

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет комп'ютерних наук та технологій
(повне найменування інституту, факультету)

Кафедра комп'ютерних систем та мереж
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавра

(ступінь вищої освіти (освітній ступінь))

на тему

РОЗРОБКА ЦЕНТРАЛЬНОЇ ЧАСТИНИ
КОМП'ЮТЕРНОЇ МЕРЕЖІ БАНКУ

Виконав: студент 4 курсу, групи КНТ-519
спеціальності

123 «Комп'ютерна інженерія»

(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Комп'ютерна інженерія»

КАЗАНСЬКИЙ О.А

(ПРИЗВИЩЕ та ініціали)

Керівник СКРУПСЬКИЙ С. Ю.

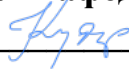
(ПРИЗВИЩЕ та ініціали)

Рецензент ЄФИМЕНКО М.В.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти (освітній ступінь) бакалаврський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ
Завідувач кафедри КУДЕРМЕТОВ Р.К.

« » 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТА

Казанський Олексій Аркадійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) розробка центральної частини комп'ютерної мережі банку

керівник проекту (роботи) Скрупський Степан Юрійович к. т. н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «24» березня 2023 року № 71

2. Строк подання студентом проекту (роботи) 10 травня 2023 року

3. Вихідні дані до проекту (роботи) Завдання кафедри на виконання бакалаврської роботи; Наукова література з тематики бакалаврської роботи

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Кібербезпека – загрози, вразливості та атаки;

2) Інструменти для підвищення безпеки даних

3) Проектування банківської мережі;

4) Діагностика розробленої мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Основні типи кібератак;

Куб кібербезпеки;

Структурна схема мережі банку.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	СКРУПСЬКИЙ С.Ю., к.т.н., доцент		
нормо контроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.03.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз наявних методів та алгоритмів розробки мережі банку, перегляд отриманих результатів, виділення недоліків та переваг	01.03.2023 р.	
2	Розробка структури системи	15.03.2023 р.	
3	Реалізація центральної частини мережі банку	20.03.2023 р.	
4	Діагностика розробленої мережі	01.04.2023 р.	
5	Оптимізація розробленої системи	10.04.2023 р.	
6	Оформлення отриманих результатів у ПЗ	01.05.2023 р.	
7	Оформлення графічного матеріалу	10.05.2023 р.	
8	Оформлення допоміжного матеріалу	17.05.2023 р.	

Студент(ка)

Керівник проекту (роботи)



(підпис)



(підпис)

Олексій КАЗАНСЬКИЙ

(Ім'я ПРІЗВИЩЕ)

Степан СКРУПСЬКИЙ

(Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 97 с., 55 рисунків, таблиця, 10 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, КІБЕРБЕЗПЕКА, КОНФІДЕНЦІЙНІСТЬ, ЗАХИСТ ДАНИХ.

Об'єкт дослідження – процес обігу даних у банківському секторі.

Метою бакалаврської роботи – розробка центральної частини комп'ютерної мережі банку, аналіз аномальної діяльності цієї мережі та підвищення її безпеки та відмовостійкості.

У теоретичній частині бакалаврської роботи я вивчав банківські інформаційні процеси, сучасні загрози безпеці комп'ютерних мереж у світі, види кібератак, технології хмарних обчислень та їх вразливості, способи забезпечення відмовостійкості мережі, безпеку операційної системи, різні технології комп'ютерних мереж та нормативно-правові акти щодо захисту даних в цілому.

Основні результати: в ході роботи було розглянуто інформаційні процеси банку, сучасні загрози безпеці комп'ютерних мереж у світі, види кібератак, хмарні технології та їх вразливості, способи забезпечення відмовостійкості мережі, безпеку операційної системи, різні технології комп'ютерних мереж та нормативно-правові акти щодо захисту даних в цілому. Крім того, описано розгортання основної філії комп'ютерної мережі банку, розслідування аномальних/зловмисних дій в мережі та, на основі отриманих емпіричних даних, зменшення вразливостей в досліджуваній мережі.

