Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Засоби забезпечення інформаційної безпеки підприємства малого бізнесу

Виконавець: студент IV курсу, групи КБ-41

_____ **Владислав ЯКОВЕНКО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Микола БРАЇЛОВСЬКИЙ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
Сергій ТОЛЮПА
24 жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Яковенку Владиславу Юрійовичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби забезпечення інформаційної безпеки підприємства малого бізнесу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Засоби забезпечення інформаційної безпеки

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією про типові загрози та вразливості, розглянути засоби забезпечення інформаційної безпеки, а саме антивірусні програми фаєрволів, криптографічні засоби шифрування даних, засоби мережевої безпеки та засоби автентифікації. Розробити рекомендації щодо вибору та впровадження цих засобів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації щодо вибору та провадження засобів забезпечення ІБ з конкретними прикладами та детальним описом.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2023 року

Завдання видав _____ (підпис) Микола БРАЇЛОВСЬКИЙ (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Владислав ЯКОВЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2020	*виконано*
2	Аналіз літератури	23.01.2020 – 11.02.2020	*виконано*
3	Обґрунтування вибору рішення	12.02.2020 – 15.02.2020	*виконано*
4	Аналіз загроз, з якими стикаються підприємства малого бізнесу	16.02.2020 – 04.03.2020	*виконано*
5	Аналіз вразливостей, які можуть призвести до порушення інформаційної безпеки	05.03.2020 – 21.03.2020	*виконано*
6	Аналіз засобів забезпечення інформаційної безпеки	22.03.2020 – 08.04.2020	*виконано*
7	Вироблення рекомендацій щодо вибору та впровадження засобів забезпечення ІБ підприємства малого бізнесу	09.04.2020 – 10.05.2020	*виконано*
8	Оформлення пояснювальної записки	11.05.2020 – 27.05.2020	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2020 – 12.06.2023	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Владислав ЯКОВЕНКО
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 50 сторінок основного тексту, 2 таблиці та 6 рисунків. Список використаних джерел містить 22 найменування і займає 3 сторінки.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

Об'єктом дослідження є процес забезпечення інформаційної безпеки на підприємствах малого бізнесу

Предметом дослідження є самі засоби, методи і стратегії, які використовуються для забезпечення інформаційної безпеки в підприємствах малого бізнесу.

У роботі проаналізована існуюча література з теорії засобів забезпечення інформаційної безпеки підприємства малого бізнесу, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми засобів забезпечення інформаційної безпеки підприємства малого бізнесу.

Розроблені рекомендації щодо вибору та впровадження засобів забезпечення інформаційної безпеки підприємства малого бізнесу.

Ключові слова: Кіберзагрози, антивірусна програма, файрволи, система запобігання вторгненням.

ЗМІСТ

ПЕРЕЛІК УМОНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

МБ	–	Малий бізнес
ІБ	–	Інформаційна безпека
КЗ	–	Кіберзагроза
ЗЗІБ	–	Засоби забезпечення інформаційної безпеки
АП	–	Антивірусна програма
ФВ	–	Файрволи
MITM	–	Man-in-the-middle attack
IPS	–	Intrusion Prevention System
IDS	–	Intrusion Detection System
VPN	–	Virtual private network
ПЗ	–	Програмне забезпечення
АЗ	–	Апаратне забезпечення
СВВ	–	Система виявлення вторгнень
ЗА	–	Засоби автентифікації
КД	–	Контроль доступу
SSL	–	Secure Sockets Layer
TLS	–	Transport Layer Security
POP	–	Post Office Protocol
SNMP	–	Simple Network Management Protocol
DDoS	–	Distributed Denial of Service
RAT	–	Remote Administration Tool
WI-FI	–	Wireless Fidelity
DHCP	–	Dynamic Host Configuration Protocol
DoS	–	Denial-of-Service
DNS	–	Domain Name System
КСЗІ	–	Комплексна система захисту інформації
КЗЗ	–	Комплекс засобів захисту

ВСТУП

Актуальність роботи зумовлюється ти, що сучасна ділова сфера все більше опирається на інформаційні технології, що ставить перед підприємствами, особливо малого бізнесу, виклики щодо забезпечення інформаційної безпеки. Враховуючи зростаючу кількість кіберзагроз, які загрожують конфіденційності, цілісності та доступності даних, розуміння та ефективне використання засобів забезпечення інформаційної безпеки стає невід'ємною частиною успішної діяльності малого бізнесу.

Мета даної бакалаврської роботи полягає у вивченні та аналізі різних засобів забезпечення інформаційної безпеки на підприємствах малого бізнесу. Основним завданням є ідентифікація типових загроз, яким підлягають підприємства малого бізнесу, та розробка рекомендацій щодо вибору та впровадження ефективних заходів безпеки. Робота також передбачає проведення практичних досліджень з метою перевірки ефективності рекомендованих засобів забезпечення інформаційної безпеки на реальних підприємствах малого бізнесу.

Об’єктом дослідження є засоби забезпечення інформаційної безпеки на підприємствах малого бізнесу, оскільки воно сприяє підвищенню рівня захисту конфіденційної інформації, запобігає можливим витокам даних, забезпечує безперебійну роботу і надійність бізнес-процесів. Результати цього дослідження можуть бути використані підприємствами малого бізнесу для розробки та впровадження ефективних стратегій інформаційної безпеки.

Предметом дослідження є самі засоби, методи і стратегії, які використовуються для забезпечення інформаційної безпеки в підприємствах малого бізнесу.

Методи дослідження використані при підготовці дипломної роботи:

1. Літературний аналіз: Дослідження наукової літератури, наукових статей, книг, журналів та інших джерел, що стосуються засобів забезпечення інформаційної

безпеки підприємств малого бізнесу. Цей метод дозволить отримати теоретичні знання та розуміння ключових понять і принципів інформаційної безпеки.

2. Аналіз статистичних даних: Використання статистичних даних, звітів та досліджень щодо кібератак на підприємства малого бізнесу. Це дозволить оцінити розповсюдженість, тренди та характеристики таких атак і встановити їх вплив на малі бізнеси.

3. Порівняльний аналіз: Порівняння різних засобів забезпечення інформаційної безпеки, їх ефективності та придатності для підприємств малого бізнесу. Цей метод дозволяє встановити переваги, недоліки та відмінності між різними рішеннями та підходами в області інформаційної безпеки.

РОЗДІЛ 1
АНАЛІЗ ТИПОВИХ ЗАГРОЗИ ТА ВРАЗЛИВОСТІ МАЛОГО БІЗНЕСУ

1.1 Аналіз загроз, з якими стикаються підприємства малого бізнесу

У сучасному цифровому світі, де технології стають неодмінною складовою будь-якого бізнесу, інформаційна безпека стає дедалі важливішою. Підприємства малого бізнесу, які займають значну частку економіки, не є винятком. Вони стикаються з різноманітними інформаційними загрозами, які можуть поставити під загрозу їхню діяльність, конфіденційність даних та репутацію ось огляд таких загроз:

Кібератака – це будь-яка навмисна спроба викрасти, викрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп'ютерної системи чи цифрового пристрою [1].

Мотиви кібератак можуть бути різними, але є три основні категорії: кримінальні, політичні та особисті.

Кримінально мотивовані зловмисники прагнуть отримати фінансову вигоду через крадіжку грошей, крадіжку даних або зрив бізнесу. Кіберзлочинці можуть зламати банківський рахунок, щоб безпосередньо вкрасти гроші, або використовувати шахрайство соціальної інженерії, щоб обманом змусити людей надіслати їм гроші. Хакери можуть викрасти дані та використати їх для крадіжки особистих даних або продати їх у темній мережі чи зберігати їх для отримання викупу.

Вимагання - ще одна популярна тактика. Хакери можуть використовувати програми-вимагачі, атаки DDoS або інші тактики, щоб утримувати дані чи пристрої в заручниках, доки компанія не заплатить. Згідно з індексом X-Force Threat Intelligence Index, 27 відсотків кібератак спрямовані на вимагання жертв.

Особисто мотивовані зловмисники, такі як незадоволені нинішні чи колишні працівники, насамперед прагнуть відплати за якусь уявну образу. Вони можуть взяти гроші, викрасти конфіденційні дані або порушити роботу систем компанії.

Політично мотивовані зловмисники часто асоціюються з кібервійною, кібертероризмом. У кібервійні суб'єкти національної держави часто атакують урядові установи чи критичну інфраструктуру своїх ворогів. Наприклад, з початку російсько-української війни обидві країни зазнали низки кібератак на життєво важливі установи. Хакери-активісти, яких називають «хактивістами», можуть не завдати значної шкоди своїм цілям. Натомість вони зазвичай прагнуть привернути увагу до своїх причин, оприлюднюючи свої напади громадськості.

Менш поширені мотиви кібератак включають корпоративне шпигунство, під час якого хакери викрадають інтелектуальну власність, щоб отримати несправедливу перевагу над конкурентами, і пильних хакерів, які використовують вразливі місця системи, щоб попередити про них інших.

Хто стоїть за кібератаками?

Здійснювати кібератаки можуть злочинні організації, державні суб'єкти та приватні особи. Один із способів класифікувати суб'єктів загрози - класифікувати їх як сторонніх або внутрішніх загроз [2].

Зовнішні загрози не мають права використовувати мережу чи пристрій, але все одно проникають. Зовнішні суб'єкти кіберзагрози включають організовані злочинні групи, професійних хакерів, спонсорованих державою акторів, хакерів-любителів і хактивістів.

Інсайдерські загрози - це користувачі, які мають авторизований і законний доступ до активів компанії та зловживають своїми привілеями навмисно чи випадково. До цієї категорії входять співробітники, ділові партнери, клієнти, підрядники та постачальники з доступом до системи.

Хоча недбалі користувачі можуть наражати свої компанії на небезпеку, кібератака вважається лише тоді, коли користувач навмисно використовує свої права для здійснення зловмисної діяльності. Співробітник, який недбало зберігає конфіденційну інформацію на незахищеному диску, не вчиняє кібератаку, але незадоволений працівник, який свідомо робить копії конфіденційних даних для особистої вигоди.

На що спрямовані кібератаки?

