ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

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

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Олександр МАТВЄЄВ
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
МАТВЄЄВ Олександр
(прізвище, ім'я)

Керівник д.ф., МАРЧЕНКО Віталій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

РЕФЕРАТ

Текстова частина магістерської роботи: 49 сторінок, 21 рисунків, 14 джерел

Об'єкт дослідження — процес забезпечення безпечної віддаленної роботи працівників організації.

Предмет дослідження — методи та засоби забезпечення безпечної роботи віддалених кормстувачів на базі Cisco Secure VPN.

Мета роботи — розробити рекомендації щодо використання технології задля забезпечення безпечної дистанційної роботи на базі рішення Cisco Secure VPN.

Методи дослідження — опрацювання літератури за темою, теорія інформації, стандарти в сфері кібербезпеки, технології компанії Cisco.

В роботі приведено основні відомості про загрози конфіденційним даним. Проаналізовано різні види загроз, детально розглянуто вплив Cisco Secure VPN для боротьби з ними. Розглянуто переваги та недоліки, що можуть виникати під час роботи.

Зазначено, що для побудови доступу до Cisco Secure VPN потрібно мати налаштоване мережеве обладнання, та надано опис корпоративного доступу до VPN. Виокремлено, що Cisco Secure VPN Cisco Secure VPN є кращим за будь-який звичайний VPN з тунельним протоколом доступу, завдяки своїй здатності захищати передачу даних через телефонну мережу загального користування та використання попередньо наданих ключів

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування технології Cisco Secure VPN, для забезпечення конфіденційності даних на компанії та працівників.

Галузь використання – кібербезпека

КІБЕРБЕЗПЕКА, КІБЕРІНЦИДЕНТ, ЗАГРОЗИ, VPN, CISCO SECURE, РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ЗА ДОПОМОГОЮ CISCO SECURE VPN.

ABSTRACT

Master's thesis: 49 pages, 21 drawings, 14 sources

Object of research - the process of ensuring safe remote work of the organization's employees.

The subject of research is methods and means of ensuring the safe operation of remote users based on Cisco Secure VPN.

Purpose - to develop recommendations for the use of technology to ensure secure remote work based on the Cisco Secure VPN solution.

Research methods - studying the literature on the topic, information the standards in the field of cybersecurity, Cisco technologies.

The article provides basic information about threats to confidential data. Different types of threats are analyzed, and the impact of Cisco Secure VPN to combat them is considered in detail. The advantages and disadvantages that may arise during operation are considered.

It is noted that in order to build access to Cisco Secure VPN, it is necessary to have configured network equipment, and a description of corporate access to VPN is provided. It is emphasized that Cisco Secure VPN Cisco Secure VPN is better than any conventional VPN with a tunnel access protocol, due to its ability to protect data transmission over the public switched telephone network and the use of pre-provided keys

Based on the research conducted in this paper, recommendations for the use of Cisco Secure VPN technology to ensure the confidentiality of company and employee data have been developed.

Scope of application - cybersecurity

CYBERSECURITY, CYBER INCIDENT, THREATS, VPN, CISCO SECURE, CYBER INCIDENT INVESTIGATION, METHODS AND MEANS OF PROTECTION USING CISCO SECURE VPN.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN - Virtual Private Network

VPNaaS - VPN as a Service

IT - Information Technology

DoS - Denial of Service

DDoS - Distributed Denial of Service

SMS - Short Message Service

DNS - Domain Name System

IoT - Internet of Things

SSL - Secure Sockets Layer

TLS - Transport Layer Security

IP - Internet Protocol

AES - Advanced Encryption Standard

IDPS - Intrusion Detection and Prevention System

Wi-Fi - Wireless Fidelity

ВСТУП

Актуальність дослідження. У великих та середніх компаніях все частіше використовують різні додатки для досягнення своїх цілей: різноманітні хмарні сервіси, служби онлайн банкінгу тощо, в той час як працівники цих компаній не завжди захищені, адже зараз майже всі працівники працюють віддалено. Цей факт є причиною для хвилювання, адже не завжди працівники використовують VPN чи інші додатки для контролю мережевого трафіку, чим і наражають на небезпеку як себе, так і компанії у яких вони працюють.

Підприємствам як ніколи важливо дбати про безпеку в Інтернеті. Оскільки більше людей, ніж будь-коли, працюють з дому, конфіденційна інформація компанії та клієнтів піддається великому ризику крадіжки.

Якщо працівник віддалено підключається до робочого комп'ютера в загальнодоступній мережі без використання VPN. Теоретично, будь-хто з цієї публічної мережі може отримати доступ до внутрішньої мережі компанії, оскільки працівник не зробив нічого, щоб приховати свою інформацію.

Необмежений доступ до файлів компанії та інформації про клієнтів може мати катастрофічні наслідки для бізнесу. Використання VPN для підключення до бізнес-мереж може допомогти гарантувати, що конфіденційні дані будуть приховані за фіктивною інформацією, що надається через VPN.

Об’єкт дослідження — процес забезпечення безпечної віддаленної роботи працівників організації.

Предмет дослідження — методи та засоби забезпечення безпечної віддаленної роботи працівників на базі рішення Cisco Secure VPN.

Мета роботи — розробити рекомендації щодо використання технології Cisco Secure VPN для забезпечення безпечної віддаленної роботи користувачів.

Наукові завдання:

– дослідити методи та засоби боротьби з атаками за допомогою VPN
– проаналізувати вплив VPN на успішність атак, переваги та недоліки;
– розробити рекомендації щодо забезпечення безпеки даних користувачів під час дистанційної роботи на базі рішення Cisco Secure VPN;

Методи дослідження — опрацювання літератури за темою, теорія інформації, технології компанії Cisco, стандарти в сфері кібербезпеки.

Практичне значення одержаних результатів полягає в розробці ефективної технології захисту інформаційної системи організації віддалених користувачів на базі Cisco Secure VPN. Запропоновані рішення слід використати для забезпечення конфіденційності, цілісності та доступності даних. Результати також можуть знайти застосування в організаціях, що працюють з віддаленими співробітниками або потребують надійного та захищеного доступу до внутрішніх ресурсів. Реалізація таких технологій дозволяє підвищити рівень інформаційної безпеки та мінімізувати ризики кібератак.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки» [1].

1 АНАЛІЗ МОЖЛИВИХ АТАК НА КОРИСТУВАЧІВ З ГЛОБАЛЬНОЇ МЕРЕЖІ ТА ЇХ НАСЛІДКІВ ПРИ ВІДДАЛЕННІЙ РОБОТІ

1.1 Аналіз можливих ризиків під час дистанційної роботи

Дистанційна робота стає все більш популярним варіантом для шукачів роботи в останні роки. Обіцянка гнучкості, відсутність необхідності їздити на роботу та можливість працювати, не виходячи з дому, приваблює багатьох людей від традиційних офісних умов. Однак, хоча віддалена робота, безумовно, має свої переваги, важливо визнати, що вона також може бути шкідливою для людини різними способами. У цій статті ми розглянемо деякі з прихованих небезпек віддаленої роботи, а також пояснимо, чому шукачам роботи слід ретельно зважити на її потенційні недоліки

А) Ізоляція та самотність

Однією з найважливіших проблем віддаленої роботи є відчуття ізоляції та самотності, яке може її супроводжувати. Коли ви працюєте вдома, ви втрачаєте соціальну взаємодію та товариські стосунки, які притаманні офісному середовищу. Люди за своєю природою є соціальними істотами, і тривала ізоляція може призвести до відчуття самотності, тривоги і навіть депресії. Пошукачі роботи повинні усвідомлювати, що віддалена робота може не забезпечити їм соціальної підтримки, необхідної для процвітання.

Б) Розмиті межі між роботою та особистим життям

Дистанційна робота часто розмиває межі між роботою та особистим життям. Без фізичного відокремлення офісу стає складно відключитися від роботи, що призводить до збільшення тривалості робочого дня і вигорання. Пошукачам роботи може бути важко встановити межі та підтримувати здоровий баланс між роботою та особистим життям, коли їхній робочий простір також є їхнім домом.

В) Зменшення можливостей для кар'єрного зростання

Віддалені працівники можуть втратити цінні можливості для кар'єрного зростання порівняно з колегами, які працюють в офісі. Працівники, які працюють в офісі, часто мають більшу видимість, можливість особистого спілкування з колегами та керівниками, а також легший доступ до наставництва. Віддаленим працівникам може бути складніше будувати міцні професійні стосунки, демонструвати свої навички та відданість справі, що потенційно може сповільнити їхній кар'єрний ріст.

Г) Проблеми комунікації

Ефективна комунікація важлива на будь-якому робочому місці. Однак віддалена робота може створювати проблеми з комунікацією, що призводить до непорозумінь і розбіжностей у команді. Пошукачі роботи можуть виявити, що віддалена робота вимагає сильної самомотивації та відмінних навичок письмової комунікації. Відсутність особистої взаємодії може перешкоджати ефективній співпраці та командній роботі, що ускладнює процвітання у віддаленому робочому середовищі.

Д) Технічні проблеми та залежність

Дистанційна робота значною мірою залежить від технологій, і технічні проблеми неминучі. Пошукачі роботи повинні бути готовими до розчарувань і зниження продуктивності, які можуть виникнути через проблеми зі зв'язком, збої в роботі програмного забезпечення або збої в роботі обладнання. Крім того, віддалені працівники можуть стати надмірно залежними від технологій, що призводить до погіршення особистих та міжособистісних навичок, які можуть мати вирішальне значення для багатьох робочих ролей.

Е) Обмежені можливості нетворкінгу

Нетворкінг є життєво важливим аспектом розвитку кар'єри. Дистанційні працівники можуть втратити можливості неформального спілкування, які природно виникають в офісі, наприклад, під час розмов біля кулера з водою або зустрічей після роботи. Пошукачі роботи повинні враховувати, що віддалена робота може вимагати більше зусиль для побудови та підтримки професійних

відносин, що потенційно може сповільнити їхній прогрес у нетворкінгу.

Дистанційна робота має незаперечні переваги, але шукачі роботи повинні усвідомлювати потенційну шкоду, яку вона може завдати людям. Ізоляція, розмиті кордони, обмежені можливості кар'єрного зростання, проблеми з комунікацією, технічні проблеми та обмежені можливості нетворкінгу, пов'язані з віддаленою роботою, можуть негативно вплинути на добробут і кар'єрний ріст людини. Перш ніж перейти на віддалену роботу, люди повинні ретельно зважити ці недоліки та переваги і подумати, чи відповідає вона їхнім особистим і професійним цілям [2].

1.2 Негативні наслідки кібератак

Дослідники кібербезпеки визначили щонайменше 57 різних способів, у які кібератаки можуть мати негативний вплив на окремих осіб, підприємства і навіть країни, починаючи від загрози життю, викликаючи депресію, штрафи регуляторних органів і закінчуючи порушенням повсякденної діяльності.

Дослідники з факультету комп'ютерних наук Оксфордського університету і Кентської школи комп'ютерних наук поставили собі за мету визначити і кодифікувати різні способи, за допомогою яких різні кіберінциденти, свідками яких ми є сьогодні, можуть мати негативні наслідки.

Вони також розглянули, як ці наслідки або шкода можуть поширюватися з плином часу. Сподіваємося, що це допоможе покращити розуміння численних наслідків кібератак для громадськості, уряду та інших академічних дисциплін.

Загалом дослідники визначили п'ять ключових тем, за якими можна класифікувати вплив кібератак:

А) Фізичний/цифровий

Б) Економічний

В) Психологічний

Г) Репутаційний

Д) Соціальний/суспільний

Кожна категорія містить конкретні наслідки, які підкреслюють серйозність впливу кібератак. Наприклад, у категорії «Фізичні/цифрові» йдеться про людські жертви або пошкодження інфраструктури, в той час як в категорії «Економічні» перераховані такі наслідки, як падіння цін на акції, регуляторні штрафи або зменшення прибутку як можливість.

У психологічній категорії перераховані такі наслідки, як депресія, збентеження, сором або розгубленість, тоді як репутаційні наслідки можуть включати втрату ключового персоналу, зіпсовані відносини з клієнтами і пильну увагу з боку засобів масової інформації.

Нарешті, на соціальному/суспільному рівні існує ризик порушення повсякденного життя, наприклад, вплив на ключові послуги, негативне сприйняття технологій або падіння внутрішнього морального духу в організаціях, що постраждали від інциденту високого рівня [3].

1.3 Різновиди кібератак

1) Шкідливе програмне забезпечення

Шкідливе програмне забезпечення - це будь-яка програма або код, створений з наміром завдати шкоди комп'ютеру, мережі або серверу. Шкідливе програмне забезпечення є найпоширенішим типом кібератак, головним чином тому, що цей термін охоплює багато підмножин, таких як програми-вимагачі, трояни, шпигунські програми, віруси, черв'яки, кейлоггери, боти, криптоджекинг і будь-який інший тип атаки, що використовує програмне забезпечення у зловмисний спосіб.