ЗМІСТ

Перелік умовних позначень	6
Вступ.....	7
1 Кібербезпека - загрози, вразливості та атаки	9
1.1 Проблеми кібербезпеки	9
1.2 Захист у кіберпросторі.....	14
1.3 Типи кібератак.....	32
1.4 Висновки до розділу 1	35
2 Інструменти для підвищення безпеки даних.....	36
2.1 Технології виявлення та запобігання мережевим атакам.	36
2.2 Загальний регламент про захист даних.....	57
2.3 Висновки до розділу 2	59
3 Проектування банківської мережі	59
3.1 Налаштування середовища проектування	59
3.2 Розробка центральної частини мережі банку.....	62
3.3 Діагностика протоколу EIGRP.....	77
3.4 Висновки до розділу 3	84
4 Діагностика розробленої мережі	84
4.1 Використання протоколу netflow	84
4.2 Інструменти для перевірки мережі та усунення вразливостей	86
4.3 Висновки до розділу 4	91
Висновки	92
Перелік джерел посилання	93

Плакат 1 – Основні типи кібератак

Плакат 2 – Куб кібербезпеки

Плакат 3 – Структурна схема мережі банку

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL– Access Control List;	PIN – Personal Identification Number;
APT– Advanced Persistent Threat;	RIP – Routing Information Protocol;
ARP– Address Resolution Protocol;	SCP – Secure Copy;
DHCP–Dynamic Host Configuration Protocol;	SHA – Secure Hash Algorithm;
DMZ – DeMilitarized Zone;	SSD – Solid-State Drive;
DNS – Domain Name Service;	SSH – Secure Shell;
DoS – Denial of Service;	STP – Spanning Tree Protocol;
EIGRP–Enhanced Interior Gateway Routing Protocol;	TCP – Transmission Control Protocol;
FTP – File Transfer Protocol;	VLAN– Virtual Local Area Network;
GDPR–General Data Protection Regulation;	VPN – Virtual Private Network;
GLBP – Gateway Load Balancing Protocol;	VRRP–Virtual Router Redundancy Protocol;
HDD – Hard Disk Drive;	ААО – аутентифікація, авторизація та облік;
HIDS – Host Intrusion Detection System;	ВМ – віртуальна машина;
HSRP – Hot Standby Router Protocol;	ДБЖ – джерела безперебійного живлення;
IDS – Intrusion Detection Systems;	ІТ– інформаційні технології;
IGMP –Internet Group Management Protocol;	ОС– операційна система;
IOS – Internetwork Operating System;	ПК– персональний комп'ютер;
IP – Internet Protocol;	ПЗ– програмне забезпечення;
IPS – Intrusion Prevention Systems;	ЦОД – центр обробки даних.
LACP – Link Aggregation Control Protocol;	
MAC – Media Access Control;	
MD– Message Digest;	
NAC– Network Access Control	
NAT – Network Address Translation;	
OSPF – Open Shortest Path First;	

ВСТУП

З ростом та розвитком компаній змінюються і їхні мережеві потреби. Виконання критично важливих завдань тісно пов'язане з мережевою інфраструктурою компанії. Збої в роботі мережі можуть призвести до зниження прибутку і втрати клієнтів. Розробники мереж повинні проектувати та впроваджувати високо масштабовані та доступні корпоративні мережі. Сучасні організації повинні швидко виявляти порушення кібербезпеки та ефективно реагувати на інциденти.

Економічний вплив кібератак важко оцінити кількісно, але, за даними CyberSecurity Ventures, щорічні глобальні втрати від кібератак до 2021 року сягнуть 6 трильйонів доларів.

Однією з головних цілей кіберзлочинців є отримання списків персональних даних та їх продаж у тіньовому інтернеті. Персональна інформація - це інформація, яка може бути використана для ідентифікації особи (ім'я, номер картки соціального страхування, дата народження, номер кредитної картки, номер банківського рахунку, державне посвідчення, адресна інформація (домашня адреса, електронна пошта, номер телефону)). Доступ до тіньової частини мережі можливий лише за допомогою спеціального програмного забезпечення. Ці розділи використовуються злочинцями для приховування своєї діяльності. Викрадені персональні дані можуть бути використані для створення фальшивих облікових записів, наприклад, кредитних карток або короткострокових позик.