Зловмисники зазвичай проникають у комп’ютерні мережі, тому що шукають щось конкретне. Загальні цілі включають:

Кошти;

Фінансові дані підприємств;

Списки клієнтів;

Дані клієнта, включно з ідентифікаційною інформацією або іншими конфіденційними персональними даними;

Адреси електронної пошти та облікові дані для входу;

Інтелектуальна власність, як-от комерційна таємниця або дизайн продукту;

У деяких випадках кібератаки взагалі не хочуть нічого красти.

Швидше, вони просто хочуть порушити роботу інформаційних систем чи IT-інфраструктури, щоб завдати шкоди бізнесу, державній установі чи іншій цілі.

Які поширені типи кібератак?

Кіберзлочинці використовують багато складних інструментів і методів для здійснення кібератак на корпоративні IT-системи, персональні комп’ютери та інші цілі. Деякі з найпоширеніших типів кібератак включають:

Шкідливе програмне забезпечення

Зловмисне програмне забезпечення – це зловмисне програмне забезпечення, яке може призвести до непрацездатності заражених систем. Зловмисне програмне забезпечення може знищити дані, викрасти інформацію або навіть видалити файли, критичні для роботи операційної системи. Зловмисне програмне забезпечення існує в багатьох формах, зокрема:

Троянські коні маскуються під корисні програми або ховаються в законному програмному забезпеченні, щоб обманом змусити користувачів встановити їх. Троян віддаленого доступу (RAT) створює секретний бекдор на пристрої жертви, тоді як троян-дропер встановлює додаткове зловмисне програмне забезпечення, коли має точку опори.

Програми-вимагачі — це складні шкідливі програми, які використовують надійне шифрування, щоб утримувати дані або системи в заручниках. Потім кіберзлочинці вимагають оплату в обмін на звільнення системи та відновлення

функціональності. Згідно з індексом аналізу загроз X-Force IBM, програмне забезпечення-вимагач є другим за поширеністю типом кібератак, на нього припадає 17% атак.

Scareware використовує фальшиві повідомлення, щоб залякати жертв і змусити їх завантажити зловмисне програмне забезпечення або передати конфіденційну інформацію шахраям.

Шпигунське програмне забезпечення – це тип зловмисного програмного забезпечення, яке таємно збирає конфіденційну інформацію, як-от імена користувачів, паролі та номери кредитних карток. Потім він надсилає цю інформацію назад хакеру.

Руткіти — це пакети зловмисних програм, які дозволяють хакерам отримати доступ на рівні адміністратора до операційної системи комп'ютера чи інших ресурсів.

Хробаки — це шкідливий код, що самовідтворюється, який може автоматично поширюватися між програмами та пристроями.

Соціальна інженерія

Атаки соціальної інженерії спонукають людей робити те, чого вони не повинні робити, наприклад ділитися інформацією, якою вони не повинні ділитися, завантажувати програмне забезпечення, яке вони не повинні завантажувати, або надсилати гроші злочинцям.

Фішинг є однією з найпоширеніших атак соціальної інженерії. Відповідно до звіту Cost of a Data Breach, це друга за поширеністю причина порушень. Найпростіші фішингові шахрайства використовують фальшиві електронні листи або текстові повідомлення для викрадення облікових даних користувачів, викрадання конфіденційних даних або поширення зловмисного програмного забезпечення. Фішингові повідомлення часто створюються так, ніби вони надходять із законного джерела. Зазвичай вони спрямовують жертву натиснути гіперпосилання, яке переведе її на шкідливий веб-сайт, або відкрити вкладення електронної пошти, яке виявляється шкідливим програмним забезпеченням.

Кіберзлочинці також розробили більш витончені методи фішингу. Фішинг — це цілеспрямована атака, спрямована на маніпулювання конкретною особою, часто з

використанням деталей із загальнодоступних профілів жертви в соціальних мережах, щоб зробити обман більш переконливим. Китовий фішинг – це тип стрімкого фішингу, спрямований спеціально на високопоставлених керівників компаній. У шахрайстві з компрометацією бізнес-електронної пошти (BEC) кіберзлочинці видають себе за керівників, продавців або інших ділових партнерів, щоб обманом змусити жертв перевести гроші або надати конфіденційні дані.

Атаки типу «відмова в обслуговуванні».

Атаки типу «відмова в обслуговуванні» (DoS) і розподілена «відмова в обслуговуванні» (DDoS) переповнюють ресурси системи шахрайським трафіком. Цей трафік перевантажує систему, перешкоджаючи відповідям на законні запити та знижуючи здатність системи працювати. Атака типу «відмова в обслуговуванні» може бути самоціллю або підготовкою до іншої атаки [2].

Різниця між DoS-атаками та DDoS-атаками полягає просто в тому, що DoS-атаки використовують одне джерело для створення шахрайського трафіку, тоді як DDoS-атаки використовують кілька джерел. DDoS-атаки часто здійснюються за допомогою ботнету, мережі підключених до Інтернету заражених шкідливим програмним забезпеченням пристроїв під контролем хакера. Ботнети можуть включати ноутбуки, смартфони та пристрої Інтернету речей (IoT). Жертви часто не знають, коли ботнет захопив їхні пристрої.

Атака типу Man-in-the-middle

Під час атаки "людина посередині" (MiTM), яка також називається "атакою підслуховування", хакер таємно перехоплює зв'язок між двома людьми або між користувачем і сервером. Атаки MitM зазвичай здійснюються через незахищені публічні мережі Wi-Fi, де зловмисникам відносно легко шпигувати за трафіком.

Хакери можуть читати електронні листи користувача або навіть таємно змінювати електронні листи до того, як вони дійдуть до одержувача. Під час атаки з захопленням сеансу хакер перериває з’єднання між користувачем і сервером, на якому розміщені важливі активи, як-от конфіденційна база даних компанії. Хакер змінює свою IP-адресу на адресу користувача, змушуючи сервер думати, що це

законний користувач, який увійшов у законний сеанс. Це дає хакеру повну свободу для крадіжки даних або іншим чином сіяти хаос.

1.2 Аналіз вразливостей, які можуть призвести до порушення ІБ

Аналіз вразливостей є важливим кроком в забезпеченні інформаційної безпеки підприємств. Він допомагає виявити потенційні слабкі місця в системі та ідентифікувати можливі загрози. Ось деякі типові вразливості, які можуть призвести до порушення інформаційної безпеки [3]:

Слабкі паролі: Використання простих або легко вгадуваних паролів зробить систему легким здобутком для зловмисників. Також, використання одного й того ж пароля для кількох облікових записів може збільшити ризик.

Відсутність оновлень: Не оновлене або застаріле програмне забезпечення може містити вразливості, які можуть бути використані зловмисниками для вторгнення в систему.

Недостатня захищеність мережі: Недостатня конфігурація мережевих пристроїв, відкриті порти, незахищені Wi-Fi мережі або недостатня шифрування даних можуть зробити мережу легко доступною для несанкціонованого доступу.

Недостатній контроль доступу: Несправні або неправильно налаштовані механізми контролю доступу можуть дозволити несанкціонованим особам отримати доступ до конфіденційної інформації або системних ресурсів.

Недостатня свідомість персоналу: Відсутність належної навченості та усвідомленості про кібербезпеку серед працівників може призвести до виконання небезпечних дій, таких як небезпечні посилання, відкриття недовіреного вкладення електронної пошти або виток конфіденційної інформації.

Недостатнє резервне копіювання даних: Відсутність регулярного резервного копіювання даних може призвести до втрати даних в разі системного збою, атаки або природного лиха.

Використання старих або ненадійних засобів зберігання даних: Застосування застарілих або ненадійних методів зберігання даних, таких як фізичні носії, може призвести до непередбачуваних втрат даних або несанкціонованого доступу.

1.3 Опис наслідків порушення інформаційної безпеки для мб

Порушення інформаційної безпеки для малого бізнесу можуть мати серйозні наслідки, які можуть негативно вплинути на фінанси, репутацію та продуктивність компанії. Ось деякі з найпоширеніших наслідків порушення інформаційної безпеки:

Втрата конфіденційності даних: Компанії можуть втратити конфіденційну інформацію, включаючи клієнтські дані, фінансові дані, виробничі секрети та іншу конкурентну інформацію. Це може призвести до порушення довіри клієнтів, втрати бізнесу та правових наслідків [4-5].

Фінансові збитки: Кібератаки можуть призвести до фінансових збитків, які включають втрату коштів, штрафи за порушення регуляторних вимог, відшкодування пошкодженим клієнтам, витрати на відновлення та втрату доходу внаслідок припинення роботи бізнесу.

Втрата репутації: Коли підприємство стає жертвою кібератаки, це може суттєво підірвати його репутацію. Новини про порушення безпеки можуть поширюватися швидко, що призводить до втрати довіри клієнтів, партнерів та інвесторів. Це може мати довготривалі наслідки і вплинути на прибутковість бізнесу.

Втрата доступу до систем: Кібератаки, такі як розповсюдження вірусів, шифрування даних або DoS-атаки, можуть спричинити припинення роботи комп'ютерних систем та мережі. Це може призвести до зупинки бізнес-процесів, втрати продуктивності та недоступності послуг для клієнтів.

Порушення вимог регуляторів: Багато галузей мають регуляторні вимоги щодо захисту конфіденційної інформації, зокрема в сферах фінансів, охорони здоров'я та захисту персональних даних. Порушення цих вимог може призвести до штрафів, правових позовів та інших наслідків, які можуть серйозно пошкодити бізнес.

Втрата довіри клієнтів: Якщо підприємство не може забезпечити безпеку даних своїх клієнтів, це може призвести до втрати довіри. Клієнти можуть перестати використовувати послуги компанії і шукати інших постачальників, які забезпечують більшу безпеку.

Недоступність бізнесу: Кібератаки можуть спричинити недоступність бізнесу на протязі тривалого часу. Це може призвести до втрати доходу, незадоволеності клієнтів та проблем зі відновленням нормального функціонування.

Враховуючи ці наслідки, важливо для малих підприємств приділити належну увагу заходам безпеки і вжити відповідні заходи для запобігання кібератакам та забезпечення інформаційної безпеки своєї організації.