2) Атаки на відмову в обслуговуванні (DoS)

Атака на відмову в обслуговуванні (DoS-атака) - це зловмисна цілеспрямована атака, яка засипає мережу фальшивими запитами з метою порушення бізнес-операцій.

Під час DoS-атаки користувачі не можуть виконувати рутинні та необхідні завдання, такі як доступ до електронної пошти, веб-сайтів, онлайн-акаунтів або інших ресурсів, які працюють на скомпрометованому комп'ютері або в мережі. Хоча більшість DoS-атак не призводять до втрати даних і зазвичай вирішуються без сплати викупу, вони коштують організації часу, грошей та інших ресурсів, необхідних для відновлення критично важливих бізнес-операцій.

Різниця між DoS і розподіленими атаками на відмову в обслуговуванні (DDoS) пов'язана з походженням атаки. DoS-атаки починаються з однієї системи, тоді як DDoS-атаки запускаються з декількох систем. DDoS-атаки швидше і важче блокувати, ніж DOS-атаки, оскільки для зупинки атаки необхідно ідентифікувати і нейтралізувати декілька систем.

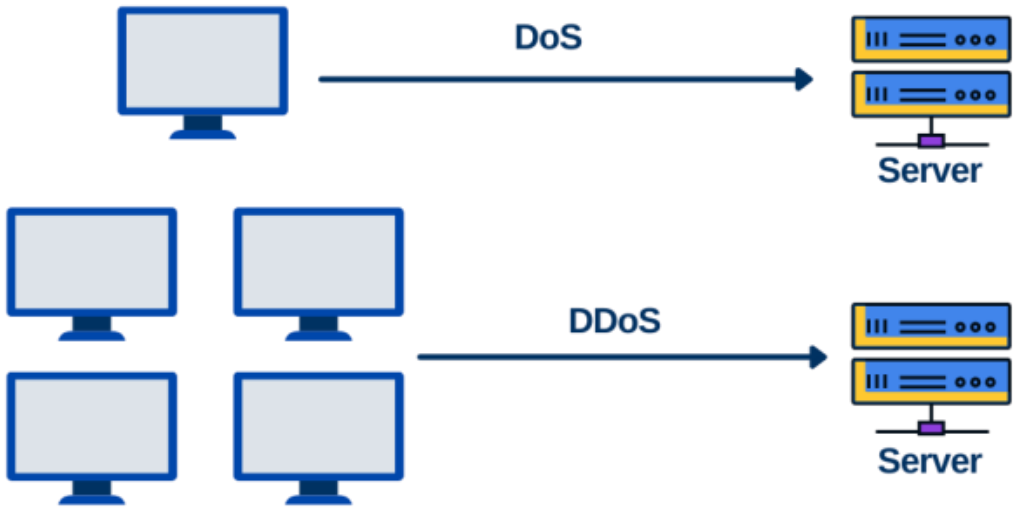

Рис.1.1. DoS та DDoS атака

3) Фішинг

Фішинг - це тип кібератаки, який використовує електронну пошту, SMS, телефон, соціальні мережі та методи соціальної інженерії, щоб змусити жертву поділитися конфіденційною інформацією - наприклад, паролями або номерами рахунків - або завантажити шкідливий файл, який інсталює віруси на їхній комп'ютер або телефон.

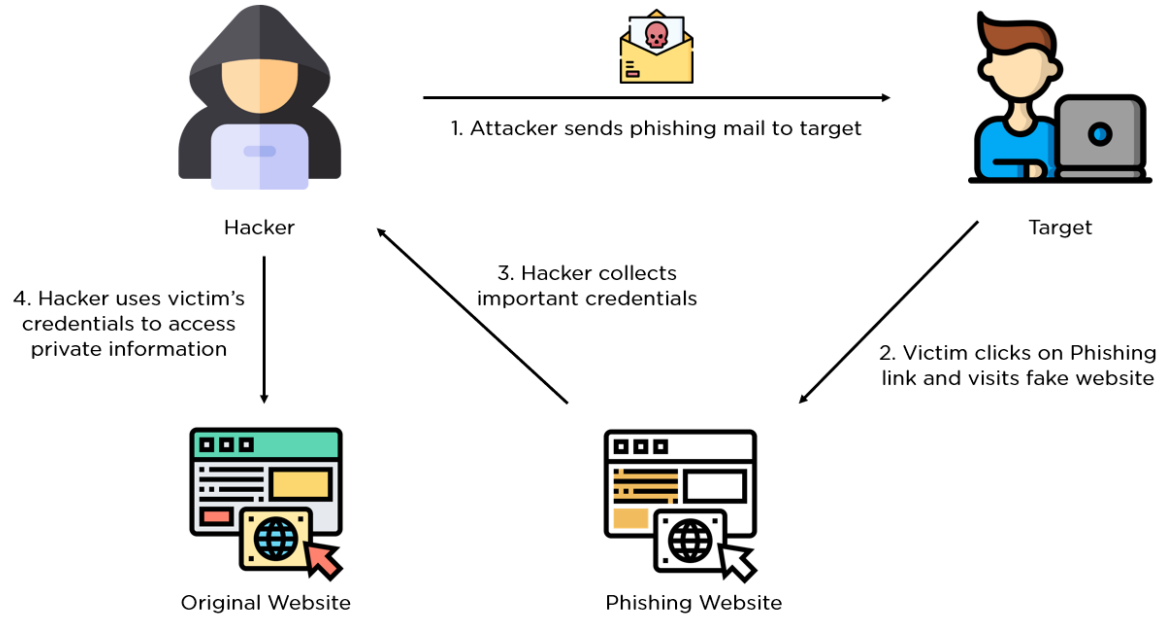

Рис.1.2. Фішингова атака

4) Спуфінг

Спуфінг - це метод, за допомогою якого кіберзлочинець маскується під відоме або надійне джерело. Таким чином, зловмисник може ввійти в контакт з жертвою і отримати доступ до її систем або пристроїв з кінцевою метою викрадення інформації, вимагання грошей або встановлення на пристрій шкідливого програмного забезпечення чи іншого шкідливого програмного забезпечення.

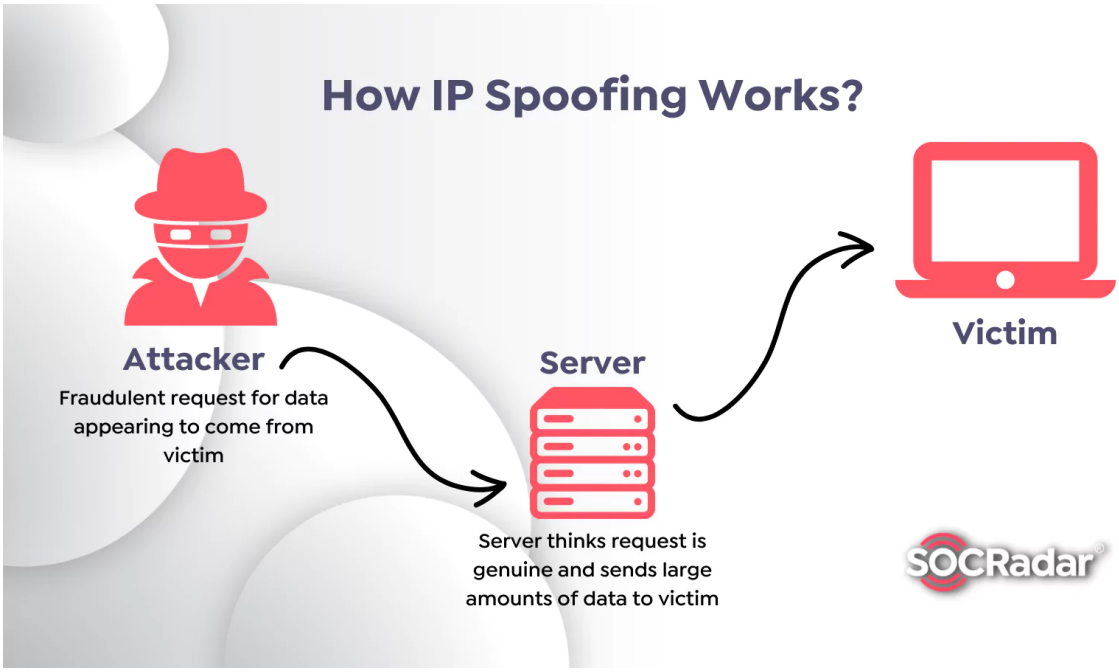

Рис.1.2. Спуфінг

5) Атаки на основі ідентифікаційних даних

Атаки на основі ідентифікаційних даних надзвичайно важко виявити. Коли облікові дані дійсного користувача скомпрометовані, а зловмисник маскується під цього користувача, часто дуже важко відрізнити типову поведінку користувача від поведінки хакера, використовуючи традиційні заходи та інструменти безпеки.

6) Атаки на введення коду

Атаки на впровадження коду полягають у тому, що зловмисник вводить шкідливий код у вразливий комп'ютер або мережу, щоб змінити хід її роботи.

7) Атаки на ланцюги поставок

Атака на ланцюжок поставок - це тип кібератаки, спрямований на довіреного стороннього постачальника, який пропонує послуги або програмне забезпечення, що є життєво важливими для ланцюжка поставок. Атаки на програмне забезпечення впроваджують шкідливий код у додаток, щоб заразити всіх користувачів програми, тоді як атаки на апаратне забезпечення компрометують фізичні компоненти з тією ж метою. Ланцюги постачання програмного забезпечення є особливо вразливими, оскільки сучасне програмне

забезпечення не пишеться з нуля: воно включає в себе багато готових компонентів, таких як сторонні API, відкритий вихідний код і власний код від постачальників програмного забезпечення.

8) Атаки з використанням соціальної інженерії

Соціальна інженерія - це метод, коли зловмисники використовують психологічну тактику, щоб маніпулювати людьми, змушуючи їх виконувати бажані дії. Використовуючи потужні мотиватори, такі як любов, гроші, страх і статус, зловмисники можуть збирати конфіденційну інформацію, яку згодом можуть використати для вимагання грошей в організації або для отримання конкурентних переваг.

9) Внутрішні загрози

IT-команди, які зосереджуються виключно на пошуку супротивників за межами організації, бачать лише половину картини. Внутрішні загрози - це внутрішні суб'єкти, такі як нинішні або колишні працівники, які становлять небезпеку для організації, оскільки мають прямий доступ до мережі компанії, конфіденційних даних та інтелектуальної власності, а також знання бізнес-процесів, політик компанії або іншої інформації, яка може допомогти здійснити таку атаку.

Внутрішні агенти, які становлять загрозу для організації, як правило, зловмисні за своєю природою. Деякі мотиви включають фінансову вигоду в обмін на продаж конфіденційної інформації в темному інтернеті та/або емоційний примус, як, наприклад, у тактиці соціальної інженерії. Але деякі інсайдерські загрози не є зловмисними за своєю природою - вони скоріше є недбалими. Для боротьби з ними організаціям слід впровадити комплексну навчальну програму з кібербезпеки, яка навчить зацікавлених осіб усвідомлювати будь-які потенційні атаки, в тому числі й ті, що можуть бути здійснені інсайдером.

10) Тунелювання DNS

DNS-тунелювання - це тип кібератаки, який використовує запити та відповіді системи доменних імен (DNS) для обходу традиційних заходів безпеки та передачі даних і коду в мережі.

Після зараження хакер може вільно займатися командно-контрольною діяльністю. Тунель дає хакеру можливість запустити шкідливе програмне забезпечення та/або витягти дані, IP-адреси чи іншу конфіденційну інформацію, кодуючи її побітно в серії DNS-відповідей.

Атаки з використанням DNS-тунелів почастішали останніми роками, частково через те, що їх відносно просто розгорнути. Набори інструментів і посібники з тунелювання навіть легко доступні в Інтернеті через такі популярні сайти, як YouTube.

11) Атаки на основі Інтернету речей

Атака на Інтернет речей (IoT) - це будь-яка кібератака, спрямована на пристрій або мережу IoT. Після компрометації хакер може отримати контроль над пристроєм, викрасти дані або приєднатися до групи заражених пристроїв, щоб створити бот-мережу для здійснення DoS- або DDoS-атак.

З огляду на те, що кількість підключених пристроїв, як очікується, буде швидко зростати, експерти з кібербезпеки очікують, що кількість інфекцій IoT також буде зростати. Крім того, розгортання мереж 5G, які сприятимуть використанню підключених пристроїв, також може призвести до збільшення кількості атак.

12) Атаки з використанням штучного інтелекту

З розвитком технологій штучного інтелекту та машинного навчання зростає і кількість випадків їхнього використання. Так само, як фахівці з кібербезпеки використовують ШІ та ML для захисту свого онлайн-середовища, зловмисники також використовують ці інструменти, щоб отримати доступ до мережі або викрасти конфіденційну інформацію [4].

1.4 Розвиток кібератак та прогнози розвитку

Коли пандемія COVID-19 набрала обертів і здавалося, що весь світ перейшов в онлайн, у 2020 році ще більше зросла кількість програм-вимагачів, фішингових

атак і витоків даних.9 Лише з початку лютого до кінця квітня кількість кібератак на фінансовий сектор зросла на 238% по всьому світу.