Зловмисники не роблять винятків. Вони націлені на вразливі кінцеві точки домашніх користувачів, малий та середній бізнес, а також великі державні та приватні організації.

Організації повинні вживати заходів для захисту своїх ресурсів, користувачів і клієнтів. Необхідно розробити та впровадити цілі кібербезпеки на практиці.

Усі технології, які змінюють світ і покращують життя людей, також роблять їх більш уразливими для атак. Одні лише технології не можуть запобігти, виявити, відреагувати та відновитися після кібератак.

Мережева безпека охоплює широкий спектр заходів і повинна розглядатися як частина загальної політики організації (компанії, фірми або підприємства) щодо забезпечення інформаційної безпеки. Оцінка вимог до безпеки мережевих даних є першим кроком у розробці плану впровадження заходів із захисту таких даних. При цьому слід враховувати характер діяльності організації, її стратегію та стиль управління, якщо дані зберігаються в мережі.

Важливість цієї бакалаврської роботи не можна недооцінювати. Кібербезпека є основним викликом для багатьох компаній у всіх галузях, а індустрія кібербезпеки стрімко розвивається. Кількість шкідливого програмного забезпечення збільшується з кожним роком, а потреба контролювати свої мережі зростає.

Метою даної бакалаврської роботи є розробка центральної комп'ютерної мережі банку та аналіз її аномальних дій з метою підвищення безпеки та відмовостійкості цієї мережі.

Основна мета цієї роботи полягає в тому, щоб:

- розробити центральну частину комп'ютерної мережі банку;
- імітувати аномальну/зловмисну активність і дослідити незвичайні мережеві зловживання;
- дослідити поточний стан загроз безпеці комп'ютерних мереж у всьому світі.

1 КІБЕРБЕЗПЕКА – ЗАГРОЗИ, ВРАЗЛИВОСТІ ТА АТАКИ

1.1 Проблеми кібербезпеки

Загрози та вразливості викликають велике занепокоєння у фахівців з кібербезпеки. Існує дві ключові визначальні умови: загрози збільшують ймовірність негативної події, наприклад, атаки, а вразливості роблять цілі більш вразливими до атак.

Дані, що потрапили до рук злочинців, можуть призвести до втрати конфіденційності для їхнього власника, вплинути на його фінансове становище, поставити під загрозу його кар'єру та особисті стосунки. Захист приватного життя - це великий бізнес. Однак Google і Facebook не обов'язково є найбільшими ризиками. Лікарні, фінансові установи, державні органи, звичайні робочі місця та електронна комерція можуть бути під більшим ризиком. Такі організації, як Google і Facebook, мають ресурси для найму висококваліфікованих кібер-експертів для захисту своїх доменів. Оскільки все більше організацій створюють величезні бази даних, що містять всі наші персональні дані, потреба в експертах з кібербезпеки зростає. Кіберзагрози є особливо небезпечними для деяких галузей та даних, які вони використовують.

Медичні пристрої, як-от фітнес-браслети, використовують хмарні платформи для бездротового передавання, зберігання та відображення медичних даних, як-от пульс, кров'яний тиск і рівень глюкози в крові. Ці пристрої генерують великі обсяги медичних даних, які можуть стати частиною медичної картки пацієнта.

Інформація про роботу може включати дані про попередні місця роботи та види діяльності. Трудові записи також можуть містити інформацію про заробітну плату та страхування. Фінансові записи можуть містити інформацію про доходи та витрати, можуть включати виписки з кредитних карток, кредитну історію та іншу банківську інформацію.

Існує ряд базових технічних послуг, які є критично важливими для роботи мереж та Інтернету. До них відносяться такі послуги, як маршрутизація, адресація,

доменні імена та управління базами даних. Всі вони є основними цілями для кіберзлочинців.