Висновок до першого розділу

У даному розділу було проведено огляд різних загроз, з якими стикаються підприємства малого бізнесу в сфері інформаційної безпеки. Було виявлено, що такі підприємства часто стають об'єктом атак з боку кіберзлочинців, оскільки вони можуть мати менші ресурси для захисту та меншу свідомість про безпеку. Загрози включають в себе кібератаки, шкідливі програми, фішингові атаки та соціальну інженерію. Було було проаналізовано різні вразливості, які можуть призвести до порушення інформаційної безпеки в малих бізнесах. Було виявлено, що недостатні заходи безпеки, недостатня оновлення та патчі, слабкі паролі, недостатнє резервне копіювання даних, недостатній контроль доступу та фізична безпека можуть стати джерелом вразливостей. Також було описано різні наслідки порушення інформаційної безпеки для малого бізнесу. Ці наслідки включають фінансові втрати, втрату клієнтів та репутації, втрату конфіденційної інформації. Порушення інформаційної безпеки може суттєво негативно вплинути на функціонування та розвиток малого бізнесу.

Отже, підприємства малого бізнесу повинні бути усвідомлені про загрози, з якими вони стикаються, а також про вразливості своєї інформаційної інфраструктури. Необхідно приділити належну увагу впровадженню ефективних заходів безпеки,

таких як резервне копіювання даних, захист від кібератак, контроль доступу та моніторинг системи. Тільки таким чином підприємства малого бізнесу зможуть запобігти порушенню інформаційної безпеки і зберегти свою ділову діяльність в безпеці.

РОЗДІЛ 2
АНАЛІЗ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Антивірусні програми та антишпигунські засоби

Антивірусні програми та антишпигунське програмне забезпечення відіграють вирішальну роль у забезпеченні інформаційної безпеки малого бізнесу. Ось огляд цих інструментів та їх важливості:

Антивірусні програми: антивірусне програмне забезпечення призначене для виявлення, запобігання та видалення зловмисного програмного забезпечення, наприклад вірусів, хробаків, троянів і програм-вимагачів, з комп'ютерів і мереж. Ці програми використовують базу даних сигнатур відомих зловмисних програм і методи поведінкового аналізу для виявлення та розміщення на карантині або видалення загроз. Антивірусні програми слід регулярно оновлювати, щоб залишатися ефективними проти останніх загроз [8].

Серед переваг антивірусних програм для малого бізнесу:

Захист від зловмисного програмного забезпечення: антивірусні програми допомагають запобігти зараженню зловмисним програмним забезпеченням, яке може призвести до витоку даних, збоїв системи та несанкціонованого доступу до конфіденційної інформації.

Сканування в режимі реального часу: антивірусне програмне забезпечення постійно відстежує файли, завантаження, вкладення електронної пошти та веб-сайти для виявлення та блокування потенційних загроз у режимі реального часу.

Безпечний перегляд веб-сторінок: багато антивірусних програм містять функції веб-захисту, які блокують доступ до шкідливих веб-сайтів і попереджають користувачів про потенційно небезпечні посилання.

Безпека електронної пошти: антивірусне програмне забезпечення сканує вхідні та вихідні вкладення електронної пошти на наявність шкідливих програм, запобігаючи поширенню заражених файлів.

Найкраще антивірусне програмне забезпечення 2023 року згідно Forbes

1. **Avira:** найкраще співвідношення ціни і якості
2. **McAfee:** найкраще для комплексних функцій
3. **Avast:** найкраще для індивідуальних підприємців і віддалених працівників
4. **Bitdefender**: найкраще для профілактики
5. **Emsisoft:** найкраще для високотехнологічного захисту
6. **F-Secure**: найкраще для налаштування
7. **Malwarebytes**: найкраще для захисту в реальному часі
8. **Norton Antivirus**: найкраще для малого бізнесу

Антишпигунське програмне забезпечення: шпигунське програмне забезпечення відноситься до програмного забезпечення, яке таємно збирає інформацію користувача без його відома чи згоди. Він може відстежувати дії в Інтернеті, фіксувати натискання клавіш, викрадати конфіденційні дані та порушувати конфіденційність. Антишпигунське програмне забезпечення розроблено спеціально для виявлення та видалення шпигунського програмного забезпечення з систем.

Серед переваг антишпигунського програмного забезпечення для малого бізнесу:

Захист від крадіжки даних: засоби захисту від шпигунського програмного забезпечення допомагають запобігти несанкціонованому доступу до конфіденційної інформації про бізнес і клієнтів, захищаючи від крадіжки особистих даних і фінансових втрат.

Захист конфіденційності: виявляючи та видаляючи шпигунське програмне забезпечення, ці програми захищають конфіденційність співробітників і клієнтів, запобігаючи несанкціонованому відстеженню та контролю.

Оптимізація продуктивності системи: шпигунське програмне забезпечення може значно уповільнити роботу системи. Антишпигунське програмне забезпечення допомагає виявляти та видаляти ресурсомістке шпигунське програмне забезпечення, підвищуючи загальну продуктивність системи [10].

Найкраще антишпигунське програмне забезпечення 2023 року згідно WizCase

Norton 360 – комплексний антивірусний план із захистом від шпигунських програм, який виявив 100% шкідливих програм і пропонує 60-денну гарантію повернення грошей!

TotalAV – захист від шпигунських програм оновлюється щодня, щоб забезпечити надійний захист, але ціна значно зростає після першого року використання.

McAfee – надійні додаткові функції для боротьби з атаками шпигунських програм, але деякі з його кращих функцій доступні тільки клієнтам зі США.

Bitdefender – багато інструментів для захисту від шпигунських програм, які особливо підійдуть для захисту фінансової інформації, але деякі основні функції доступні тільки користувачам ОС Windows.

Intego – Система запобігання загрозам виявляє новітнє шкідливе ПЗ на ПК і Mac

Щоб забезпечити ефективність антивірусного та антишпигунського програмного забезпечення, малим підприємствам слід дотримуватись таких найкращих практик:

1. Регулярні оновлення: оновлюйте антивірусні та антишпигунські програми за допомогою останніх визначень вірусів і виправлень безпеки, щоб залишатися захищеним від нових загроз.

2. Регулярне сканування: заплануйте регулярне сканування системи, щоб виявити та видалити будь-яке зловмисне або шпигунське програмне забезпечення, яке могло уникнути захисту в режимі реального часу.

3. Звички безпечного перегляду: навчіть співробітників правилам безпечного перегляду в Інтернеті, наприклад, уникайте підозрілих веб-сайтів, не натискайте невідомі посилання чи вкладені файли та обережно ставтеся до спроб фішингу.

4. Безпечні джерела програмного забезпечення: завантажуйте програмне забезпечення та оновлення лише з надійних джерел, щоб мінімізувати ризик завантаження заражених файлів.

5. Поінформованість співробітників: навчіть співробітників розпізнавати будь-які підозрілі дії, електронні листи або програмне забезпечення, які можуть вказувати на загрозу безпеці, і повідомляти про них.

Впровадження надійних засобів захисту від вірусів і шпигунського програмного забезпечення має важливе значення для малого бізнесу, щоб захистити свої цінні дані, підтримувати безперервність роботи та зберегти довіру клієнтів.

2.2 Файрволи та системи виявлення вторгнення

Брандмауери та системи виявлення вторгнень (IDS) є критично важливими компонентами інфраструктури кібербезпеки організації. Давайте дослідимо їхню роль і важливість у захисті малого бізнесу.

Брандмауер - це пристрій, який розташовується між внутрішньою мережею організації та кінцевою мережею з безкоштовною передачею пакетів і фільтрацією даних. Він дозволяє контролювати і пересилати певні пакети, а також блокувати інші. Наприклад, брандмауер може фільтрувати вхідні пакети, які призначені для конкретного хосту або сервера, такого як HTTP, або використовуватися для обмеження доступу до певного хосту або сервісу в організації [11].

На (Рисунку 2.1) показано встановлення брандмауера в мережі. Основні функції та переваги брандмауерів включають:

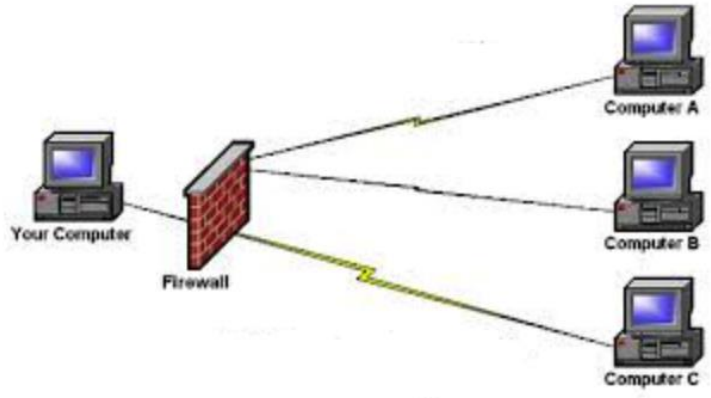

Рисунок 2.1 - Встановлення брандмауера в мережі

Firewall відстежує і блокує всі потенційно небезпечні підключення, тим самим ефективно захищаючи особисті дані користувача. Але не варто плутати брандмауер з антивірусними програмами, які призначені для боротьби з погрозами, вже розташованими на комп'ютері або на знімних носіях. Проти мережевих атак антивіруси безсилі. А що таке брандмауер і чим він займається? Він не стежить за тим, які дії виконуються на самому комп'ютері (зрозуміло, якщо не передається інформація в мережу). Головним завданням брандмауера є спостереження саме за мережевим трафіком. Тільки спільне використання антивіруса і firewall може гарантувати повну безпеку комп'ютера.