23 квітня 2020 року Всесвітня організація охорони здоров'я (ВООЗ) повідомила про тривожний витік електронних адрес і паролів. Група елітних хакерів, очевидно, провела велику фішингову кампанію, в результаті якої у співробітників ВООЗ було викрадено 450 активних облікових даних для входу в систему. Далі хакери викрали майже 25 000 приватних електронних адрес з таких установ, як Центр з контролю і профілактики захворювань (CDC), Національні інститути охорони здоров'я (NIH) і Фонд Білла і Мелінди Гейтс.

Організації з розміром, славою та ресурсами державних установ все ще вразливі до кібератак. У 2020 році компанія Software AG була другим за величиною постачальником програмного забезпечення в Німеччині та сьомим за величиною в Європі. У жовтні того ж року внаслідок атаки вірусу-здирника було викрадено близько одного терабайта її даних. Викравши інформацію компанії, хакери заблокували її IT-інфраструктуру і погрожували оприлюднити конфіденційні дані до отримання викупу в розмірі 23 мільйонів доларів.

За прогнозами, до 2029 року кіберзлочинність коштуватиме бізнесу 15,63 трильйона доларів США, тому фахівці з кібербезпеки перебувають у постійному пошуку кількох поширених типів кіберзагроз.

1) Удосконалені атаки з використанням програм-вимагачів

Атаки з використанням програм-вимагачів не є чимось новим, але останніми роками вони стали більш складними. Сьогодні існують навіть постачальники програм-вимагачів як послуг, які надають свої програми в оренду іншим кіберзлочинцям в обмін на відсоток від прибутку.12 Така бізнес-модель призвела до збільшення кількості атак з використанням програм-вимагачів у всьому світі. За даними Statista, у 2023 році 72,7% організацій по всьому світу постраждали від атак зловмисників у порівнянні з 55,1% у 2018 році.

2) Вплив третіх сторін

Оскільки все більше компаній співпрацюють з третіми сторонами, такими як підрядники та постачальники, кіберзлочинці обходять складні системи безпеки,

зламуючи менш захищені мережі цих третіх сторін. Наприклад, у 2021 році хакери проникли в мережі Facebook, Instagram та LinkedIn, зламавши стороннього підрядника (найнятого трьома компаніями) на ім'я Socialarks. Під час атаки кіберзлочинці здійснили витік персональних даних понад 214 мільйонів користувачів соціальних мереж.

3) Компрометація фінансових даних

Чим більше ми зберігаємо свої фінансові дані онлайн, тим важливішим стає їх захист. Номери кредитних карток, пін-коди банківських рахунків, номери телефонів, інвестиційні рахунки та інша особиста ідентифікаційна інформація (PII) регулярно зламуються і використовуються в злочинних цілях, вимагаючи великих витрат часу, грошей і зусиль, оскільки люди, які стали жертвами атак, намагаються відновити свою фінансову довіру і приватність.

4) Атаки, що фінансуються державою

Сьогодні держави використовують власні кібернавички для атак на критично важливу інфраструктуру інших урядів. Найпоширенішими системами, що піддаються атакам, є електромережі та транспортні системи. Як правило, суб'єкти загроз, пов'язані з національними державами, здійснюють ці атаки з метою викрадення інтелектуальної власності, даних військової розвідки та інших видів конфіденційної інформації, якою керують урядові організації.

1.5 Кібератаки майбутнього та їх наслідки

У найближчі роки маштаб кіберзагроз продовжуватиме розвиватися і ставатиме дедалі складнішим. Новітні технології, такі як штучний інтелект і машинне навчання, мають багато переваг, але вони також привносять нові тенденції в ландшафт кібератак. Кіберзлочинці постійно використовуватимуть ШІ для здійснення своїх атак і намагатимуться випередити існуючі заходи безпеки. Очікувані кібер-тренди включають:

1) Ризики 5G та периферійних обчислень:

Подальше розгортання мереж 5G і впровадження периферійних обчислювальних пристроїв створить додаткові вразливості, якими, ймовірно, скористаються кіберзлочинці

2) Загрози квантових обчислень:

Квантові обчислення становлять небезпеку для сучасних технологій шифрування і навіть можуть зробити їх застарілими; ми можемо побачити зростаючу потребу в нових квантово-стійких методах шифрування для подолання проблем безпеки

3) Проблеми безпеки біометричних даних: Оскільки використання біометричних даних стає все більш поширеним у системах безпеки, зловмисники можуть зламати такі бази даних; це може назавжди скомпрометувати дані і прокласти шлях до широкомасштабної крадіжки особистих даних [5].

1) *Вартість кібератак*

За прогнозами Cybersecurity Ventures, у 2024 році глобальна вартість кібератак сягне 9,5 трильйонів доларів США, причому значну частину цього зростання спричинять програми-вимагачі, фішинг та витоки даних .

Ці фінансові наслідки виходять за рамки безпосередніх збитків і включають в себе довгострокові наслідки, такі як репутаційні втрати, судові витрати і регуляторні штрафи.

Як зазначає Cobalt Magazine, зростаюча складність цих атак ускладнює захист від них, особливо зважаючи на те, що програми-вимагачі продовжують атакувати підприємства кожні 11 секунд.

Перехід на віддалену роботу ще більше збільшив вразливості, що призводить до більш дорогих витоків даних, оскільки децентралізовані системи залишаються відкритими для експлуатації.

Insurance Journal повідомляє, що у відповідь на ці зростаючі ризики премії з кіберстрахування підскочили на 50% у 2022 році, оскільки компанії прагнуть захистити себе.

За даними Cybersecurity Ventures, очікується, що вартість кіберзлочинів продовжить зростати, потенційно досягнувши $10,5 трлн щорічно до 2025 року.

Ця статистика кібербезпеки від Cybersecurity Ventures підкреслює гостру необхідність для бізнесу впроваджувати надійні стратегії кібербезпеки, щоб захистити себе від ескалації фінансових збитків та операційних ризиків у найближчі роки.

2) *Статистика витоків критичних даних та хакерських атак*

У 2024 році витоки даних продовжують залишатися дорогим викликом для організацій у всьому світі. Згідно зі звітом IBM «Вартість витоку даних у 2024 році», середня вартість витоку даних зросла на 12% порівняно з попереднім роком, досягнувши $4,62 млн.

Найбільше постраждала галузь охорони здоров'я, де витрати на порушення в середньому становлять $10,93 млн за інцидент через чутливий характер даних.

Фішингові атаки та атаки на ділову електронну пошту (BEC) є одними з найпоширеніших і найдорожчих - в середньому $4,88 млн на одне порушення. Ключовим фактором, що зумовлює зростання цих витрат, є час, необхідний для виявлення та реагування на інциденти.

Середня тривалість життєвого циклу виявлення та локалізації порушень становить 277 днів, що ще більше посилює фінансові наслідки для постраждалих організацій.

Крім того, компанії, які впровадили штучний інтелект і автоматизацію в свої системи безпеки, значно скоротили свої витрати, заощадивши в середньому 2,22 мільйона доларів на один інцидент, порівняно з тими, хто не використовував ці технології.

Це свідчить про зростаючу важливість інвестування в передові інструменти безпеки для пом'якшення фінансових та операційних наслідків витоку даних.

Ці дані свідчать про те, що організаціям необхідно не лише вдосконалювати свої засоби захисту кібербезпеки, але й оптимізувати стратегії реагування на інциденти, щоб скоротити час на виявлення та локалізацію інцидентів, що в кінцевому підсумку мінімізує вплив порушень у майбутньому.

3) *Статистика фішингу*

Фішингові атаки стали ще більш поширеною загрозою у 2024 році, на них

припадає майже 30% усіх витоків даних у світі, згідно зі звітом IBM «Вартість витоку даних у 2024 році» (2024 Cost of a Data Breach Report).

Ці атаки дуже ефективні, оскільки експлуатують людську довіру, виманюючи у жертв конфіденційну інформацію або облікові дані для доступу.

Середня вартість витоку даних, пов'язаного з фішингом, зараз становить $4,88 млн за інцидент, що підкреслює його фінансові втрати для організацій (Verizon DBIR).

Фішингові кампанії еволюціонують, зловмисники використовують штучний інтелект для створення все більш переконливих електронних листів і веб-сайтів, що ускладнює виявлення шахрайства для приватних осіб і компаній.

Крім того, згідно зі звітом IBM « Вартість витоку даних у 2024 році», пов'язані з фішингом порушення часто займають до 206 днів, що значно подовжує операційні та фінансові збитки.

Ця тенденція у сфері безпеки підкреслює критичну важливість інвестицій у навчання співробітників та впровадження передових антифішингових технологій, таких як фільтрація електронної пошти та інструменти виявлення на основі штучного інтелекту, для боротьби з постійно зростаючою загрозою.

4) *Статистика програм-вимагачів*

У 2024 році кількість атак програм-вимагачів продовжує зростати, причому кількість інцидентів постійно зростає в різних галузях.

Згідно зі звітом Управління ООН з наркотиків і злочинності (UNODC), ці атаки відбуваються із загрозливою швидкістю: новий інцидент відбувається приблизно кожні 11 секунд.

За оцінками Cybersecurity Ventures, глобальна вартість збитків від програм-вимагачів може сягнути 30 мільярдів доларів до кінця року, підкреслюючи зростаючу серйозність цих атак.

Сектор охорони здоров’я залишається особливо вразливим: звіт IBM Cost of a Data Break Report за 2024 рік показує, що злам програм-вимагачів у сфері

охорони здоров’я обходиться в середньому в 10,93 мільйона доларів США за інцидент.

Крім того, простої, спричинені програмами-вимагачами, призводять до значних фінансових втрат: за даними Egnyte, компанії втрачають у середньому 8500 доларів США на годину через збій у роботі. Ці тривалі періоди відновлення посилюють фінансові та операційні труднощі, з якими стикаються постраждалі компанії.

Незважаючи на великі виплати викупу, відновлення даних не гарантується. Багатьом організаціям важко повністю відновити свої системи після сплати викупу.

Ці статистичні дані щодо кібербезпеки підкреслюють нагальну потребу компаній інвестувати в посилення заходів кібербезпеки та ефективні стратегії реагування на інциденти для боротьби зі зростаючою загрозою програм-вимагачів.

5) *Статистика шкідливих програм*

Нещодавній звіт Statista показує постійне зростання інцидентів зі зловмисним програмним забезпеченням: у 2023 році по всьому світу було виявлено понад 6,06 мільярда атак, особливо зосереджених в Азіатсько-Тихоокеанському регіоні.

Серед типів шкідливих програм, які найчастіше блокувалися, були трояни, хробаки та програми-вимагачі, які продовжують становити серйозну загрозу в різних секторах.

За даними Station X, у 2024 році 81% організацій зіткнулися із загрозами зловмисного програмного забезпечення. Ця статистика підкреслює поширеність і постійність зловмисного програмного забезпечення як ключової проблеми кібербезпеки.

З таким високим відсотком постраждалих компаній боротьба зі зловмисним програмним забезпеченням за допомогою розширених стратегій виявлення та запобігання є більш важливою, ніж будь-коли, для мінімізації ризиків і захисту конфіденційних даних.

6) *Статистика кібербезпеки за галузями*

Згідно з різними статистичними даними кібербезпеки за 2024 рік, ризики кібербезпеки значно відрізняються в різних галузях, і певні сектори стикаються з більш серйозними загрозами.

6.1) *Статистика кібербезпеки охорони здоров'я*

Сектор охорони здоров'я став головною мішенню для кіберзлочинців, головним чином через величезні обсяги конфіденційних даних, які він обробляє, і життєво важливі послуги, які він надає.

У 2023 році середня вартість витоку даних у сфері охорони здоров'я зросла до 10,93 мільйона доларів за інцидент, що майже вдвічі більше, ніж у фінансовому секторі, який становив у середньому 5,9 мільйона доларів за витік. Ці кібератаки не тільки порушують конфіденційні дані пацієнтів, але й створюють серйозні ризики для безпеки та добробуту пацієнтів.

За даними Всесвітнього економічного форуму, такі атаки можуть порушити роботу цілої системи охорони здоров'я, поставивши під загрозу життя та роботу. Із зростанням цифровізації послуг охорони здоров'я зміцнення кібербезпеки стало невідкладним пріоритетом для галузі.

6.2) *Статистика кібербезпеки фінансової галузі*

Кібератаки у фінансовому секторі зросли більш ніж удвічі з часу пандемії, піддаючи компанії більшому ризику. Деякі, як-от Equifax, зіткнулися зі значними штрафами, сплативши понад 1 мільярд доларів після серйозного порушення в 2017 році.

Відповідно до звіту МВФ про глобальну фінансову стабільність за квітень 2024 року, надзвичайні збитки від кібератак значно зросли з 2017 року і зараз досягли 2,5 мільярда доларів. Ці втрати можуть загрожувати фінансовій стабільності компанії та створити проблеми з фінансуванням.

