analysis – [Електронний ресурс] / Finances Online – Режим доступа: World Wide Web. – URL: https://financesonline.com/cybersecurity-statistics/ – Загл. с экрана (переглянуто 10 січня 2023).
11. 10 Cybersecurity Trends for 2021/2022: Latest Predictions You Should Know – [Електронний ресурс] / Finances Online – Режим доступа: World Wide Web. – URL: https://financesonline.com/cybersecurity-trends/– Загл. с экрана (переглянуто 10 січня 2023).
12. 73 Important Cybercrime Statistics: 2020/2021 Data Analysis & Projections – [Електронний ресурс] / Finances Online – Режим доступа: World Wide Web. – URL: https://financesonline.com/cybercrime-statistics/– Загл. с экрана (переглянуто 10 січня 2023).
13. 20 Best IT Security Software Solutions of 2021 – [Електронний ресурс] / Finances Online – Режим доступа: World Wide Web. – URL: https://financesonline.com/top-20-it-security-software-solutions/ – Загл. с экрана (переглянуто 10 січня 2023).
14. 2021 Threat Predictions Report. – [Електронний ресурс] / McAfee, LLC– Режим доступа: World Wide Web. – URL:https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report/ – Загл. с экрана (переглянуто 13 січня 2023).
15. 2020 Global Cost of Insider Threats Ponemon Report – [Електронний ресурс] / Observeit– Режим доступа: World Wide Web. – URL: https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf – Загл. с экрана (переглянуто 13 січня 2023).

16. Mobile devices blur work and personal privacy raising cyber risks.– [Електронний ресурс] / Scimex– Режим доступа: World Wide Web. – URL: https://www.scimex.org/newsfeed/mobile-devices-blur-work-and-personal-privacy-raising-cyber-risks,-says-qut-researcher– Загл. с экрана (переглянуто 13 січня 2023).
17. Network Security: Top 5 Fundamentals. – [Електронний ресурс] / Itmanagerdaily – Режим доступа: World Wide Web. – URL: http://www.itmanagerdaily.com/network-security-fundamentals/ – Загл. с экрана (переглянуто 13 січня 2023).
18. The Complete Guide to Internet Security / M. S. Merkow, J. Breithaupt. – AMACOM, 2018. – pp. 34-52

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)