Робоча архітектура

Брандмауер часто встановлюється далеко від решти мережі, щоб жодні вхідні запити не потрапляли безпосередньо до ресурсу приватної мережі. Якщо брандмауер налаштовано належним чином, системи з одного боку брандмауера захищені від систем з іншого боку. Брандмауери зазвичай фільтрують трафік на основі двох методологій:

- Брандмауер може дозволити будь-який трафік, крім того, що вказано як обмежений. Він залежить від типу використовуваного брандмауера, джерела, адрес призначення та портів
- Брандмауер може заборонити будь-який трафік, який не відповідає конкретним критеріям на основі мережевого рівня, на якому працює брандмауер

Тип критеріїв, які використовуються для визначення того, чи слід пропускати трафік, залежить від одного типу до іншого. Брандмауер може залежати від типу трафіку або адрес і портів джерела чи призначення. Брандмауер також може використовувати складні правила, засновані на аналізі даних програми, щоб визначити, чи слід пропускати трафік.

Плюси і мінуси брандмауера

Кожен пристрій безпеки має переваги та недоліки, і брандмауери нічим не відрізняються. Якби ми застосували суворі захисні механізми в нашій мережі, щоб захистити її від злому, тоді навіть наш законний зв'язок міг би працювати з ладу; або якщо ми дозволимо комунікації всього протоколу в нашій мережі, то її можуть легко

зламати зловмисники. Ми повинні підтримувати баланс між суворо пов’язаними та слабко пов’язаними функціями.

Плюси

- Брандмауер - це механізм виявлення вторгнень. Брандмауери є специфічними для політики безпеки організації. Параметри брандмауера можна змінити, щоб внести відповідні зміни до функціональності брандмауера.
- Брандмауери можна налаштувати так, щоб блокувати вхідний трафік за протоколами POP і SNMP і дозволяти доступ до електронної пошти.
- Брандмауери також можуть блокувати служби електронної пошти для захисту від спаму.
- Брандмауери можна використовувати для обмеження доступу до певних служб. Наприклад, брандмауер може надати публічний доступ до веб-сервера, але заборонити доступ до Telnet та інших непублічних доменів.
- Брандмауер перевіряє вхідний і вихідний трафік на відповідність правилам брандмауера. Він діє як маршрутизатор для переміщення даних між мережами.
- Брандмауери - чудові аудитори. Завдяки широким можливостям дискового або дистанційного журналювання вони можуть реєструвати будь-який трафік, який проходить.

Мінуси

- Брандмауер не може запобігти розкриттю конфіденційної інформації за допомогою соціальної інженерії.
- Брандмауер не може захистити від того, що було авторизовано. Брандмауери дозволяють звичайний зв’язок між затвердженими програмами, але якщо самі ці програми мають недоліки, брандмауер не зупинить атаку: для брандмауера зв’язок авторизований.
- Брандмауери настільки ефективні, наскільки ефективні правила, на які вони налаштовані.
- Брандмауери не можуть зупинити атаки, якщо через них не проходить трафік.
- Брандмауери також не можуть захистити від спроб тунелювання. Захищені програми можуть бути атаковані за допомогою троянських програм. Тунелювання

поганих речей через HTTP, SMTP та інші протоколи досить просте та легко продемонстроване.

Системи виявлення вторгнень (IDS): IDS — це інструмент безпеки, розроблений для моніторингу мережевого трафіку та виявлення потенційних порушень безпеки або зловмисної діяльності. Він аналізує мережеві пакети, системні журнали та інші джерела інформації, щоб виявити шаблони та сигнатури, пов’язані з відомими атаками чи аномаліями (Рисунок 2.2).

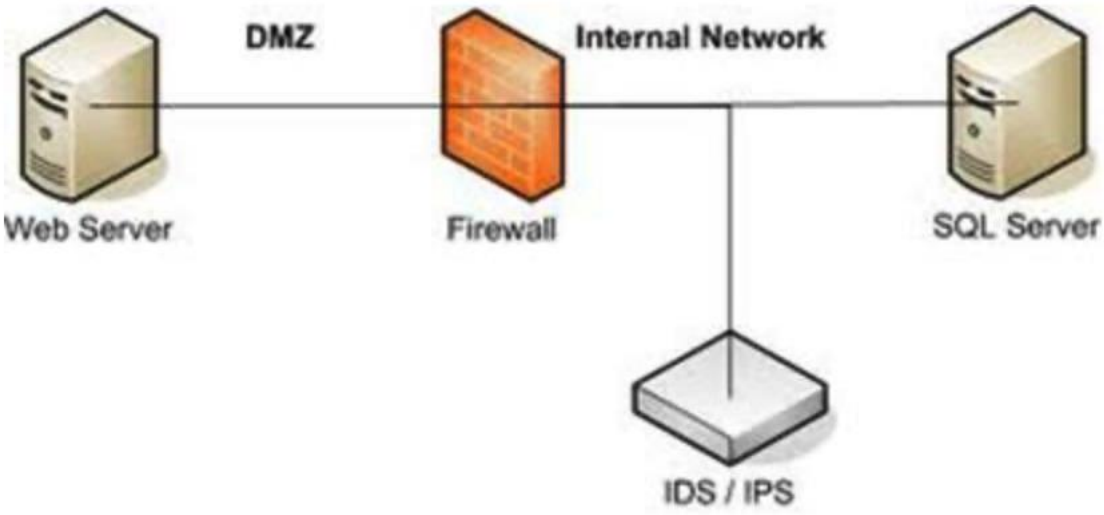

Рисунок 2.2 - Система виявлення вторгнень (IDS)

Система виявлення вторгнень (IDS) є ще одним інструментом в арсеналі комп’ютерної безпеки адміністратора мережі. Він перевіряє всю вхідну та вихідну мережеву активність. IDS визначає будь-який підозрілий шаблон, який може свідчити про атаку на систему, і діє як перевірка безпеки для всіх транзакцій, які відбуваються в системі та з неї [14].

Виділяють чотири основні типи IDS

NIDS (Network Intrusion Detection System) - це незалежна платформа, яка використовується для виявлення вторгнень шляхом моніторингу мережевого трафіку та відстеження кількох хостів. Системи виявлення мережевих входів забезпечують доступ до мережевого трафіку шляхом підключення до мережевого концентратора,

комутатора, який налаштований на віддзеркалення портів, або мережевого крана. Датчики NIDS розташовуються в стратегічних точках мережі для моніторингу, часто в демілітаризованій зоні (DMZ) або на межі мережі. Ці датчики записують весь мережевий трафік та аналізують вміст окремих пакетів для виявлення виявлено шкідливого трафіку. Прикладом NIDS є Snort.

HIDS (Host-based Intrusion Detection System) - це система виявлення вторгнень, яка заснована на хості (індивідуальному комп'ютері або сервері). HIDS складається з агента, який встановлюється на хості та використовується для ідентифікації входу. Він аналізує системні виклики, програми журналів, зміни у файлі системи (включаючи двійкові файли, файли з паролями, бази даних прав доступу та інше) та інші дії та стан хоста для виявлення виявлених загроз. Датчики HIDS фактично представляють собою програмний агент, а деякі IDS на основі програми належать до цієї категорії. Прикладом HIDS є OSSEC.

Системи виявлення вторгнень також можуть використовувати спеціальні інструменти та приманки, або залежати від фізичної безпеки будівлі, щоб виявити несанкціоноване проникнення. У випадку фізичної безпеки будівлі IDS відбувається як система сигналу

Система виявлення вторгнень по периметру (PIDS)

Виявляє та точно визначає місце спроб вторгнення на периметрі критичної інфраструктури. Використовуючи або електроніку, або більш просунуту волоконно-оптичну кабельну технологію, встановлену на огорожі по периметру, PIDS виявляє перешкоди на огорожі. Якщо вторгнення виявлено та розцінено системою як спробу вторгнення, спрацьовує тривога.

Система виявлення вторгнень на основі віртуальної машини (VMIDS)

VMIDS виявляє вторгнення за допомогою моніторингу віртуальної машини. Використовуючи це, ми можемо розгорнути систему виявлення вторгнень із моніторингом віртуальної машини. Це найновіший тип, і він все ще знаходиться в стадії розробки. Немає потреби в окремій системі виявлення вторгнень, оскільки використовуючи її, ми можемо контролювати загальну діяльність.

2.3 Криптографічні засоби та шифрування даних

Криптографічні засоби та шифрування даних є важливими компонентами інформаційної безпеки для малого бізнесу. Вони забезпечують механізми захисту конфіденційних даних від несанкціонованого доступу та забезпечують їх конфіденційність і цілісність. Давайте дослідимо важливість і переваги криптографічних інструментів і шифрування даних [16]:

Криптографічні інструменти:

Алгоритми шифрування. Криптографічні інструменти використовують алгоритми шифрування для перетворення даних у формат, який неможливо прочитати, відомий як зашифрований текст. Лише уповноважені сторони з відповідним ключем дешифрування можуть розшифрувати зашифрований текст і отримати вихідні дані.

Хеш-функції: криптографічні хеш-функції генерують унікальне хеш-значення фіксованого розміру або дайджест для певного введення. Хеш-функції використовуються для перевірки цілісності даних, гарантуючи, що дані не були підроблені.

Цифрові підписи: цифрові підписи забезпечують спосіб перевірки автентичності та цілісності цифрових документів або повідомлень. Вони використовують криптографію з асиметричним ключем, щоб прив’язати цифровий підпис до вмісту, дозволяючи одержувачам перевіряти особу відправника та виявляти будь-які зміни в даних.

Шифрування даних:

Конфіденційність: шифрування гарантує, що конфіденційні дані залишаються конфіденційними, навіть якщо їх перехоплюють або до них мають доступ неавторизовані особи. Зашифровані дані марні без відповідного ключа дешифрування.

Відповідність: багато нормативних положень вимагають захисту конфіденційних даних за допомогою шифрування. Впровадження заходів

шифрування може допомогти малим підприємствам відповідати вимогам і уникнути можливих штрафів.

Безпечне зберігання даних: шифрування даних перед їх збереженням на пристроях, серверах або хмарних платформах додає додатковий рівень безпеки. У разі порушення даних або несанкціонованого доступу зашифровані дані залишаються захищеними.

Безпечний зв’язок: шифрування даних під час передачі (наприклад, за допомогою таких протоколів, як SSL/TLS) гарантує, що дані, якими обмінюються між системами або через мережі, є безпечними та не можуть бути перехоплені чи змінені.