Крім того, непрямі витрати, такі як шкода репутації та необхідність посилених заходів безпеки, ще більше посилюють фінансовий тиск на постраждалі компанії.

6.3) *Статистика кібербезпеки підприємств*

Згідно з дослідженням Betanews, кіберзлочинці можуть успішно проникнути в 93% корпоративних мереж. Ця тривожна статистика підкреслює зростаючу вразливість корпоративної безпеки, особливо у зв'язку з тим, що атаки, керовані штучним інтелектом, стає все важче виявляти. У дослідженні, проведеному Positive Technologies, тести на проникнення в таких секторах, як фінанси, енергетика, уряд та IT, показали, що зловмисники можуть подолати захист і отримати доступ до локальних мереж у 93% випадків.

Крім того, CISCO повідомила, що 40% малих і середніх підприємств (МСП), які зазнали кібератаки, зазнали щонайменше восьмигодинного простою, причому цей простій спричинив значні фінансові збитки.

Хоча 43% кібератак спрямовані на малий бізнес, лише 14% з них відчувають себе достатньо підготовленими до захисту від таких загроз, як показало дослідження «Вартість кіберзлочинів», проведене компанією Accenture.

6.4) *Статистика кібербезпеки в освіті*

Згідно з Опитуванням порушень кібербезпеки 2024, проведеним Департаментом науки, інновацій та технологій (DSIT), 71% середніх шкіл та 52% початкових шкіл повідомили, що зазнали кібератак у минулому році.

Найпоширенішим методом був фішинг: 92% початкових шкіл та 89% середніх шкіл стикалися зі спробами фішингу.

Незважаючи на підвищену увагу до безпеки, початкові та середні школи рідше, ніж коледжі та університети, звертаються за подальшими рекомендаціями щодо заходів кібербезпеки.

Хоча 75% початкових шкіл і 81% середніх шкіл впровадили політику кібербезпеки, у звіті зазначається, що початкові школи, як правило, мають менш просунутий захист.

Це підкреслює постійну потребу в поліпшенні кібербезпеки в навчальних закладах, особливо на початковому рівні [6].

Висновки до першого розділу

Проаналізовано можливі ризики які трапляються під час віддаленної роботи працівників у компаніях, тенденції їх розвитку у майбутньому та вплив.

Розглянуто можливі наслідки дій кіберзлочинців при успішних атаках на компанії по всьому світу з урахуванням витрат на компенсації роботи підприємств тощо.

Зазначено, що зупинення функціонування компанії та її бізнес процесів призводить до втрат доходів компанії та довіри користувачів до підприємства, через що страждає його репутація. Це призводить до сповільнення безнес процессів компанії що може призвести до банкротства.

2 ДОСЛІДЖЕННЯ МЕТОДІВ БОРОТЬБИ З КІБЕРАТАКАМИ ЗА ДОПОМОГОЮ VPN СЕРВІСІВ

2.1 Методи боротьби з атаками

У сучасному світі кібербезпека важлива як ніколи. Зважаючи на постійне зростання загроз для бізнесу, наявність надійного рішення для захисту є абсолютно необхідною.

Існує занадто багато загроз, щоб ігнорувати ризики - від програм-вимагачів до фішингу, вони можуть коштувати дуже значних витрат, а профілактика є ключем до успіху в досягненні надійного захисту систем.

1. Навчання персоналу.

Один з найпоширеніших способів, як кіберзлочинці отримують доступ до даних, - через співробітників компанії. Вони надсилають шахрайські електронні листи, видаючи себе за когось із працівників організації, і просять або надати особисті дані, або доступ до певних файлів. Посилання часто здаються законними для недосвідченого ока, і легко потрапити в пастку.

Один з найефективніших способів захисту від кібератак і всіх видів витоку даних - це навчання співробітників запобіганню кібератак та інформування їх про поточні кібератаки.

2. Постійне оновлення свого програмного забезпечення та систем.

Часто кібератаки відбуваються через те, що системи користувачів або програмне забезпечення не повністю оновлені, залишаючи вразливі місця. Кіберзлочинці використовують ці слабкі місця, щоб отримати доступ до мережі. Коли вони потрапляють всередину, часто буває занадто пізно вживати превентивних заходів.

Щоб протистояти цьому, розумно інвестувати в систему управління виправленнями , яка буде керувати всім програмним забезпеченням і системними оновленнями, підтримуючи систему стійкою і актуальною.

3. Забезпечений захист кінцевих точок.

Захист кінцевих точок захищає мережі, які віддалено підключені до пристроїв. Мобільні пристрої, планшети та ноутбуки, підключені до корпоративної мережі, надають шляхи доступу до загроз безпеці. Ці шляхи необхідно захистити за допомогою спеціального програмного забезпечення для захисту кінцевих точок.

4. *Встановлений брандмауер.*

Захист мережі за допомогою брандмауера - один з найефективніших способів захиститися від будь-якої кібератаки. Система брандмауера заблокує будь-які атаки грубої сили на мережу та/або системи до того, як вони зможуть завдати шкоди.

5. *Резервне копіювання даних.*

На випадок катастрофи (часто кібератаки) компанія повинна мати резервну копію даних, щоб уникнути серйозних проблем, втрати даних і інших фінансових втрат.

6. *Контрольований доступ до систем.*

Атака на систему може бути фізичною, тому контроль над тим, хто може отримати доступ до мережі, є дуже важливим. Хтось може просто зайти до офісу чи підприємства і вставити USB-носій із зараженими файлами в один з комп'ютерів, що дозволить йому отримати доступ до всієї мережі або заразити її.

7. *Безпека Wi-Fi.*

Будь-який пристрій може заразитися при підключенні до мережі, якщо цей заражений пристрій потім підключиться до бізнес-мережі, вся система буде під серйозною загрозою.

Захист і приховування бездротових мереж - одна з найбезпечніших речей, яку може зробити для своєї системи кожен користувач. Оскільки бездротові технології розвиваються все більше і більше з кожним днем, з'являються тисячі пристроїв, які можуть підключитися до мережі і скомпрометувати її.

8. *Особисті кабінети співробітників.*

Кожному працівнику потрібен власний логін для кожної програми. Кілька користувачів, що підключаються під одними і тими ж обліковими даними, можуть поставити бізнес під загрозу.

Наявність окремих логінів для кожного співробітника допоможе зменшити кількість фронтів атак. Користувачі будуть входити в систему лише один раз на день і використовуватимуть лише свій власний набір логінів. Підвищена безпека - не єдина перевага, власник бізнесу також отримає покращену зручність використання для його співробітників.

9. *Управління доступом.*

Одним із ризиків для власників бізнесу, які мають працівників, є встановлення ними програмного забезпечення на службових пристроях, що може скомпрометувати системи.

Керування правами адміністратора та блокування встановлення або навіть доступу співробітників до певних даних у мережі є корисним для безпеки.

10. *Управління паролями.*

Встановлення однакових паролів може бути небезпечним. Якщо зловмисник дізнається пароль, він отримає доступ до всього, що є у системі.

Встановлення різних паролів для кожної програми, яка використовується, є реальною перевагою для безпеки, а часта їх зміна дозволить підтримувати високий рівень захисту від зовнішніх і внутрішніх загроз [7].

11. Використання VPN

VPN захищають користувачів від хакерів. Вони приховують реальні IP-адреси користувачів, що ускладнює хакерські атаки на них, і можуть запобігти різним типам кібератак, включаючи DDoS-атаки, атаки «людина посередині», зараження шкідливим програмним забезпеченням, перехоплення сеансів і фішингові спроби [8].

2.2 Типи VPN та їх характеристика

1) Міжмережевий VPN

Міжмережевий VPN встановлює зв'язок між двома або більше окремими мережами, наприклад, головною мережею компанії та мережею її супутникових офісів. Багато організацій впроваджують міжмережеві VPN, щоб використовувати інтернет-шляхи для передачі конфіденційних даних замість приватних каналів MPLS.

Організації з декількома філіями, розташованими в різних регіонах, часто використовують VPN-мережі типу «сайт-сайт». Завдяки такому налаштуванню компанії можуть безпечно інтегрувати свою центральну мережу з віддаленими офісами, забезпечуючи безперебійний зв'язок і спільний доступ до ресурсів так, ніби вони є однією єдиною мережею. Рішення site-to-site може бути розгорнуте як VPN на основі екстранету, коли компанія з'єднує свою мережу з мережами партнерів, постачальників або клієнтів.

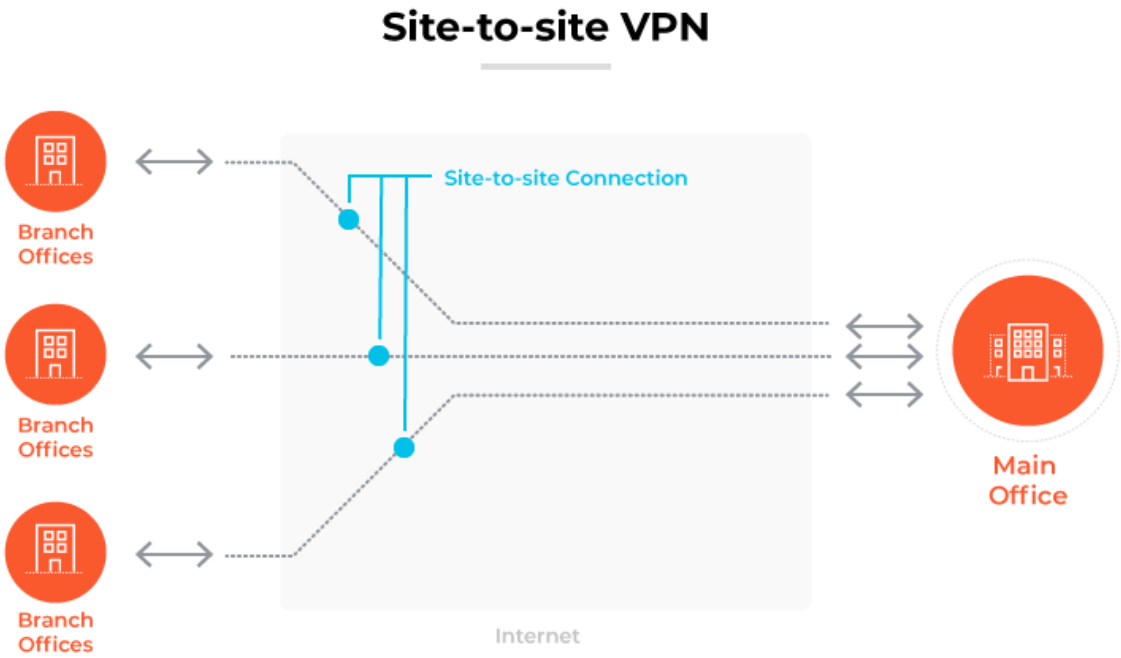

Рис.2.1. Міжмережевий VPN

2) VPN віддаленного доступу

Віддалений доступ до VPN дозволяє користувачам, які перебувають за межами офісу, безпечно підключатися до додатків та інформації в головному центрі обробки даних компанії, шифруючи всі передані та отримані дані користувача.

VPN віддаленного доступу забезпечує безпеку незалежно від публічного місцезнаходження користувача, створюючи практично приватне з'єднання за допомогою тунелю між мережею підприємства і віддаленим користувачем.

Це досягається шляхом шифрування даних, що робить їх нерозбірливими для потенційних перехоплювачів. Користувачі можуть взаємодіяти з мережею своєї компанії так, ніби вони перебувають на місці, забезпечуючи безпечну передачу даних, не побоюючись зовнішнього втручання або витоку даних.

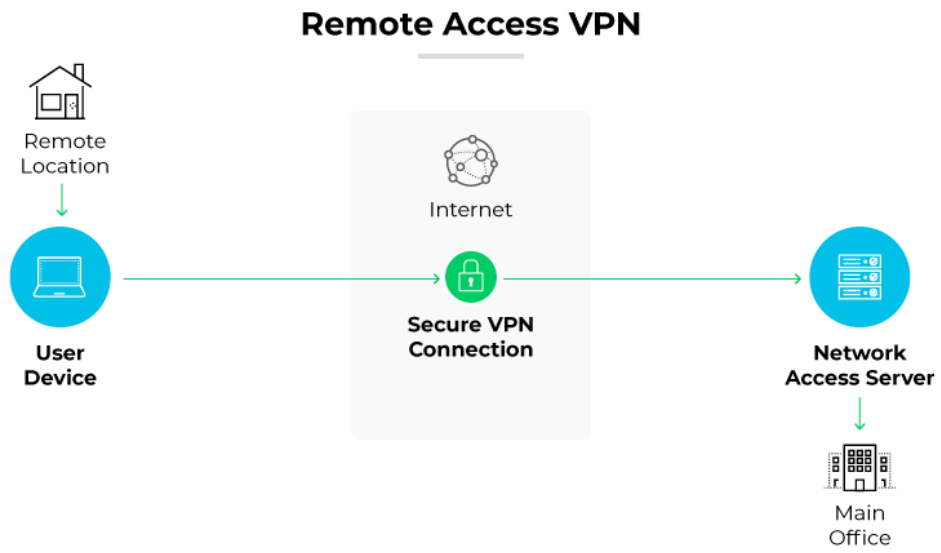

Рис.2.2. VPN віддаленного доступу

3) Хмарний VPN

Хмарний VPN, який іноді називають хостинговим VPN або VPN як послуга (VPNaaS), - це підхід до VPN, адаптований для хмарних середовищ. Такий VPN дозволяє користувачам отримати безпечний доступ до ресурсів, даних і додатків

компанії в хмарі через веб-інтерфейс або спеціальний додаток на настільних або мобільних пристроях.