Злочинці використовують інструменти трасування пакетів для перехоплення потоку даних, що проходять через мережу. Це означає, що всі конфіденційні дані, такі як імена користувачів, паролі та номери кредитних карток, можуть бути скомпрометовані. Сніфери пакетів відстежують і записують всю інформацію, що проходить через мережу.

Злочинці також можуть використовувати пристрої-обманки, такі як відкриті точки доступу Wi-Fi. Якщо зловмисники встановлюють їх поблизу громадських місць, наприклад, кафе, туди можуть увійти незахищені люди, а фахівці зі сніферу пакетів можуть скопіювати особисті дані.

Наприклад Служба доменних імен (DNS)-це www.facebook.com, на цифрові IP-адреси. Якщо DNS-сервер не знає вашої IP-адреси, він надішле запит на інший DNS-сервер. Під час атаки підробки DNS, також відомої як отруєння кешу DNS, зловмисник вставляє фальшиві дані в кеш транслятора DNS. Атака з отруєнням кешу DNS використовує вразливість програмного забезпечення протоколу DNS, щоб змусити DNS-сервери перенаправляти трафік для певного домену на комп'ютер зловмисника замість законного власника цього домену.

Пакети переносять дані через мережі та Інтернет. Підробка пакетів, також відома як ін'єкція пакетів, втручається у встановлені мережеві комунікації, створюючи пакети так, ніби вони є частиною реального сеансу зв'язку. Така фальсифікація дає змогу зловмисникам пошкоджувати або перехоплювати пакети. Цей процес дозволяє зловмисникам перехоплювати авторизовані з'єднання або заважати користувачам використовувати певні мережеві сервіси. Експерти називають це атакою "людина посередині".

Ці приклади - лише крапля в морі загроз, які злочинці створюють для Інтернету та мережевих сервісів.

Атаки можуть відбуватися як зсередини організації, так і ззовні. Ці атаки можуть здійснюватися випадково або навмисно користувачами, такими як співробітники або партнери:

- неправильне поводження з конфіденційною інформацією;
- загрожує роботі внутрішніх серверів та обладнання мережевої інфраструктури;
- підключення заражених носіїв до комп'ютерної системи компанії полегшує зовнішні атаки;
- ненавмисно дозволяє шкідливому програмному забезпеченню потрапляти в мережу через шкідливі електронні листи або веб-сайти.

Внутрішні загрози можуть завдати більшої шкоди, ніж зовнішні, оскільки інсайдерські користувачі мають прямий доступ до будівель та інфраструктурного обладнання. Інсайдерські зловмисники зазвичай знають структуру мережі компанії, її ресурси та конфіденційні дані. Вони також можуть бути обізнані із заходами безпеки та політиками безпеки і можуть мати різні рівні привілеїв користувачів та адміністраторів.

Зовнішні загрози від зловмисників-аматорів або досвідчених зловмисників можуть використовувати вразливості мережевого обладнання або здійснювати соціальну інженерію, наприклад, спуфінг. Зовнішні атаки використовують слабкості та вразливості для отримання доступу до внутрішніх ресурсів.

Дані компанії включають дані про людські ресурси, дані про інтелектуальну власність і фінансові дані. Кадрова інформація охоплює заяви про прийняття на роботу, інформацію про заробітну плату, пропозиції про роботу, контракти зі співробітниками і будь-яку інформацію, використовувану для прийняття рішень про працевлаштування. Інтелектуальна власність, така як патенти, торгові марки та плани виробництва продукції, дає змогу компаніям отримати економічну перевагу перед конкурентами. Ця інтелектуальна власність вважається комерційною таємницею, і втрата цієї інформації може негативно вплинути на майбутнє компанії. Фінансові дані, такі як звіти про прибутки та збитки, баланси та інформація про рух грошових коштів, надають інформацію про фінансовий стан компанії. На рисунку 1.1 показано середню загальну вартість втрати даних по країнах у 2021 році, за даними IBM [1].