Керування ключами:

Генерація та зберігання ключів. Криптографічні інструменти покладаються на ключі шифрування для шифрування та дешифрування даних. Правильна генерація ключів і безпечне зберігання є важливими для запобігання несанкціонованому доступу до конфіденційних даних.

Ротація ключів: регулярна зміна ключів шифрування зменшує ризик компрометації ключа та підвищує безпеку. Ротацію ключів слід здійснювати відповідно до найкращих практик і в координації з процесами шифрування даних.

Розповсюдження ключів. Безпечне розповсюдження ключів шифрування авторизованим сторонам має вирішальне значення для безпечного зв’язку та обміну даними. Для забезпечення конфіденційності та цілісності під час розповсюдження ключів необхідно впроваджувати безпечні протоколи обміну ключами.

Під час впровадження криптографічних інструментів і шифрування даних малим підприємствам слід враховувати наступне [17]:

Визначте конфіденційні дані: визначте типи даних, які потребують шифрування, як-от особиста інформація (PII), фінансові записи, інтелектуальна власність і дані клієнтів.

Алгоритми та міцність шифрування: виберіть відповідні алгоритми шифрування та довжину ключа на основі найкращих галузевих практик і нормативних вимог.

Безпечне керування ключами: установіть безпечні процедури для створення, зберігання, ротації та розповсюдження ключів. За потреби використовуйте безпечні механізми зберігання ключів, такі як апаратні модулі безпеки (HSM).

Шифрування протягом усього життєвого циклу даних: застосовуйте шифрування не лише під час передачі даних, але й у стані спокою (у сховищі) і під час обробки.

Контроль доступу користувачів: реалізуйте надійні механізми автентифікації користувачів і засоби контролю доступу, щоб гарантувати доступ до зашифрованих даних лише авторизованим особам.

Регулярні перевірки безпеки. Проводьте періодичні перевірки безпеки та оцінки вразливостей, щоб виявити та усунути будь-які недоліки в криптографічних реалізаціях.

Використовуючи криптографічні інструменти та шифрування даних, малі підприємства можуть зменшити ризик несанкціонованого доступу до даних, підтримувати довіру клієнтів, дотримуватися нормативних актів і захищати свою конфіденційну інформацію протягом усього життєвого циклу.

2.4 Засоби аутентифікації та контролю доступу

Автентифікація та контроль доступу є критично важливими компонентами інформаційної безпеки для малого бізнесу. Вони допомагають забезпечити доступ до конфіденційних даних, систем і ресурсів лише авторизованим особам. Давайте розглянемо деякі поширені засоби автентифікації та контролю доступу:

Автентифікація на основі пароля:

Імена користувачів і паролі: це найпоширеніша форма автентифікації. Користувачі вводять унікальну комбінацію імені користувача та пароля для доступу до систем або програм. Важливо дотримуватися надійної політики паролів (наприклад, мінімальна довжина, вимоги до складності) і заохочувати регулярне оновлення паролів [18].

Багатофакторна автентифікація (MFA): MFA додає додатковий рівень безпеки, вимагаючи від користувачів надавати додаткові облікові дані, наприклад одноразовий пароль (OTP), біометричні дані (відбиток пальця або розпізнавання обличчя) або фізичний маркер. MFA значно підвищує безпеку, вимагаючи кількох факторів для автентифікації.

Біометрична автентифікація:

Розпізнавання відбитків пальців: користувачі автентифікуються, надаючи свій унікальний відбиток пальця, який порівнюється із зареєстрованими відбитками пальців для перевірки.

Розпізнавання обличчя: риси обличчя скануються та порівнюються зі збереженими шаблонами, щоб підтвердити особу користувача.

Сканування райдужної оболонки або сітківки ока: ці методи використовують унікальні візерунки райдужної оболонки або сітківки ока для автентифікації користувачів.

Розпізнавання голосу: голоси користувачів аналізуються та порівнюються з їхніми зареєстрованими голосовими шаблонами для автентифікації.

Смарт-карти та токени:

Смарт-карти: ці картки містять вбудовані мікрочіпи, які зберігають облікові дані користувача. Користувачі пред’являють картку зчитувальному пристрою, який аутентифікує картку та надає доступ.

USB-токени: пристрої на базі USB, які зберігають облікові дані для автентифікації та вимагають від користувачів вставити маркер у USB-порт для автентифікації.

Контроль доступу на основі ролей (RBAC):

RBAC призначає дозволи та права доступу користувачам на основі їхніх ролей в організації. Це спрощує керування доступом, групуючи користувачів у ролі та надаючи їм дозволи. Такий підхід зменшує складність керування правами доступу окремих користувачів.

Списки контролю доступу (ACL):

ACL — це списки дозволів, пов’язаних із певними ресурсами, такими як файли, папки або мережеві пристрої. Вони визначають, які користувачі або групи мають дозвіл на виконання певних дій або доступ до певних ресурсів.

Керування привілейованим доступом (PAM):

PAM зосереджується на управлінні та захисті привілейованих облікових записів, які мають підвищені права доступу. Рішення PAM забезпечують більш суворий контроль, такий як моніторинг сеансів, обмежений за часом доступ і робочі процеси затвердження, щоб зменшити ризики, пов’язані з привілейованими обліковими записами [19].

Єдиний вхід (SSO):

SSO дозволяє користувачам пройти автентифікацію один раз і отримати доступ до кількох систем або програм без повторного введення облікових даних. Це спрощує процес автентифікації та зменшує потребу користувачів запам’ятовувати декілька паролів.

Журнали аудиту та моніторинг:

Реєстрація та моніторинг дій користувачів забезпечують видимість спроб доступу, помилок автентифікації та підозрілої поведінки. Це допомагає виявляти та досліджувати потенційні інциденти безпеки або спроби несанкціонованого доступу.

Впроваджуючи заходи автентифікації та контролю доступу, малим підприємствам слід враховувати такі найкращі практики:

Реалізуйте принцип найменших привілеїв, надаючи користувачам лише дозволи, необхідні для виконання їхніх робочих функцій.

Регулярно переглядайте та оновлюйте права доступу користувачів, щоб переконатися, що вони відповідають ролям і обов’язкам співробітників.

Розкажіть користувачам про важливість надійних паролів, гігієни паролів і ризики, пов’язані з розголошенням або повторним використанням паролів.

Увімкніть блокування облікових записів і запровадьте політику блокування облікових записів для захисту від атак грубої сили.

Регулярно відстежуйте та переглядайте журнали аудиту та події безпеки, щоб виявити аномалії або потенційні порушення безпеки.

Застосуйте захищені протоколи для віддаленого доступу, такі як віртуальні приватні мережі (VPN), щоб захистити дані під час передачі.

Регулярно виправляйте та оновлюйте системи та програми для усунення вразливостей, які можуть бути використані для несанкціонованого доступу.

2.5 Безпека мереж та віртуальних приватних мереж (vpn)

Безпека мереж, особливо коли йдеться про малий бізнес, має вирішальне значення для захисту конфіденційних даних, збереження конфіденційності та запобігання несанкціонованому доступу. Віртуальні приватні мережі (VPN) зазвичай використовуються для підвищення безпеки мережі. Давайте розглянемо аспекти безпеки мереж і VPN:

Безпека мереж:

Сегментація мережі: впровадження сегментації мережі допомагає розділити мережу на окремі сегменти, такі як VLAN або підмережі, для контролю доступу та запобігання можливим порушенням. Він запобігає бічному переміщенню, обмежуючи вплив інциденту безпеки на певний сегмент мережі [21].

Захищена мережева архітектура: розробка захищеної мережевої архітектури передбачає розміщення міжмережевих екранів, систем виявлення вторгнень та інших пристроїв безпеки для моніторингу та контролю мережевого трафіку. Впровадження захищених протоколів і технологій, таких як Secure Sockets Layer (SSL) і Transport Layer Security (TLS), забезпечує зашифрований зв’язок між компонентами мережі.

Контроль доступу: Реалізація надійних механізмів контролю доступу є важливою. Це включає застосування надійних методів автентифікації, таких як комбінації імені користувача та пароля або багатофакторна автентифікація, для перевірки особи користувачів перед наданням доступу до мережі. Списки контролю доступу (ACL) і контроль доступу на основі ролей (RBAC) допомагають обмежити доступ авторизованому персоналу на основі їхніх ролей і обов’язків.

Моніторинг мережі: постійний моніторинг мережевого трафіку та дій дозволяє виявляти підозрілу поведінку, спроби несанкціонованого доступу або аномалії.

Системи виявлення вторгнень (IDS) і рішення для управління інформацією та подіями безпеки (SIEM) можуть допомогти в моніторингу в реальному часі та сповіщенні.

Регулярні оновлення та виправлення. Важливо, щоб мережеві пристрої, такі як маршрутизатори, комутатори та брандмауери, оновлювали останні версії програмного забезпечення та виправлення безпеки. Регулярні оновлення усувають відомі вразливості та підвищують безпеку мережі.

Безпека віртуальних приватних мереж (VPN)

Віртуальна приватна мережа (VPN) — це безпечне та приватне мережеве з'єднання, встановлене через загальнодоступний Інтернет або будь-яку іншу незахищену мережу. VPN використовують шифрування, щоб захистити конфіденційні дані від несанкціонованого доступу та забезпечити безпечне з'єднання, навіть через Інтернет. Технологія VPN дозволяє віддаленим користувачам або філіям підключатися до приватної мережі так, ніби вони фізично підключені, створюючи віртуальне мережеве розширення, звідси й назва Віртуальна приватна мережа. Основними перевагами VPN є підвищена конфіденційність і безпека, а також доступ до ресурсів, які можуть бути обмежені або заблоковані в місці розташування користувача (Рисунок 2.3).