На відміну від звичайного VPN, які потребують спеціальної інфраструктури в місці розташування користувача, хмарні VPN легко інтегруються в хмарну дистрибутивну структуру компанії. Однією з важливих переваг хмарних VPN є швидке налаштування та розгортання по всьому світу.

Використання хмарної VPN підвищує рівень безпеки порівняно з традиційними VPN і сприяє більш адаптивному, гнучкому і масштабованому налаштуванню хмарних сервісів для бізнесу.

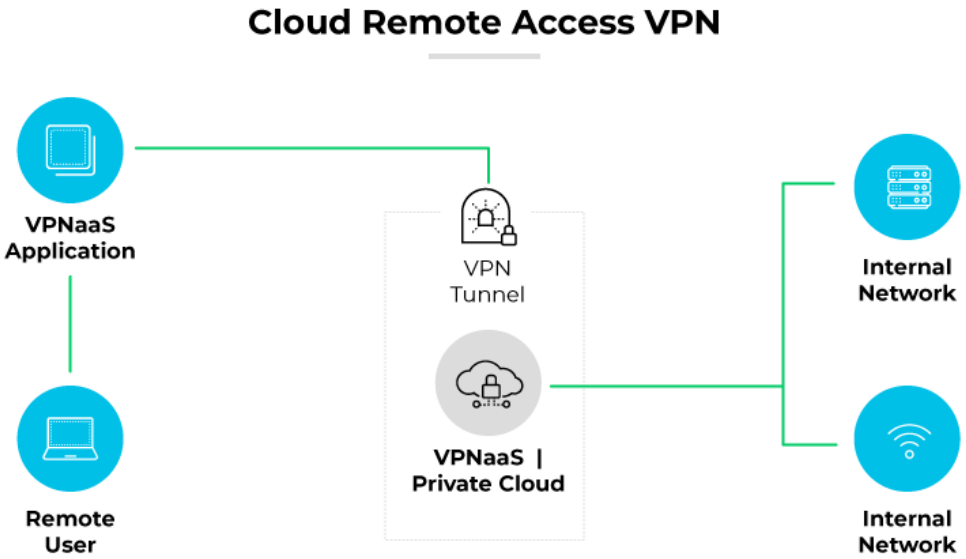

Рис.2.3. Хмарний VPN

4) SSL VPN

SSL VPN, або віртуальна приватна мережа на рівні захищених сокетів (Secure Sockets Layer), дозволяє віддаленим користувачам підключатися до приватних мереж у безпечний спосіб. Вона використовує протокол безпеки SSL або його наступника, протокол безпеки транспортного рівня (TLS), щоб забезпечити зашифровану передачу даних між пристроєм користувача і шлюзом VPN. Таке шифрування захищає цілісність і конфіденційність даних, гарантуючи, що неавторизовані суб'єкти не зможуть їх перехопити або змінити.

На відміну від деяких VPN-рішень, SSL VPN не вимагає спеціалізованого клієнтського програмного забезпечення на пристроях користувачів. Замість цього вона використовує стандартні веб-браузери, що робить її більш доступною і зменшує складність розгортання. Весь зв'язок між веб-браузером користувача і пристроєм VPN шифрується, що робить передачу даних через потенційно небезпечні мережі безпечною.

Існує два типи SSL VPN:

4.1) Портальний SSL VPN

У цій моделі користувачі отримують доступ до однієї веб-сторінки або порталу, який містить посилання на інші ресурси приватної мережі. Відвідавши певний веб-сайт і ввівши облікові дані, користувачі можуть ініціювати безпечне SSL-з'єднання. Потім цей портал надає доступ до визначених додатків або мережевих служб, як це визначено організацією.

4.2) Тунельний SSL VPN

Цей варіант є більш комплексним і дозволяє користувачам отримати безпечний доступ до багатьох мережевих сервісів, а не лише до тих, що базуються на веб-технологіях. Він створює зашифрований тунель за протоколом SSL, що забезпечує безпечний доступ до різних ресурсів. Для оптимальної роботи Tunnel SSL VPN можуть знадобитися браузери, оснащені додатковими програмами, такими як JavaScript або Flash.

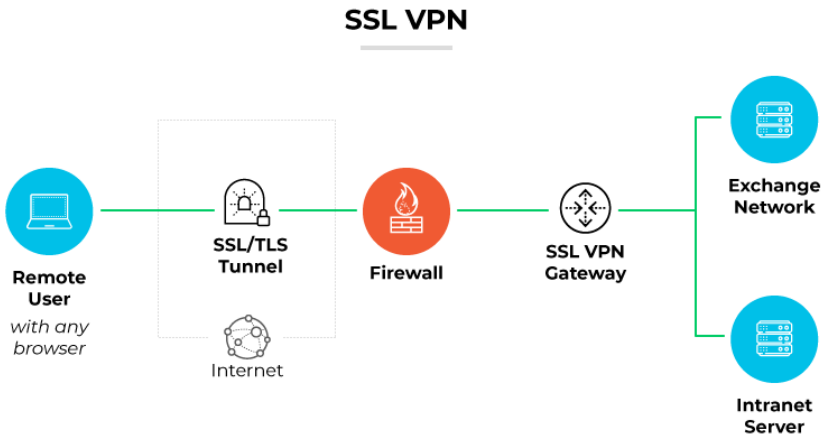

Рис.2.4. SSL VPN

5) Подвійний VPN

Подвійний VPN - це скоріше конфігурація, ніж тип технології VPN. Ця конфігурація передбачає спрямування трафіку користувача через два послідовні VPN-сервери, забезпечуючи два рівні шифрування. При стандартному використанні VPN дані надходять з пристрою користувача на один VPN-сервер, а потім до місця призначення в Інтернеті. При використанні подвійної конфігурації VPN дані користувача спочатку шифруються і надсилаються на початковий VPN-сервер. Потім вони знову шифруються і надсилаються на другий VPN-сервер, перш ніж досягти кінцевого місця призначення в Інтернеті.

Хоча метод подвійного VPN підвищує безпеку, додаючи додатковий рівень шифрування, він також може призвести до зниження швидкості з'єднання. Це уповільнення є результатом того, що дані проходять через два окремі сервери і піддаються подвійному шифруванню. Хоча цей метод вигідний для тих, хто прагне підвищеної безпеки, він може бути не ідеальним для всіх через потенційний вплив на продуктивність.

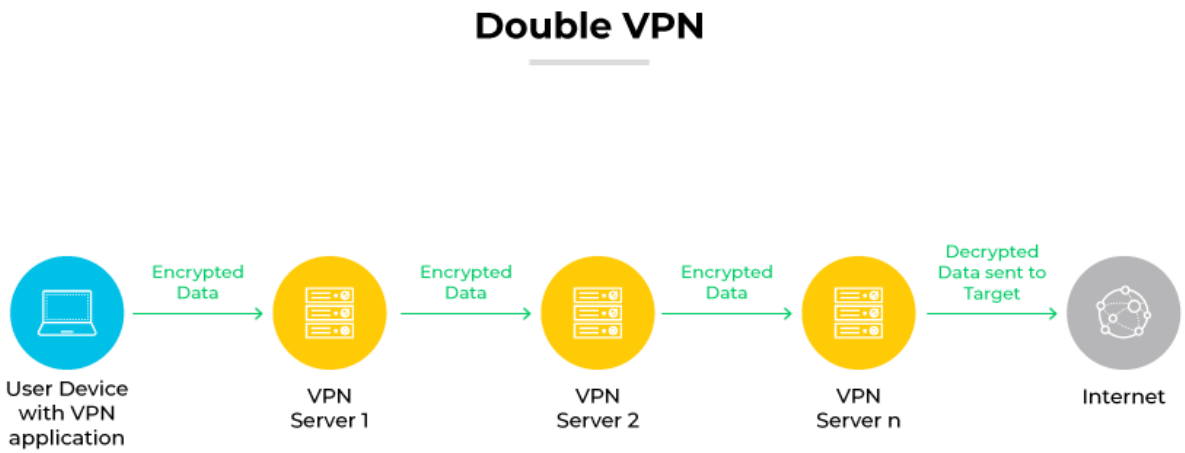

Рис.2.5. Подвійний VPN

2.3 Переваги та недоліки використання VPN

VPN були винайдені для забезпечення безпечного з'єднання між офісами компаній. З початку 1990-х років вони еволюціонували і стали критично важливим аспектом кібербезпеки для будь-якого типу бізнесу. Переваги VPN для бізнесу полягають у наступному:

1. Доступні рішення для захисту

VPN пропонують недорогий варіант захисту порівняно з апаратними брандмауерами та програмним забезпеченням для захисту від вторгнень. Апаратне забезпечення потребує обслуговування та оновлення прошивки, а програмні засоби необхідно ліцензувати та оновлювати. На відміну від них, VPN прості в управлінні, мають єдину ліцензію і забезпечують достатній захист від загроз для більшості компаній.

Шифрування та анонімізація IP-адреси також додають додаткової безпеки в мережі. Пристрої компанії можуть створювати віртуальні особи на іншому кінці планети, обманюючи потенційних зловмисників і знижуючи ймовірність вторгнень.

2. Ефективність передачі даних

Компанії можуть зіткнутися з проблемою зменшення швидкості передачі даних так само, як і приватні особи. Корпоративні провайдери можуть обмежувати швидкість з'єднання або нормувати пропускну здатність вище певного рівня. Коли ви використовуєте VPN, ймовірність цього набагато нижча. Ваш провайдер не може виміряти використання даних співробітниками, що дозволяє їм передавати великі обсяги даних без обмежень. Це дуже корисно для секторів з інтенсивним використанням даних, таких як рендеринг зображень або розробка програмного забезпечення.

3. Безпечне підключення для віддаленої роботи

Віддалена робота різко зросла під час пандемії Covid і залишатиметься значною частиною трудового життя. Але віддалений доступ може становити загрозу безпеці. Переїзд до домашнього офісу чи загальнодоступної мережі Wi-Fi

розширює поверхню загрози, а домашнє підключення до Інтернету, яке використовують працівники, може наражати дані на зовнішніх зловмисників.

VPN вирішують ці проблеми. Коли користувач використовує VPN, віе створюює безпечне з'єднання між локальними серверами та віддаленими пристроями. Шифрування та анонімність роблять працівників невидимими для сторонніх, незалежно від того, користуються вони громадським Wi-Fi у кафе чи вдома.

Працівники можуть бути максимально продуктивними, незалежно від того, яку мережу Wi-Fi їм потрібно використовувати. Вони можуть завантажувати та завантажувати важливі файли в залах очікування аеропорту або в громадському транспорті. І вони можуть залишатися на зв'язку, коли подорожують, не турбуючись про безпеку.

4. Надійна конфіденційність даних

Віртуальні приватні мережі є важливим інструментом конфіденційності для всіх компаній. Без шифрування та анонімізації конфіденційна інформація постійно знаходиться під загрозою. Інтернет-провайдер може реєструвати та читати трафік за бажанням. Окремі програми можуть збирати дані користувачів для маркетингових цілей (або кіберзлочинності). Служби SaaS і пошукові системи також реєструють активність користувачів.

Реєстрація даних може не бути проблемою для звичайних браузерів. Але компанії регулярно повідомляють конфіденційну інформацію про стратегію, проекти та клієнтів. Дані компанії надзвичайно цінні для зловмисників і конкурентів і завжди мають бути захищені. Використання VPN вирішує цю проблему. Анонімізація IP-адреси дуже ускладнює реєстрацію або відстеження.

5. Гнучка безпека для кожного пристрою та налаштування

Гнучкість є однією з найбільших переваг захисту віртуальної приватної мережі. Компанії можуть додати покриття VPN до нових пристроїв за лічені секунди. Коли робочі станції підключаються або менеджери додають нових користувачів, VPN миттєво вмикаються, захищаючи мережеві активи від зовнішніх загроз. Безпека мережі змінюється природно зі зміною периметра.

За потреби компанії можуть додавати VPN до кількох пристроїв. Працівники можуть користуватися тим самим захистом на ноутбуках, планшетах і смартфонах. Команди, які працюють поза офісом, можуть об'єднати всі пристрої в одній службі віртуальної приватної мережі, тоді як маршрутизатори VPN захищають офісне середовище. Завдяки захисту VPN безпека адаптується до будь-якої ситуації.