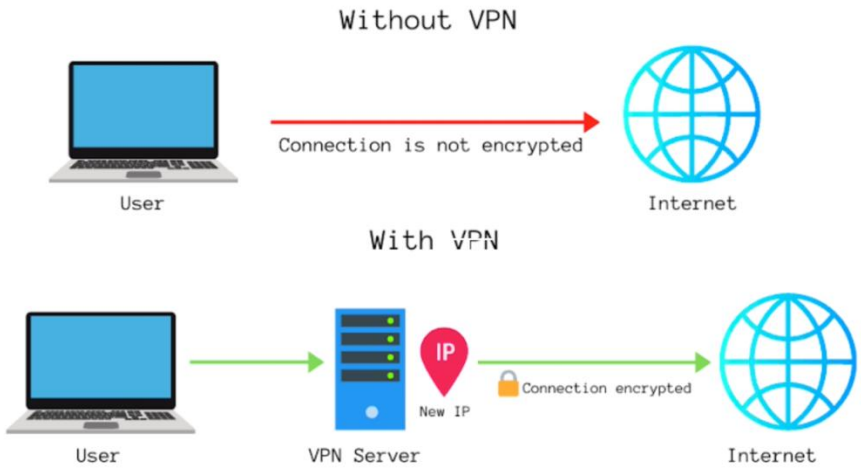

Рисунок 2.3 - Віртуальна приватна мережа (VPN)

Шифрування мережі VPN використовують протоколи шифрування, такі як IPsec (Internet Protocol Security) або SSL/TLS, для шифрування даних, що передаються

через мережу. Це гарантує, що конфіденційна інформація залишається захищеною та недоступною для неавторизованих осіб.

Тунелювання мережі VPN створюють безпечні тунелі між кінцевими точками, інкапсулюючи та захищаючи дані під час передачі. Це запобігає прослуховування та перехоплення даних.

Автентифікація та контроль доступу VPN потребують автентифікації користувача для встановлення з'єднання. Для доступу до VPN користувачі повинні надати дійсні облікові дані, як від імена користувачів і паролі або цифрові сертифікати. Це гарантує, що лише авторизовані користувачі можуть підключатися до мережі.

Безпека кінцевих точок VPN. Безпека кінцевих точок VPN, таких як сервери VPN і клієнтські пристрої, є надзвичайно важливою. Правильна конфігурація, виправлення та захист кінцевих точок VPN допомагають захистити від вразливостей і потенційних атак.

Ведення журналів і аудит VPN повинні вести журнали VPN-з'єднань, включаючи дії користувачів, часові позначки та IP-адреси. Можливості реєстрації та аудиту допомагають контролювати та досліджувати будь-який підозрілий або неавторизований доступ до VPN.

Вибір постачальника VPN. При використанні стороннього постачальника VPN важливо вибрати авторитетного та надійного постачальника, який дотримується суворих правил безпеки. Перегляньте стандарти шифрування постачальника, політику обробки даних і методи конфіденційності, перш ніж вибрати послугу VPN.

Варто зазначити, що хоча VPN забезпечують безпечне підключення, інші заходи безпеки, такі як захист кінцевих точок, регулярні оцінки безпеки та навчання працівників, є важливими для комплексної безпеки мережі.

Якщо вам важлива конфіденційність, використовуйте VPN під час кожного підключення до Інтернету. Програма VPN працює у фоновому режимі на вашому пристрої, тому вона не заважатиме вам використовувати інші програми, дивитися потоковий контент і шукати інформацію в Інтернеті. І ви будете спокійні, знаючи, що ваша конфіденційність надійно захищена

Малі підприємства повинні оцінити свої вимоги до безпеки мережі, оцінити свою інфраструктуру та впровадити відповідні заходи безпеки для захисту своїх мереж і даних. Регулярний моніторинг, оновлення та дотримання найкращих практик сприяють підтримці безпечного мережевого середовища.

Висновок до другого розділу

Забезпечення інформаційної безпеки для малого бізнесу є складним завданням, яке вимагає комплексного підходу та використання різноманітних засобів. Під час аналізу різних аспектів інформаційної безпеки, таких як антивірусні програми, файрволи, криптографічні засоби, засоби аутентифікації та VPN, можна зробити наступні висновки.

Ці засоби забезпечують захист від різних загроз і вразливостей, з якими стикаються підприємства малого бізнесу. Антивірусні програми та антишпіонські засоби запобігають інфікуванню системи шкідливими програмами. Файрволи та системи виявлення вторгнень контролюють трафік і виявляють незвичайні активності. Криптографічні засоби та шифрування даних забезпечують конфіденційність та цілісність інформації. Засоби аутентифікації та контролю доступу дозволяють ідентифікувати користувачів та керувати їхнім доступом. Безпека мереж та VPN забезпечують захист мережі та безпечну передачу даних через відкриті мережі.

Використання цих засобів допомагає підвищити рівень безпеки і запобігти можливим порушенням інформаційної безпеки для малого бізнесу. Рекомендується впроваджувати комплексний підхід, враховуючи потреби та особливості кожного бізнесу, для ефективного захисту інформаційних ресурсів. Застосування цих засобів разом з правильною політикою безпеки та свідомістю співробітників є ключем до успішного забезпечення інформаційної безпеки малого бізнесу у сучасному інформаційному середовищі.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ЩОДО ВИБОРУ ТА ВПРОВАДЖЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІБ МАЛОГО БІЗНЕСУ

3.1 Фактори, що впливають на вибір засобів забезпечення інформаційної безпеки для малого бізнесу

Забезпечення інформаційної безпеки є невід'ємною частиною успішного функціонування будь-якого бізнесу, включаючи малі підприємства. У сучасному цифровому світі, де кіберзагрози стають все більш витонченими і поширеними, важливо мати належні заходи безпеки для захисту важливої інформації, даних клієнтів та бізнес-процесів. Вибір і впровадження засобів забезпечення інформаційної безпеки для малого бізнесу є складним завданням, яке вимагає обґрунтованих рішень і врахування різних факторів. Від правильної стратегії безпеки залежить успішність бізнесу, захищеність важливих даних і збереження репутації компанії.

Один з найважливіших аспектів - це розмір та потреби компанії. Малі бізнеси мають свої особливості, і їхні потреби можуть відрізнятися від великих корпорацій. Важливо зрозуміти, скільки працівників працює в компанії, який обсяг даних обробляється, і які конкретні загрози можуть впливати на бізнес. Враховуючи ці фактори, можна підібрати відповідні засоби безпеки.

Фінансові обмеження також впливають на вибір засобів безпеки. Бюджет компанії визначає доступність рішень. Важливо збалансувати вартість з можливостями і ефективністю рішень.

Аналіз потенційних загроз та вразливостей є ще одним ключовим етапом. Різні компанії можуть бути вразливі до різних типів атак, тому важливо обрати засоби безпеки, які надають захист від конкретних загроз, що можуть впливати на бізнес.

Функціональність та можливості також мають значення при виборі засобів безпеки. Різні компанії можуть мати різні вимоги щодо функцій, таких як

антивірусний захист, захист електронної пошти, фаєрволів, криптографії та інші. Важливо зрозуміти, які саме функції необхідні для ефективної захисту даних.

Репутація та надійність постачальника також впливають на вибір засобів безпеки. Важливо довіряти постачальнику та бути впевненим у якості його рішень.

Нарешті, врахування законодавчих вимог та стандартів безпеки є критичним аспектом. Різні галузі мають свої правила та вимоги до забезпечення безпеки даних. Важливо обрати засоби безпеки, які відповідають вимогам і стандартам вашої галузі.

Загалом, вибір засобів забезпечення інформаційної безпеки для малого бізнесу вимагає ретельного аналізу та оцінки. Врахування факторів, таких як розмір компанії, бюджет, потенційні загрози, функціональність, репутація постачальника та вимоги законодавства, допоможе зробити обґрунтований вибір та забезпечити ефективний рівень безпеки для вашого бізнесу

3.2 Рекомендації щодо вибору та впровадження засобів забезпечення іб малого бізнесу

У сучасному цифровому світі, де комп'ютерна та інформаційна технологія займають центральне місце в бізнес-процесах, захист інформації стає надзвичайно важливим завданням для малих бізнесів. Зростаюча кількість загроз та кібератак, а також значення конфіденційності, цілісності та доступності даних ставлять підприємства перед необхідністю вибору та впровадження ефективних засобів забезпечення інформаційної безпеки.

Цей розділ дипломної роботи присвячений розгляду рекомендацій щодо вибору та впровадження засобів забезпечення інформаційної безпеки для малого бізнесу. Він містить цінну інформацію та практичні поради, які допоможуть підприємствам зробити обґрунтований вибір та належним чином захистити свою інформацію від потенційних загроз.

1. Оцінка потреб. Почніть з ретельної оцінки потреб вашого бізнесу в інформаційній безпеці. Розгляньте, які типи даних ви обробляєте та зберігаєте, і визначте, які з них мають найвищу важливість і конфіденційність. Далі, з'ясуйте, які

загрози можуть впливати на ці дані, наприклад, віруси, шпигунське програмне забезпечення, несанкціонований доступ або атаки зламу. Нарешті, оцініть ризики, які ви готові прийняти, враховуючи можливі наслідки порушення безпеки даних для вашого бізнесу.

2. Вибір антивірусного програмного забезпечення. Вибір належного антивірусного програмного забезпечення є невід'ємною складовою ефективної інформаційної безпеки для малого бізнесу. У світі, де кіберзагрози стають все більш поширеними та складними, малі підприємства потребують надійного захисту своїх комп'ютерних систем та цінної корпоративної інформації. У (таблиці 3.1) наведено основні аспекти для вибору антивірусного програмного забезпечення:

Таблиця 3.1

Основні аспекти для вибору антивірусного програмного забезпечення

Особливості та вимоги	**Опис**
Сумісність	Переконайтеся, що антивірусне рішення сумісне з операційною системою (наприклад, Android, iOS, Windows).
Сканування в реальному часі	Постійний моніторинг діяльності, файлів та завантажень на планшеті для виявлення та запобігання загрозам від шкідливого ПЗ.
Виявлення та видалення шкідливого ПЗ	Ефективне виявлення та видалення різних видів шкідливого ПЗ, включаючи віруси, шпигунське ПЗ та програми-вимагачі.
Конфіденційність та захист даних	Функції для захисту особистої інформації, безпечного перегляду, анти-фішингу та шифрування даних.
Додаткові функції	Додаткові можливості, такі як антивикрадення, сканування програм, захист від веб-загроз та батьківський контроль.
Зручний інтерфейс	Легкий у використанні та налаштуванні інтерфейс програми для керування параметрами безпеки.