6. Легка підтримка та обслуговування

Апаратні рішення безпеки вимагають постійного моніторингу та оновлень. Це забирає час команд безпеки, який можна витратити на тонке налаштування інших питань безпеки. У VPN керування сервером передається стороннім постачальникам. Сервіси VPN обслуговують сервери та забезпечують безпеку – більш ефективний варіант для невеликих компаній. Стороннє керування також зменшить витрати на підтримку порівняно з власними альтернативами.

7. VPN добре працюють із застарілими системами

VPN пропонують рішення безпеки для компаній, яким наразі бракує ресурсів для здійснення цифрової трансформації в хмару. Шифрування VPN накладає на існуючі програми. Немає необхідності змінювати їх код або конфігурацію. Поки користувачі можуть отримати доступ до програм через Інтернет, захист VPN зробить їх безпечнішими у використанні. Покриття VPN також скорочує витрати на заміну застарілого програмного забезпечення до потрібного моменту [9].

Попри всі переваги, існує ряд недоліків зв'язаних з використанням VPN, а саме:

1. *Обмеження пропускної здатності*

Однією з головних проблем під час використання VPN є можливе зниження швидкості Інтернету. Шифрування даних і їх маршрутизація через віддалені сервери може призвести до затримки, що спричинить повільніше з'єднання. Додаткові кроки, пов'язані з тунелюванням VPN, можуть значно вплинути на швидкість завантаження та завантаження.

Це може бути особливо проблематично для компаній, які покладаються на швидке та безперебійне з’єднання для таких дій, як відеоконференції або потокове передавання вмісту високої чіткості.

2. Проблеми безпеки та довіри

VPN покладаються на шифрування для безпечної передачі даних. Однак, якщо постачальник VPN використовує слабкі протоколи шифрування або не вміє належним чином запровадити шифрування, він може наражати дані користувача на перехоплення та компрометацію.

Сервери VPN також можуть стати цілями для кібератак, особливо якщо вони не обслуговуються належним чином або не мають оновлень безпеки. Зламаний VPN-сервер розкриває дані користувачів і потенційно надає несанкціонований доступ зловмисникам. Регулярні перевірки безпеки та своєчасні виправлення необхідні для забезпечення цілісності серверної інфраструктури VPN.

3. Проблеми сумісності

Технологія VPN може бути складною, і не всі служби VPN сумісні з усіма пристроями та операційними системами. Деякі протоколи VPN можуть не працювати на певних платформах або вимагати налаштування вручну, через що процес налаштування стає тягарем для менш обізнаних у техніці користувачів. Певні програми та веб-сайти можуть не працювати оптимально або взагалі не працювати, коли ввімкнено VPN, що може призвести до розчарування в роботі користувача.

4. Юридичні та нормативні наслідки

Використання VPN для доступу до геообмеженого вмісту або обходу цензурних заходів може порушувати місцеве законодавство або порушувати умови певних платформ. Хоча самі VPN є законними в більшості країн, діяльність, що здійснюється через них, може бути нелегальною. Важливо знати про правові та етичні наслідки, пов’язані з використанням VPN, особливо під час роботи в країнах із суворішими правилами Інтернету.

5. Поганий досвід користувача

VPN передають трафік до центру обробки даних або штаб-квартири компанії, що означає, що відстань відіграє вирішальну роль у продуктивності. Це також створює центральну пропускну здатність. Чим далі хтось, тим більше затримки він відчуває. Крім того, чим більше користувачів використовують обмежену пропускну здатність, тим більший вплив на продуктивність.

Подібним чином транспортування трафіку для підключення до хмарних додатків або програм SaaS є неефективним. У результаті багато співробітників уникають VPN або подібних рішень для віддаленого доступу, окрім випадків, коли це необхідно, що ще більше підвищує ризик, обмежуючи видимість і контроль [10].

2.4 Повний функціонал VPN та його властивості

VPN означає віртуальну приватну мережу. Це тип мережі, до якої користувач може підключитися, і яка допоможе захистити онлайн-безпеку та конфіденційність.

VPN діє як тунель, через який усі дані переходять від місцезнаходження користувача до місця призначення. Усе це належним чином зашифровано та захищено, тому стороння сторона не може бачити, які дані він передає.

Використання VPN має багато переваг, зокрема:

1. Конфіденційність

2. Анонімність

3. Безпека

4. Шифрування

5. *Маскування або зміна вашої оригінальної IP-адреси*

VPN працює шляхом маршрутизації/пересилання всіх даних із ноутбука чи телефону через VPN до Інтернету, а не безпосередньо через Інтернет-провайдера.

Коли користувач використовує VPN, він шифрує всі дані на стороні клієнта. Після того як дані зашифровано, вони проходять через VPN-тунель, до якого інші не мають доступу, а потім потрапляють в Інтернет.

Перш ніж пройти через тунель VPN, запит спочатку надсилається його провайдеру, але оскільки він зашифрований, провайдер не може зрозуміти, до чого ви намагаєтеся отримати доступ. Тому він пересилає його запит на сервер VPN. Потім VPN надсилає запит на потрібну IP-адресу або веб-сайт [11].

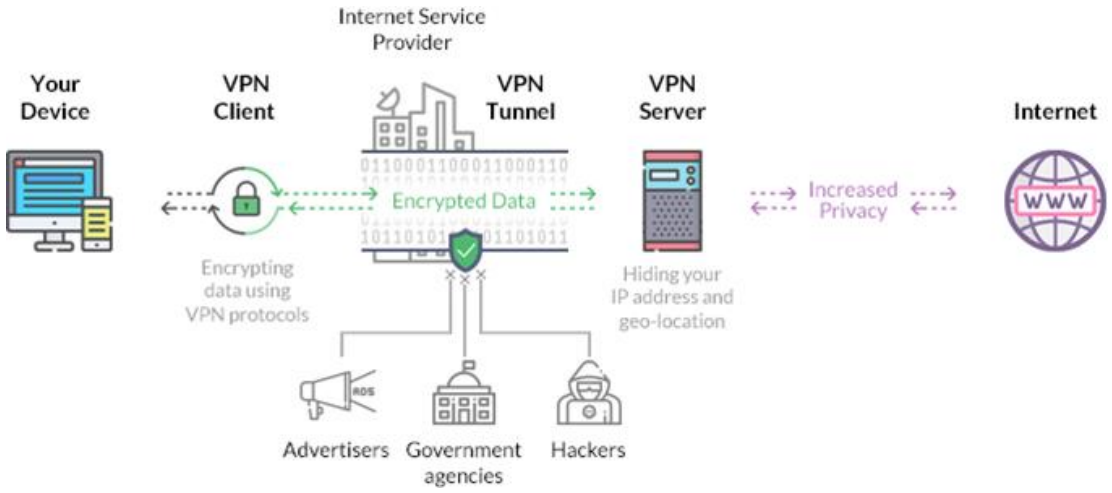

Рис.2.6. Принцип роботи VPN

Коли VPN пропускає трафік через безпечний тунель, щоб тримати його невидимим для третіх сторін, він приховує дані, щоб ніхто не міг скомпрометувати їх під час передачі. Шифрування VPN – це процес кодування інформації на обох кінцях цього тунелю. Він перетворює звичайний текст на зашифрований текст, складність якого залежить від типу шифрування, яке використовує певна служба VPN.

VPN використовують різні шифри, деякі з яких, наприклад AES-256, набагато ефективніші за інші.

Надійні служби VPN забезпечують наскрізне шифрування. Це означає, що ваші дані захищені на кожному етапі процесу спілкування. Навіть якщо повідомлення чи запит розшифровуються попутно, вони все одно захищені від потенційних кіберзагроз.

Ключ шифрування — це рядок інформації, необхідної для кодування та декодування даних. Завдяки ключу шифрування лише особа або пристрій, які його мають, можуть отримати доступ до зашифрованих даних, розшифрувавши їх.

Існує два основних типи ключів шифрування, які широко використовуються в VPN:

1. Симетричні ключі шифрування.

Цей тип шифрування забезпечує обидві сторони процесу зв’язку однаковим ключем шифрування. За допомогою симетричного методу шифрування простий текст перетворюється на зашифрований за допомогою ключа шифрування, а потім отримувач може «розблокувати» його за допомогою подібного ключа. Однак цей підхід не підходить, якщо дані, надіслані з пристрою користувача, мають інший пункт призначення – сервер VPN.

2. Асиметричний ключ шифрування.

За такого підходу замість подібного ключа доведеться використовувати два різні ключі шифрування – відкритий ключ для шифрування повідомлення та закритий ключ для його розшифровки. Таким чином, відкритий ключ допомагає перетворити повідомлення на код, а потім надсилає його власнику закритого ключа, єдиному, хто може його декодувати.

Більшість служб VPN використовують як симетричні, так і асиметричні підходи до шифрування даних користувачів. У той час як зв'язок базується на принципах асиметричного шифрування, обмін ключами відбувається за допомогою симетричного шифрування.

Рис.2.7. Шифрування під час роботи VPN

Наступні типи шифрів VPN є найбільш поширеними, але не всі вони однаково потужні. Зокрема, існують шифри, які використовують 64, 128 і 256 біт. Тут варто зауважити, що чим більше біт надає шифр, тим він безпечніший. Тому, обираючи службу VPN, користувачеві обов'язково слід врахувати тип шифрування, який вона використовує.

1. Blowfish

Blowfish — найстаріший стандарт шифрування VPN із 64-бітними блоками. Остання версія Blowfish підтримує 128-бітне шифрування. Однак він все ще має багато вразливостей і, швидше за все, буде зламаний, ніж його більш сучасні альтернативи.

2. Camellia

Camellia — досить потужний блоковий шифр, доступний із протоколом безпеки OpenVPN. Сьогодні Camellia підтримує 64, 128 і навіть 256 бітове шифрування.

3. AES

AES (Advanced Encryption Standard) — найвідоміший блоковий шифр і золотий стандарт для сучасних рішень VPN. Він вважається найбезпечнішим і

найпотужнішим методом шифрування даних і їх передачі без ризику бути зламаним.

Ось два основних типи шифрування AES:

1. 128-бітне шифрування AES.

AES-128 не вимагає багато ресурсів і є швидшим за інші методи шифрування. Однак 128 біт може бути недостатньо, якщо користувач надає пріоритет конфіденційності в Інтернеті.

2. 256-бітове шифрування AES.

Сьогодні цей стандарт шифрування є найбільш безпечним. Він розбиває 256 фрагментів загального тексту на 256 блоків, унеможливлюючи викрадення даних користувача хакерами за допомогою атаки грубої сили. Їм знадобляться роки, щоб розшифрувати одне повідомлення чи запит. Ось чому всі надійні постачальники VPN використовують шифрування AES-256 [12].

Рис.2.8. Приклад AES-256 шифрування

2.5 Порівняння різних VPN від різних постачальників

Рис.2.9. Proton VPN

На додаток до звичайних можливостей VPN, він включає багатохопове підключення та доступ до мережі Tor через VPN. Він також оснащений переосмисленим інтерфейсом програми для приємного використання. Хоча базова платна служба VPN має середню ціну, вона також має найкращу безкоштовну підписку на VPN.

Обліковий запис у Proton VPN також надає доступ до інших продуктів у Proton, зокрема Proton Mail і Proton Drive. Це включає в себе безкоштовні облікові записи, що робить його відмінним додатком. Також, він має функцію Stealth, яка розроблена, щоб забезпечити додаткову безпеку особливо загрозливим користувачам.

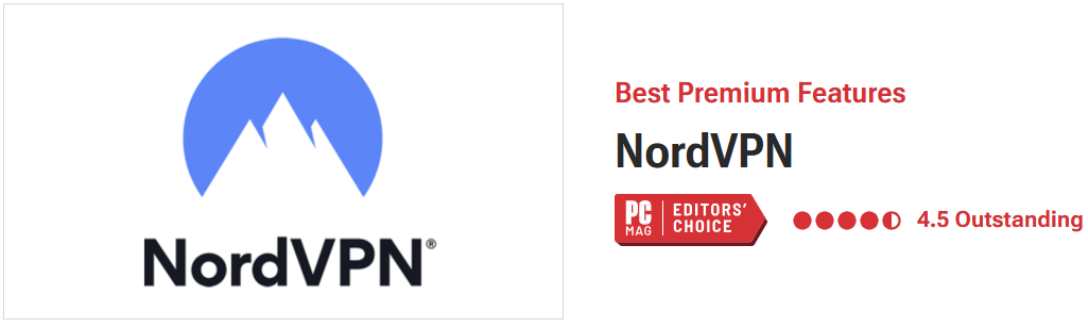

Рис.2.10. NordVPN

З самого початку він включає такі функції, як багатохопове з'єднання та доступ до Tor через VPN, обидві з яких досі рідко зустрічаються серед конкурентів. У все ще новому світі VPN.

NordVPN завжди був надійним продуктом для використання та зберіг послідовний і сучасний дизайн на всіх своїх платформах. Nord не боїться змін, адже стала однією з перших VPN-компаній, яка повністю охопила новий протокол WireGuard VPN і сервери лише з оперативною пам’яттю.