Якщо говорити про конкретні приклади, то на сьогоднішній день можна виділити топ-2 антивірусних програм для малого бізнесу - це Bitdefender (Bitdefender Small Office Security), Norton (Norton Small Business).

Функціональність:

Bitdefender Small Office Security: Забезпечує антивірусний захист, антиспам, виявлення і блокування шкідливих посилань, фаервол, захист від фішингу, шифрування файлів та резервне копіювання даних.

- Norton Small Business: Надає антивірусний захист, антиспам, захист від шкідливих посилань, фаервол, захист від фішингу та мережевий моніторинг.

Ефективність:

- Bitdefender Small Office Security: Зарекомендував себе як один з найкращих антивірусів з високою ефективністю виявлення шкідливого програмного забезпечення.
- Norton Small Business: Має потужний двигун виявлення загроз, що дозволяє ефективно боротися з відомими і новими видами вірусів.

Вплив на продуктивність системи:

- Bitdefender Small Office Security: Має низький вплив на продуктивність системи завдяки оптимізації ресурсів та швидкому скануванню.
- Norton Small Business: Забезпечує ефективний захист, маючи мінімальний вплив на продуктивність системи.

Керування та адміністрування:

- Bitdefender Small Office Security: Надає централізоване керування та адміністрування через хмарний портал.
- Norton Small Business: Має зручний інтерфейс управління для простого керування безпекою бізнесу.

Вартість:

- Bitdefender Small Office Security: Пропонує різні пакети з різними цінами, залежно від обсягу функціональності та кількості пристроїв. Пакет на рік та з 20 пристроями коштує 500$.
- Norton Small Business: Має гнучку ціноутворення, що дозволяє підібрати оптимальний план за доступну ціну. Пакет на рік та з 20 пристроями коштує 260$.

Але все ж таки я б рекомендував зупинитись на антивірусній програмі Norton з пакетом Norton Small Business. Norton Small Business – це простий у використанні продукт для стартапів та малого бізнесу. Це хмарний сервіс із простим розгортанням та керуванням пристроями, який ідеально підходить для малого бізнесу, оскільки IT-відділ не потрібен для його впровадження.

3. Безпека електронної пошти

Безпека електронної пошти є одним з найважливіших аспектів інформаційної безпеки для малого бізнесу. З моменту виникнення електронної пошти вона стала невід'ємною частиною ділового спілкування та обміну інформацією. Проте, разом зі зручністю та ефективністю використання електронної пошти постають і загрози, пов'язані зі зловживанням та несанкціонованим доступом до конфіденційних даних. Тому, для малого бізнесу важливо розуміти основні аспекти та принципи безпеки електронної пошти, а також обрати відповідні заходи та засоби, щоб захистити свою бізнес-інформацію від потенційних загроз.

Microsoft Office 365 Advanced Threat Protection (ATP) — це хмарна служба фільтрації електронної пошти, яка допомагає захистити вашу організацію від невідомих зловмисних програм і вірусів, забезпечуючи захист від загроз нульового дня та функціональність SafeLink. Він також надає потужні інструменти класифікації даних для інформації у вашій мережі, SharePoint, OneDrive та середовищі електронної пошти, щоб захистити від витоку та втрати даних.

Microsoft Outlook / O365 / Office 365 – Кнопка попередження про фішинг – хоча ця утиліта Outlook не є набором інструментів безпеки, вона дозволяє користувачам миттєво повідомляти про фішингові або підозрілі електронні листи вашій команді IT-безпеки, які, можливо, пройшли через правила карантину та інші засоби захисту електронної пошти. Після повідомлення за допомогою кнопки сповіщення про фішинг, відповідні електронні листи перевіряються вашою IT-командою, і можуть бути вжиті додаткові дії, зокрема нові правила карантину чи зміни в політиці. Хороший інструмент, який можна мати у своїй сумці хитрощів, щоб допомогти перешкодити спробам соціальної інженерії.

Використовуйте фільтрацію електронної пошти для блокування шкідливих файлів.Подумайте про блокування типів файлів, які вам ніколи не знадобляться як бізнес. Блокуйте будь-які вкладення з виконуваним вмістом, щоб запобігти випадковому виконанню шкідливих сценаріїв на ваших пристроях. Нижче в (Таблиці 3.2) наведено список типів файлів, які варто заблокувати або помістити в карантин:

Таблиця 3.2

Список типів файлів, які варто заблокувати або помістити в карантин

.app	.arj	.bas	.bat	.cgi	.chm	.cmd
.com	.cpl	.dll	.exe	.hta	.inf	.ini
.ins	.jar	.js	.jse	.lnk	.mht	.mhtm
.mhtml	.msi	.ocx	.pcd	.pif	.pl	.py
.reg	.scr	.sct	.sh	.shb	.shs	.url
.vb	.vbe	.vbs	.vbx	.ws	.wse	.wsf

4. Менеджер паролів. У сучасному цифровому світі, де безпека даних є надзвичайно важливою, ефективне керування паролями є необхідністю для малого бізнесу. Збереження унікальних та складних паролів для кожного облікового запису може стати викликом, особливо коли компанія має багато співробітників і використовує різні онлайн-сервіси та програми. У таких випадках, менеджер паролів стає незамінним інструментом для забезпечення безпеки електронних облікових записів. Він дозволяє зберігати, керувати та генерувати безпечні паролі, а також автоматично заповнювати їх на різних пристроях та платформах.

Основні аспекти, які слід враховувати при виборі менеджера паролів для малого бізнесу, включають наступне:

Функціональність: Важливо забезпечити, щоб менеджер паролів мав всі необхідні функції для ефективного керування паролями. Це включає можливість генерації сильних та унікальних паролів, автоматичне заповнення паролів на різних пристроях та браузерах, а також можливість синхронізації паролів між пристроями.

Безпека: Важливо, щоб менеджер паролів мав надійні заходи безпеки для захисту вашої бізнес-інформації. Це може включати шифрування даних, двофакторну автентифікацію, можливість встановлення майстер-пароля та контроль доступу до паролів для співробітників.

Інтеграція та сумісність: Переконайтеся, що обраний менеджер паролів може інтегруватися з існуючими програмами та сервісами, які ви використовуєте у своєму бізнесі. Також варто перевірити, які пристрої та операційні системи підтримуються, щоб забезпечити сумісність зі всіма пристроями вашої компанії.

На основі огляду різних джерел та рекомендацій, хочу порекомендувати менеджер паролів LastPass. Цей менеджер паролів відомий своєю широкою функціональністю та надійністю. Він пропонує синхронізацію паролів на різних пристроях, автоматичне заповнення паролів на веб-сайтах та захищене зберігання паролів у хмарі. Якщо говорити про платну підписку яку пропонує даний менеджер паролів то вона складає 69$ на рік в яку також входять Single Sign-on (SSO) та Multifactor Authentication (MFA).

5. Вибір брандмауера. Захист комп'ютерної мережі від потенційних загроз та несанкціонованого доступу є критичним завданням для малого бізнесу. У сучасному цифровому світі, де інформація є найціннішим активом, необхідність в ефективних заходах безпеки стає все більшою.

Брандмауери є важливою першою лінією захисту від хакерів, троянів, шпигунського програмного забезпечення, вірусів та інших мерзенних загроз.

Сучасні брандмауери пропонуються в багатьох варіантах, які можна адаптувати до розміру вашої компанії та проблем безпеки. Хорошим вибором для невеликих компаній є брандмауер Cisco Meraki рівня 7 «нового покоління» Cisco, включений до їхніх пристроїв безпеки MX. Він включає в себе простий у використанні централізований веб-інтерфейс і надає адміністраторам повний контроль над доступом користувачів, вмістом і додатками в їхній мережі, а також відстежує трафік для підтримки надійного периметра захисту.

6. Навчання персоналу. Регулярні тренінги з питань безпеки для ваших співробітників є ключовим фактором зниження ризику. Регулярне спілкування щодо

того, що можна і чого не можна робити в безпеці, а також стимульовані фішингові кампанії для оцінки старанності співробітників допоможуть їм бути в курсі потенційних атак фішингу та соціальної інженерії. Один із таких команд яку варто розглянути, це KnowBe4.

KnowBe4 є провідним постачальником послуг з навчання та підвищення освіченості щодо кібербезпеки. Вони спеціалізуються на наданні тренінгів з безпеки електронної пошти та соціальної інженерії, які допомагають організаціям зменшити ризики інцидентів з кібербезпеки, пов'язаних з людським фактором. Вони пропонує широкий спектр модулів навчання, риболовлі-симуляції та оцінок освіченості, які можуть бути налаштовані під потреби конкретної організації. Вони надають інтерактивні навчальні матеріали, які допомагають працівникам розпізнавати фішингові атаки, охороняти паролі та безпечно поводитися в онлайн-середовищі.

Підписка SaaS - це місячна ціна за місце, оплачувана щорічно. Вони пропонують 3 рівні Silver, Gold, Platinum або Diamond для задоволення потреб вашої організації, що складається з трьох рівнів доступу до навчання та всіх більш потужних функцій (Рисунок 3.1-3.2).

Training Content	Level I	Level II	Level III
Training Modules	13	58	184
Micro Modules (90 sec-5 min)	9	34	150
Video Modules	4	65	561
Posters / Images	41	52	246
Newsletters / Security Documents	15	37	281
Games	-	1	25

Рисунок 3.1 - Підписка SaaS з 3-рівневим режимом вибору

Бібліотека контенту KnowBe4 постійно поповнюється свіжим новим контентом. Цифри, перелічені вище, показують загальний обсяг контенту KnowBe4 ModStore за рівнем передплати і можуть бути змінені. KnowBe4 - найпопулярніша у світі інтегрована платформа для навчання та моделювання фішингової безпеки. Понад 60 000 організацій у всьому світі використовують його. Тепер у вас є спосіб краще справлятися з насущними проблемами IT-безпеки, такими як соціальна інженерія, фішинг та атаки програм-вимагачів.

Features	Silver	Gold	Platinum	Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program (ASAP)	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Brandable Content	✓	✓	✓	✓
Assessments	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration (ADI)	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓

Рисунок 3.2 - Підписка SaaS з 3-рівневим режимом вибору

Якщо говорячи про ціни за їхні послуги то вони варіюються в залежності від кількості людей та який із трьох рівнів ви виберете (Рисунок 3.3).