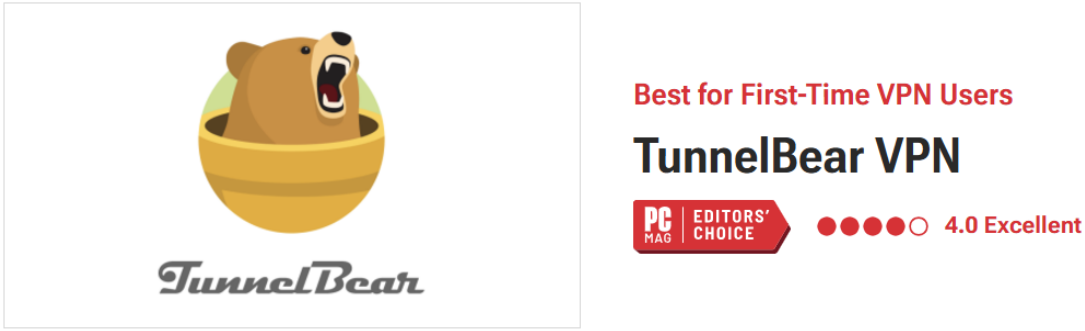

Рис.2.11. TunnelBear VPN

Сервіс надзвичайно простий у використанні та пропонує безкоштовну підписку з обмеженою пропускною спроможністю, що робить його чудовим вибором для тих, хто не знайомий із мережами VPN і може спробувати, перш ніж купувати. TunnelBear VPN також має один із найпрозоріших процесів аудиту в галузі, що робить його ім’ям, якому можна довіряти.

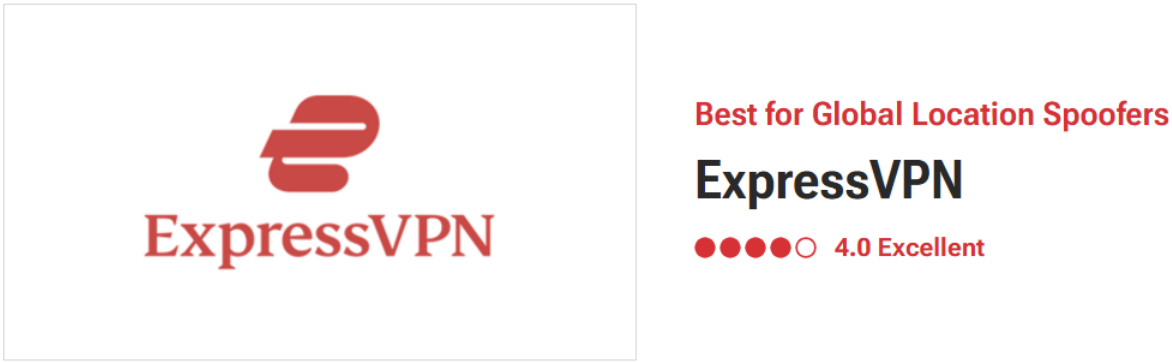

Рис.2.12. ExpressVPN

ExpressVPN присутній у 95 країнах та на щастя має дуже мало віртуальних серверів, більшість його серверів є фізично реальними. Замість WireGuard він пропонує власний протокол Lightway VPN, який використовує криптографічну бібліотеку wolfSSL з відкритим кодом і пройшов аудит третьої сторони.

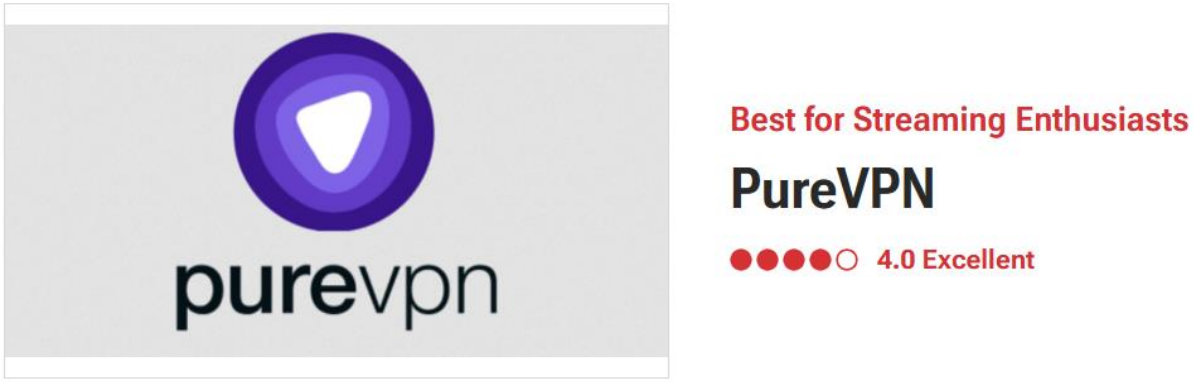

Рис.2.13. PureVPN

PureVPN швидкий і має масу серверів по всьому світу, безліч доповнень, прозору політику конфіденційності тощо, все це робить його привабливим, комплексним VPN.

Рис.2.14. CyberGhost VPN

CyberGhost – це дорогий, але надзвичайно потужний VPN-сервіс із величезною колекцією серверів. Він добре працював під час тестування та пропонує сім одночасних підключень, антивірусний захист і блокувальник реклами, серед інших додаткових функцій.

Рис.2.15. IPVanish VPN

В середньому VPN захищає п’ять пристроїв за підписку, IPVanish в свою чергу не обмежує кількість пристроїв. Крім того, IPVanish має вражаюче глобальне покриття серверів, велику кількість додаткових функцій і широку підтримку платформи для завантаження.

Рис.2.16. Mullvad VPN

Mullvad VPN має рідкісну систему облікових записів, орієнтовану на конфіденційність, і навіть дозволяє платити анонімно. Mullvad VPN надзвичайно прозорий, надаючи клієнтам величезну кількість інформації про те, як працює їхній сервіс. Найкраще те, що послуга Mullvad VPN має постійну фіксовану ставку та є надзвичайно доступною — лише 5 євро на місяць.

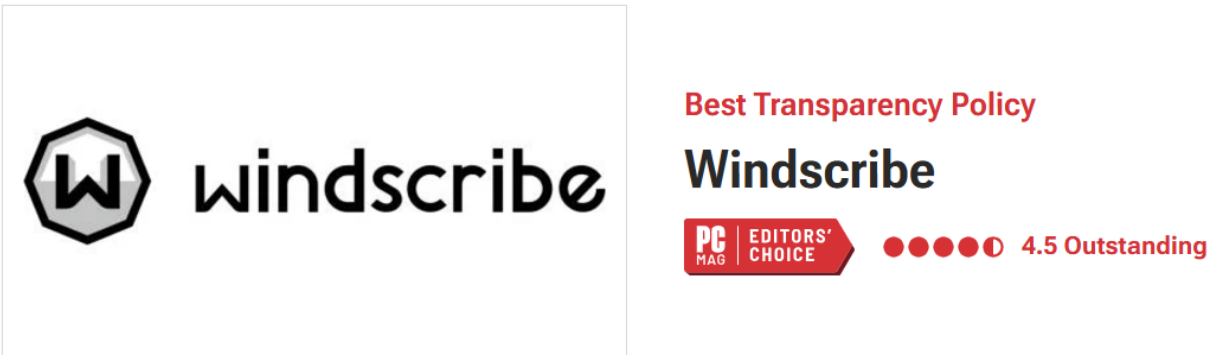

Рис.2.17. Windscribe

Windscribe має багато можливостей, включаючи неперевершену базу даних підтримки разом із корисним помічником зі штучним інтелектом, доступ до бібліотеки Open Netflix у всіх регіонах, і високий рівень безкоштовного обслуговування.

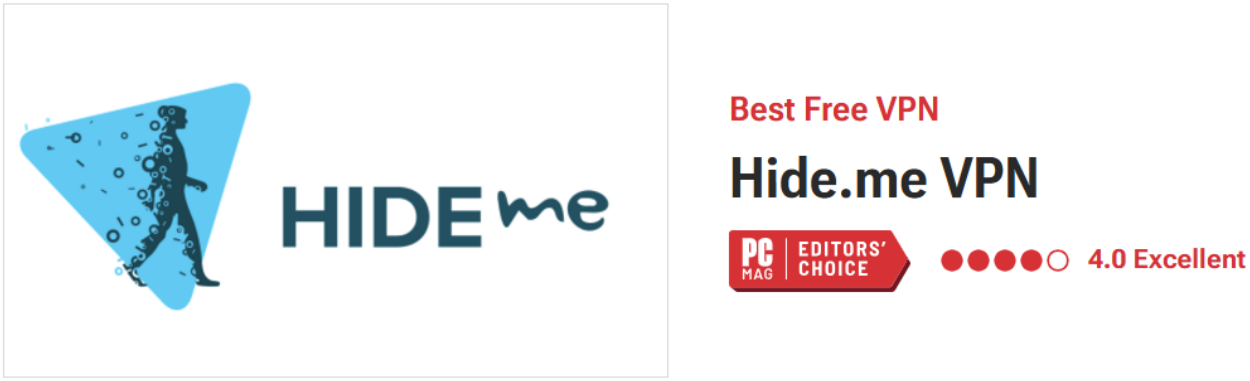

Рис.2.18. Hide.me VPN

Hide.me VPN — це щось на зразок універсальної мережі, яка пропонує привабливу ціну, а також зручне розповсюдження клієнта та сервера. Крім того, безкоштовний клієнт Hide.me не поступається деяким кращим платним варіантам [13].

Висновки до другого розділу

Проаналізовано методи боротьби з кібератаками та способи захисту від них.

Досліджено, що будь-яка система не може вважатись цілком безпечною, але зменшити ризик проникнення шкідливого програмного забезпечення може кожен, якщо буде дотримуватись простих інструкцій та проводити інструктаж своїм працівникам в компанії відносно актуальних кіберзагроз.

Зазначено, що інують кращі рішення аніж VPN, але зпоміж своїх конкурентів відносно ціни та якості - VPN є лідером у галузі, адже дає можливість постійного шифрування трафіку за відносно невеликі кошти.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІДДАЛЕННИХ КОРИСТУВАЧІВ НА БАЗІ CISCO SECURE VPN

3.1 Загальний огляд CiscoSecure VPN Client

Cisco AnyConnect VPN — це потужне рішення безпеки, розроблене компанією Cisco Systems, призначене для встановлення безпечних з’єднань між користувачами та корпоративними мережами через Інтернет. Це дозволяє віддаленим користувачам безпечно отримувати доступ до корпоративних ресурсів, незалежно від їхнього фізичного розташування чи умов мережі.

Cisco AnyConnect VPN працює, створюючи безпечне та зашифроване з’єднання між пристроєм користувача та корпоративною мережею чи іншими захищеними ресурсами. Ось як це працює:

1. *Ініціювання підключення*: коли користувач ініціює підключення до корпоративної мережі або інших захищених ресурсів, клієнтське програмне забезпечення Cisco AnyConnect VPN, встановлене на його пристрої, створює запит на підключення.

2. *Автентифікація*: користувач повинен пройти автентифікацію на сервері VPN за допомогою своїх облікових даних, таких як ім’я користувача та пароль. Залежно від конфігурації процес автентифікації також може включати багатофакторні методи автентифікації для підвищення безпеки.

3. *Встановлення безпечного тунелю*: після автентифікації Cisco AnyConnect VPN встановлює безпечний тунель між пристроєм користувача та сервером VPN. Цей тунель зашифровано за допомогою передових протоколів шифрування, таких як SSL/TLS або IPsec, для захисту даних, що передаються через Інтернет.

4. *Шифрування даних*: усі дані, що передаються між пристроєм користувача та сервером VPN, шифруються в безпечному тунелі. Це шифрування гарантує, що

конфіденційна інформація залишається конфіденційною та безпечною, навіть якщо вона перетинає ненадійні мережі або публічні точки доступу Wi-Fi.

5. *Маршрутизація трафіку*: за допомогою безпечного тунелю Cisco AnyConnect VPN направляє весь мережевий трафік із пристрою користувача через сервер VPN. Це дозволяє користувачеві отримувати доступ до ресурсів у корпоративній мережі або інших захищених мережах так, ніби вони безпосередньо підключені до них.

6. *Контроль доступу та політики*: Cisco AnyConnect VPN забезпечує застосування політик контролю доступу, визначених IT-адміністраторами організації. Ці політики визначають, які користувачі мають доступ до певних ресурсів і які дії вони можуть виконувати після підключення до VPN.

7. *Безперервний моніторинг і безпека*: протягом сеансу VPN Cisco AnyConnect VPN безперервно відстежує з'єднання на наявність будь-яких загроз безпеці або аномалій. Він використовує різні механізми безпеки, такі як системи виявлення/запобігання вторгненням (IDPS) і функції безпеки кінцевої точки, щоб забезпечити цілісність і конфіденційність з'єднання.

8. *Завершення та очищення*: коли користувач завершує сеанс VPN або виходить із системи, Cisco AnyConnect VPN акуратно завершує безпечний тунель і очищає будь-які тимчасові ресурси, пов'язані з підключенням. Це гарантує відсутність залишкових слідів сеансу VPN на пристрої користувача.

Загалом Cisco AnyConnect VPN забезпечує надійне та безпечне рішення для віддаленого доступу, що дозволяє користувачам безпечно підключатися до корпоративних мереж і ресурсів з будь-якого місця, зберігаючи при цьому конфіденційність і цілісність передачі даних [14].

3.2 Налаштування Cisco Secure VPN Client

Налаштування Cisco Secure VPN передбачає виконання кількох кроків для забезпечення безпечного та безперебійного з'єднання. Для налаштування Cisco Secure VPN користувач повинний слідувати наступним крокам:

Крок 1: Отримати VPN-клієнт Cisco AnyConnect

Відвідати веб-сайт Cisco або звернутись до IT-відділу організації, щоб отримати клієнтське програмне забезпечення Cisco AnyConnect VPN, сумісне з операційною системою (наприклад, Windows, macOS, iOS, Android).

Крок 2: Встановити Cisco AnyConnect VPN Client

Завантажити клієнтське програмне забезпечення Cisco AnyConnect VPN на пристрій.

Дотримуючись вказівок на екрані встановити програмне забезпечення.

Запустити VPN-клієнт Cisco AnyConnect після встановлення.

Крок 3: Налаштувати підключення VPN

Відкрити VPN-клієнт Cisco AnyConnect.

Ввести адресу сервера VPN, надану IT-відділом організації.

За бажанням користувач може налаштувати додаткові параметри підключення, наприклад метод автентифікації та протокол VPN.

Крок 4: Автентифікація

Ввести свої облікові дані, включаючи ім’я користувача та пароль, щоб авторизуватися на сервері VPN.

Дотримуватись будь-яких додаткових вказівок при автентифікації, наприклад багатофакторної автентифікації, якщо її ввімкнено.

Крок 5: Встановити підключення

Натиснути кнопку «Підключитися» або «Увійти», щоб встановити підключення до сервера VPN.

Зачекати, поки VPN-клієнт Cisco AnyConnect встановить безпечний тунель до сервера VPN.

Крок 6: Перевірити підключення

Після підключення, користувач повинний переконатися, що він успішно встановив з’єднання з VPN.

Перевірити стан з’єднання та деталі в інтерфейсі клієнта Cisco AnyConnect VPN.

Перевірити підключення до мережі, щоб переконатися, що він може безпечно отримати доступ до ресурсів у корпоративній мережі.

Крок 7: Налаштувати додаткові параметри (необов’язково)

Залежно від політики та вимог організації користувачеві може знадобитися налаштувати додаткові параметри VPN, наприклад розділене тунелювання, налаштування DNS або конфігурації проксі.

Крок 8: Від’єднатись від VPN-з’єднання

Коли користувачеві більше не потрібно використовувати з’єднання VPN, йому слід від’єднатись від сервера VPN.

Натиснути кнопку «Відключити» або «Вийти» в інтерфейсі клієнта Cisco AnyConnect VPN, щоб припинити з’єднання VPN.

Крок 9: Усунення несправностей

Якщо під час налаштування або використання у користувача виникають проблеми, йому слід звернутись до документації Cisco AnyConnect VPN або попросити допомоги у служби підтримки IT його організації.

Загальні дії щодо усунення несправностей включають перевірку підключення до мережі, перевірку налаштувань сервера VPN і перевірку правильності облікових даних автентифікації.

Виконуючи ці кроки, користувач зможе успішно встановити та налаштувати Cisco AnyConnect VPN для безпечного віддаленого доступу до корпоративних мереж і ресурсів. Також, слід пам’ятати, що під час використання Cisco AnyConnect VPN для віддаленого підключення слід дотримуватися правил безпеки організації та передових практик.

3.3 Основні характеристики Cisco AnyConnect VPN

Cisco AnyConnect VPN пропонує ряд ключових функцій, які роблять його комплексним і ефективним рішенням для безпечного віддаленого доступу. Ось деякі з його ключових особливостей:

1. *Безпечний віддалений доступ*: Cisco AnyConnect VPN забезпечує безпечний доступ до корпоративних мереж і ресурсів з будь-якої точки світу, дозволяючи співробітникам працювати віддалено без шкоди для безпеки.

2. *Багатофакторна автентифікація (MFA)*: підтримує багатофакторні методи автентифікації, включаючи паролі, токени та біометричні дані, щоб забезпечити безпечну автентифікацію користувача та зменшити ризик несанкціонованого доступу.

3. *Безпека кінцевої точки*: Cisco AnyConnect VPN пропонує функції захисту кінцевої точки для захисту від шкідливих програм, фішингових атак та інших загроз безпеці. Він допомагає захистити пристрої, підключені до корпоративної мережі, забезпечуючи повну безпеку.

4. *Розширене шифрування*: за допомогою розширених протоколів шифрування Cisco AnyConnect VPN шифрує всі дані, що передаються через Інтернет, захищаючи конфіденційну інформацію від перехоплення та несанкціонованого доступу.

5. *Централізоване керування*: адміністратори можуть централізовано керувати та застосовувати політики безпеки в розподілених мережах за допомогою Cisco AnyConnect VPN. Це централізоване керування спрощує адміністрування та забезпечує узгоджені заходи безпеки.

6. *Сумісність з платформами*: Cisco AnyConnect VPN сумісний із широким спектром операційних систем і пристроїв, включаючи Windows, macOS, iOS і Android. Ця сумісність забезпечує повну інтеграцію з існуючою інфраструктурою та різними середовищами пристроїв.

7. *Масштабованість*: Cisco AnyConnect VPN масштабується, щоб пристосуватися до зростаючої кількості віддалених користувачів і пристроїв без шкоди для безпеки чи продуктивності. Це гнучке рішення, яке може адаптуватися до мінливих потреб бізнесу та змінних вимог до мережі.

3.4 Переваги використання Cisco AnyConnect VPN

1. Cisco AnyConnect VPN підтримує широкий спектр пристроїв і операційних систем, включаючи Windows, macOS, iOS і Android.

2. Cisco AnyConnect VPN використовує протоколи шифрування та автентифікації галузевого стандарту для забезпечення найвищого рівня безпеки віддаленого доступу.

3. Хоча Cisco AnyConnect VPN в основному розроблено для корпоративного використання, деякі організації можуть пропонувати персональний доступ до VPN своїм співробітникам для віддаленої роботи.

Переваги використання Cisco AnyConnect VPN включають покращену безпеку, можливості віддаленого доступу, багатофакторну автентифікацію, безпеку кінцевої точки, централізоване керування, сумісність з платформами і масштабованість. Використовуючи ці переваги, організації можуть створити безпечне та ефективне середовище віддаленої роботи, зберігаючи при цьому відповідність нормативним вимогам.

3.5 Рекомендації щодо побудови безпечної віддаленної роботи

1. *Підключення через VPN.*

Віртуальні приватні мережі є одними з найпопулярніших інструментів безпеки для віддалених працівників, оскільки вони захищають дані в Інтернеті, зберігаючи при цьому таку саму безпеку, функціональність і зовнішній вигляд, якби вони були в мережі компанії.

2. *Встановлення багатофакторної аутентифікації.*

Багато компаній опираються запровадженню багатофакторної автентифікації. Очікування коду автентифікації — це крок, на який багато людей воліють не йти. Однак ця практика надзвичайно ефективна для запобігання порушень безпеки.

3. *Навчання співробітників передовим практикам.*

У компанії повинні бути створені чіткі правила безпеки для своїх співробітників, щоб вони розуміли, як захистити себе та свої дані.

4. *Оновлення програмного забезпечення.*

Незалежно від того, чи використовують співробітники обладнання компанії чи власні пристрої, переконайтеся, що вони знають, як запускати оновлення програмного забезпечення. Оновлення або виправлення програмного забезпечення можуть включати нові або вдосконалені функції, покращувати стабільність програмного забезпечення, додавати заходи безпеки та видаляти застарілі функції.

5. *Контроль фішингу електронної пошти.*

Працівникам компанії не слід відкривати чи натискати на підозрілі листи. Кіберзлочинці використовують фішинг, щоб спонукати користувачів ділитися даними та обліковими даними для входу, як правило, через електронну пошту, миттєвим або текстовим повідомленням. Хоча заходи IT-безпеки можуть допомогти, захист від фішингу починається з обізнаності співробітників.

6. *Створення надійних паролів.*

Унікальні паролі є необхідною мірою безпеки, яку багато працівників не сприймають серйозно. Не сілд покладатися на паролі, які легко зламати.

7. *Контроль бездротових мереж.*

Незахищені мережі полегшують кіберзлочинцям доступ до електронних листів і паролів. Не слід працювати в кав’ярнях чи в інших місцях, якщо в цьому немає крайньої необхідності [15].

Висновки до третього розділу

Проаналізовано основі можливості Cisco Secure VPN та розглянуто його налаштування для організації безпечної віддаленної роботи працівників у компанії.

Зазначено, що для побудови доступу до Cisco Secure VPN потрібно розгорнути та налаштувати мережеве обладнання, надано опис процесу.

Виокремлено, що Cisco Secure VPN є кращою версією серед усіх постачальників VPN послуг, адже він підтримує різні типи шифрування, дозволяє під’єднуватись з різних девайсів, а також захищає передачу даних через телефонну мережу загального користування. При цьому, він підтримує використання попередньо наданих ключів.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні теоретичні та наукові результати:

1) Проаналізовано можливі види атак на системи та методи для боротьби з ними. Розглянуто методи виявлення цим атак а також методи забезпечення конфіденційності персональних данних користувачів.

2) Досліджено, що саме помилки людей найчастіше призводять до порушень цілісності корпоративних даних у мережі, адже людина є найвразливішою ланкою у будь-якій системі.

3) Зазначено, що Cisco Secure VPN знижує ризик вторгнення у мережу, адже він шифрує мережевий трафік що проходить через нього.

4) Виокремлено можливі способи захисту мережі за допомогою технології Cisco Secure VPN.

5) Зроблено висновок, що будь-який програмно апаратний комплекс не зможе захистити повністю жодну систему, адже до тих пір поки в компанії є люди - вона буде вразливою. Програмно-апаратні комплекси та інші програмні рішення створені для того щоб мінімізувати ризики атак на корпоративну мережу всередині компанії тощо, але гарантувати повний захист вони не зможуть. Проте якщо проводити працівникам інструктажі, таким чином підвищувати їх обізнаність у світі актуальних загроз, то компанія може зберегти на цьому втрату своїх коштів та репутації. Саме за рахунок комплекних рішень та дій всередині компанії можна досягти високого рівня безпеки працівників під час віддаленної роботи із власних домівок.

ПЕРЕЛІК ПОСИЛАНЬ

1. Матвєєв О.А. Технологія захисту інформаційної системи організації віддалених користувачів. «Актуальні проблеми кібербезпеки» : Всеукр. науково-практ. конф., м. Київ, 25 жовт. 2024 р. Київ, 2024. С. 121–123.

2. The Hidden Dangers of Remote Work: Why It Can Be Harmful to the Individual URL: https://www.davron.net/the-hidden-dangers-of-remote-work-why-it-can-be-harmful-to-the-individual/

3. Researchers identify negative impacts of cyber attacks URL: https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks

4. 12 Most Common Types of Cyberattacks URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

5. Future Cyber Threats URL: https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats

6. The Business Impact of a Cyberattack in 2024: A Deep Dive URL: https://dev.to/donesrom/the-business-impact-of-a-cyberattack-in-2024-a-deep-dive-ndo

7. 10 Ways to Prevent Cyber Attacks URL: https://leaf-it.com/10-ways-prevent-cyber-attacks/

8. Does A VPN Protect From Hackers? Experts Answer (2024) URL: https://www.provendata.com/blog/does-vpn-protect-from-hackers/#:~:text=Yes%2C%20VPNs%20protect%20users%20from,session%20hijacking%2C%20and%20phishing%20attempts.

9. What are the main VPN benefits for businesses? URL: https://nordlayer.com/learn/vpn/benefits-of-vpn/

10. What are the disadvantages of using VPNs? URL: https://www.todyl.com/blog/disadvantages-using-vpns

11. How Does a VPN Work? URL: https://www.freecodecamp.org/news/how-does-a-vpn-work/

12. What is VPN encryption? URL: https://veepn.com/blog/what-is-vpn-encryption/

13. The Best VPN Services for 2024 URL: https://www.pcmag.com/picks/the-best-vpn-services

14. What Is Cisco AnyConnect VPN? A Complete Guide URL: https://medium.com/@gregorylaned/what-is-cisco-anyconnect-vpn-a-complete-guide-8566bc768da9

15. REMOTE SECURITY BEST PRACTICES FOR EMPLOYERS URL: https://www.helixstorm.com/blog/security-tips-for-working-remotely

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)