MSRP USD Monthly Pricing Per Seat 1 Year Term	Silver	Gold	Platinum	Diamond	SecurityCoach	Compliance Plus	PhishER
25-50	$1.80	$2.18	$2.55	$3.05	-	-	-
51-100	$1.60	$1.93	$2.25	$2.75	-	-	-
101-500	$1.30	$1.55	$1.80	$2.30	$1.20	$0.63	$1.00
501-1000	$1.20	$1.43	$1.65	$2.15	$1.10	$0.55	$0.75
1001-2000	$1.10	$1.30	$1.50	$2.00	$1.00	$0.48	$0.65
2001-3000	$1.00	$1.18	$1.35	$1.85	$0.90	$0.42	$0.55
3001-5000	$0.90	$1.05	$1.20	$1.70	$0.75	$0.36	$0.50
5001+	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote	Get A Quote

Рисунок 3.3 - Цінова політика підписок

Завдяки зручній школі навчання безпеки світового класу KnowBe4 надає вам можливість самостійно зареєструватися, а також перевірити фішингову безпеку до та після навчання, щоб показати відсоток кінцевих користувачів, схильних до фішингу. Високоефективні, часті випадкові тести захисту від фішингу від KnowBe4 надають кілька варіантів виправлення у випадку, якщо працівник піддасться симуляції фішингової атаки.

Висновок до третього розділу

Вибір та впровадження засобів забезпечення інформаційної безпеки для малого бізнесу вимагає уважного підходу і врахування кількох ключових аспектів. Оцінка потреб організації, вибір антивірусного програмного забезпечення, безпека електронної пошти, менеджер паролів, вибір брандмауера та навчання персоналу є важливими компонентами ефективної стратегії безпеки.

При виборі засобів забезпечення інформаційної безпеки, необхідно провести грунтовну оцінку потреб своєї організації, зрозуміти основні ризики та вразливості. Вибір антивірусного програмного забезпечення повинен базуватись на його функціональності, ефективності, ціні та підтримці. Забезпечення безпеки електронної пошти має включати антиспам-фільтри, захист від вірусів та шифрування листів. Використання менеджера паролів допоможе забезпечити безпеку облікових записів

та зменшити ризик неправильного використання паролів. Вибір брандмауера важливий для контролю трафіку та захисту мережі. Навчання персоналу стосовно безпеки інформації є ключовим елементом, що допоможе знизити ризик соціального інжинірингу та інших видів атак.

Загальною метою вибору та впровадження засобів забезпечення інформаційної безпеки для малого бізнесу є забезпечення захисту від потенційних загроз та збереження конфіденційності, цілісності та доступності даних. Дбайливий аналіз потреб, правильний вибір імплементованих рішень та постійне оновлення стратегії безпеки є ключовими факторами успішного функціонування малого бізнесу в умовах зростаючих кіберзагроз.

ВИСНОВКИ

У даній дипломній роботі були розглянуті важливі аспекти забезпечення інформаційної безпеки для малого бізнесу. В роботі був проведений аналіз типових загроз, з якими стикаються підприємства малого бізнесу, а також аналіз вразливостей, які можуть призвести до порушення інформаційної безпеки. Описані наслідки порушення інформаційної безпеки для малого бізнесу, що підкреслює важливість захисту даних та інформації.

Далі було проаналізовано різні засоби забезпечення інформаційної безпеки, зокрема антивірусні програми, антишпіонські засоби, файрволи, системи виявлення вторгнень, криптографічні засоби, засоби аутентифікації та контролю доступу, а також безпеку мереж та віртуальних приватних мереж (VPN). Ці засоби відіграють важливу роль у захисті даних та систем малого бізнесу від кіберзагроз.

В кінці роботи було надано рекомендації щодо вибору та впровадження засобів забезпечення інформаційної безпеки для малого бізнесу. Було висвітлено фактори, які впливають на вибір цих засобів, такі як обсяг даних, типи загроз, фінансові можливості тощо. Дано рекомендації щодо вибору антивірусного програмного забезпечення, забезпечення безпеки електронної пошти, використання менеджера паролів, вибору брандмауера та навчання персоналу.

На підставі проведеного аналізу можна зробити висновок, що забезпечення інформаційної безпеки для малого бізнесу є критично важливим завданням. Малі бізнеси стикаються з різноманітними загрозами та вразливостями, які можуть призвести до серйозних наслідків, включаючи втрату даних, порушення безпеки, фінансові втрати та пошкодження репутації.

Ефективне забезпечення інформаційної безпеки вимагає комплексного підходу та використання різних засобів забезпечення. Вибір відповідних засобів залежить від конкретних потреб та характеристик малого бізнесу. Антивірусні програми, файрволи, криптографічні засоби, засоби аутентифікації та навчання персоналу є важливими компонентами системи забезпечення інформаційної безпеки.

Рекомендації, надані у дипломній роботі, можуть слугувати орієнтиром для малих бізнесів при виборі та впровадженні засобів забезпечення інформаційної безпеки. Врахування факторів, що впливають на вибір, і правильне впровадження засобів забезпечення дозволить малому бізнесу досягти високого рівня інформаційної безпеки, захистити свої активи та забезпечити стабільність та успішність діяльності.

Однак, варто зауважити, що безпека інформації є постійним процесом, і необхідно постійно оновлювати та вдосконалювати систему забезпечення інформаційної безпеки, враховуючи змінюючі загрози та технологічний прогрес.

В цілому, розроблені рекомендації та проведений аналіз допоможуть малим бізнесам зрозуміти необхідність та значення забезпечення інформаційної безпеки, а також надати їм важливу інформацію та інструменти для вибору та впровадження відповідних засобів забезпечення. Виконання цих рекомендацій допоможе малим бізнесам ефективно захистити свої активи, зберегти довіру клієнтів та забезпечити успішну діяльність у сфері інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Principles of Information Security [Електронний ресурс]. – Режим доступу до ресурсу: https://books.google.com.ua

2. Security in Computing [Електронний ресурс]. – Режим доступу до ресурсу: https://eopcw.com

3. Computer and Information Security Handbook [Електронний ресурс]. – Режим доступу до ресурсу: https://booksite.elsevier.com

4. Neutralization: new insights into the problem of employee information systems security policy violations [Електронний ресурс] – Режим доступу до ресурсу: https://www.jstor.org

5. Information security governance: a simplified approach [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net.

6. Tan, J., & Teo, T. Factors influencing the adoption of information security management standards in small and medium-sized enterprises. Journal of Strategic Information Systems, 26(4) / Tan, J., & Teo, T.., 2017. – 289-314 с.

7. Vishnu, V., Chatterjee, S., & Ray, S. Small business information security adoption: An empirical investigation. Journal of Organizational Computing and Electronic Commerce / Vishnu, V., Chatterjee, S., & Ray, S.., 2018. – 20-43 с.

8. Baryamureeba, V., & Tushabe, F. Information security awareness and practices among small and medium enterprises: Evidence from Uganda. International Journal of Computer Science and Information Security / Baryamureeba, V., & Tushabe, F.., 2018. – 111-117 с.

9. Damiani, E., Cappelli, A., & Frati, F. Assessing and improving the information security posture of small and medium-sized enterprises. IEEE Transactions on Dependable and Secure Computing / Damiani, E., Cappelli, A., & Frati, F.., 2019. – 53-68 с.

10. Ma, Z., & Cai, L. Factors affecting information security investment in small and medium-sized enterprises: A comparative study of China and the United States. Information & Management / Ma, Z., & Cai, L.., 2020. – 103-150 с.

11. Ghosh, A. K., & Swaminathan, S. Managing information security risks in small and medium enterprises (SMEs) in emerging economies: The moderating role of top management support. Journal of Enterprise Information Management / Ghosh, A. K., & Swaminathan, S.., 2017. – 746-769 с.

12. Raman, R., & Saini, R. Information security awareness among employees in small and medium-sized enterprises: A case study. Information Systems Management / Raman, R., & Saini, R.., 2018. – 326-338 с.

13. Tsohou, A., & Mylonopoulos, N. An exploratory study of information security culture in small and medium-sized enterprises. Journal of Information Privacy and Security / Tsohou, A., & Mylonopoulos, N.., 2018. – 97-113 с.

14. Bhattacharyya, A., & Chakrabarti, S. A review of information security management frameworks in small and medium-sized enterprises. Journal of Cases on Information Technology / Bhattacharyya, A., & Chakrabarti, S.., 2019. – 32-49 с.

15. Chatterjee, S., & Vishnu, V. Information security risk management practices in small and medium-sized enterprises: A systematic literature review / Chatterjee, S., & Vishnu, V.., 2020. – 102-145 с.

16. Rindova, V. P., & Kotha, S. Information security in small and medium-sized enterprises: A review and synthesis. / Rindova, V. P., & Kotha, S.., 2021. – 241-271 с.

17. "Small Business Information Security: The Fundamentals" [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

18. "Cyber Security for Small Business" [Електронний ресурс] // Federal Communications Commission (FCC) – Режим доступу до ресурсу: (https://www.fcc.gov/sites/default/files/cybersecurity_for_small_businesses.pdf).

19. ДСТУ ISO/IEC 27032:2016. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). На заміну ISO/IEC 27032:2015 ; чинний від 2018-01-01. Вид. офіц. 2016.

20. Кириленко М.В., Перов В.І. "Інформаційна безпека підприємства" [Електронний ресурс] – 2018. – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/221618957.pdf.

21. Шипулін Ю.В. "Методика інформаційної безпеки підприємств малого бізнесу" [Електронний ресурс] – 2020. – Режим доступу до ресурсу: http://nbuv.gov.ua/UJRN/ntusareg_2020_35_4_12.

22. Москаленко О.С., Гончарова О.А. "Організаційно-економічний механізм забезпечення інформаційної безпеки підприємств малого бізнесу" [Електронний ресурс] – 2021. – Режим доступу до ресурсу: http://nbuv.gov.ua/UJRN/ijee_2021_3_28.