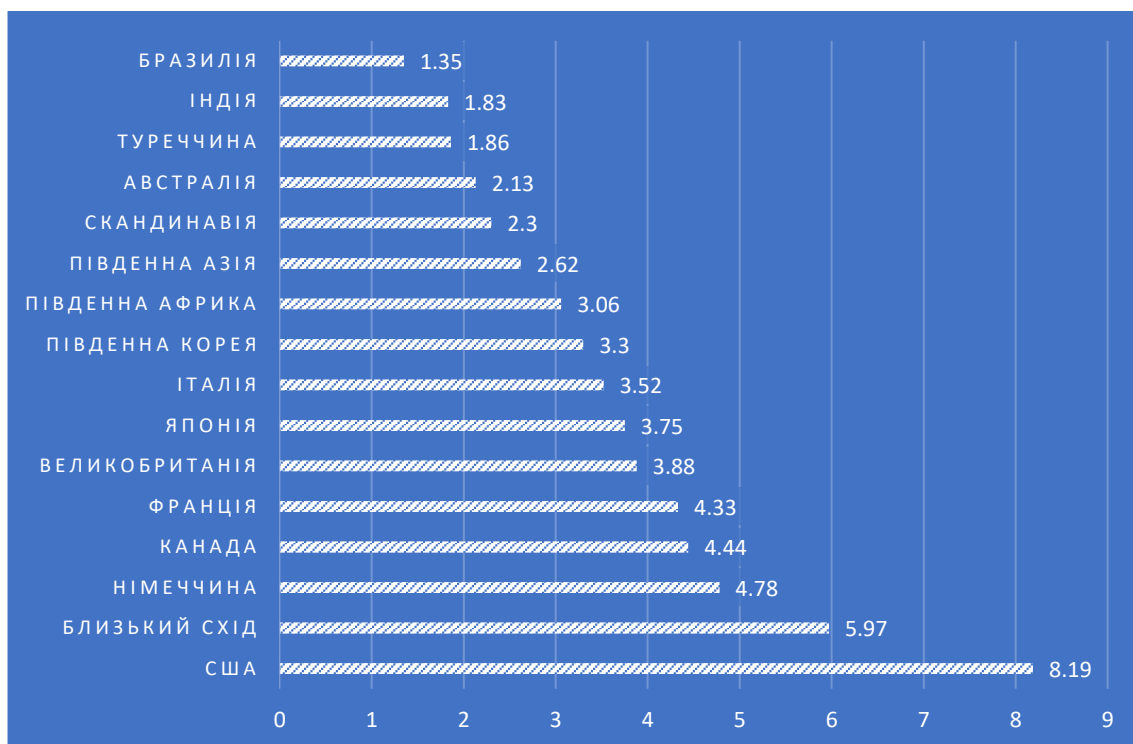


Рисунок 1.1 – Середні загальні витрати на втрату даних за країнами

В основі сучасних вразливостей програмного забезпечення лежать помилки програмування, вразливості протоколів або неправильна конфігурація системи. Все, що потрібно зробити кіберзлочинцю - це використати одну з них. Наприклад, поширеною атакою є модифікація програми шляхом створення певного потоку даних всередині програми, що призводить до її збою. Такий збій може стати точкою входу для несанкціонованого проникнення в додаток, що може призвести до витoku інформації.

Сьогодні кібератаки стають все більш витонченими - сучасні постійні загрози (Advanced Persistent Threats, APT) - це довготривалі, безперервні атаки на комп'ютери, які спрямовані на певну ціль. Злочинці зазвичай обирають цілі АРТ з бізнес – або політичних міркувань; АРТ є дуже прихованими, використовують складне шкідливе програмне забезпечення і тривають протягом тривалого періоду часу.

АРТ – атаки майже завжди дотримуються так званого "ланцюжка вбивств". Ланцюжок вбивства - це ряд кроків, які зловмисник виконує для проникнення в інформаційну систему. На рисунку 1.2 показані етапи ланцюга вбивства [2].

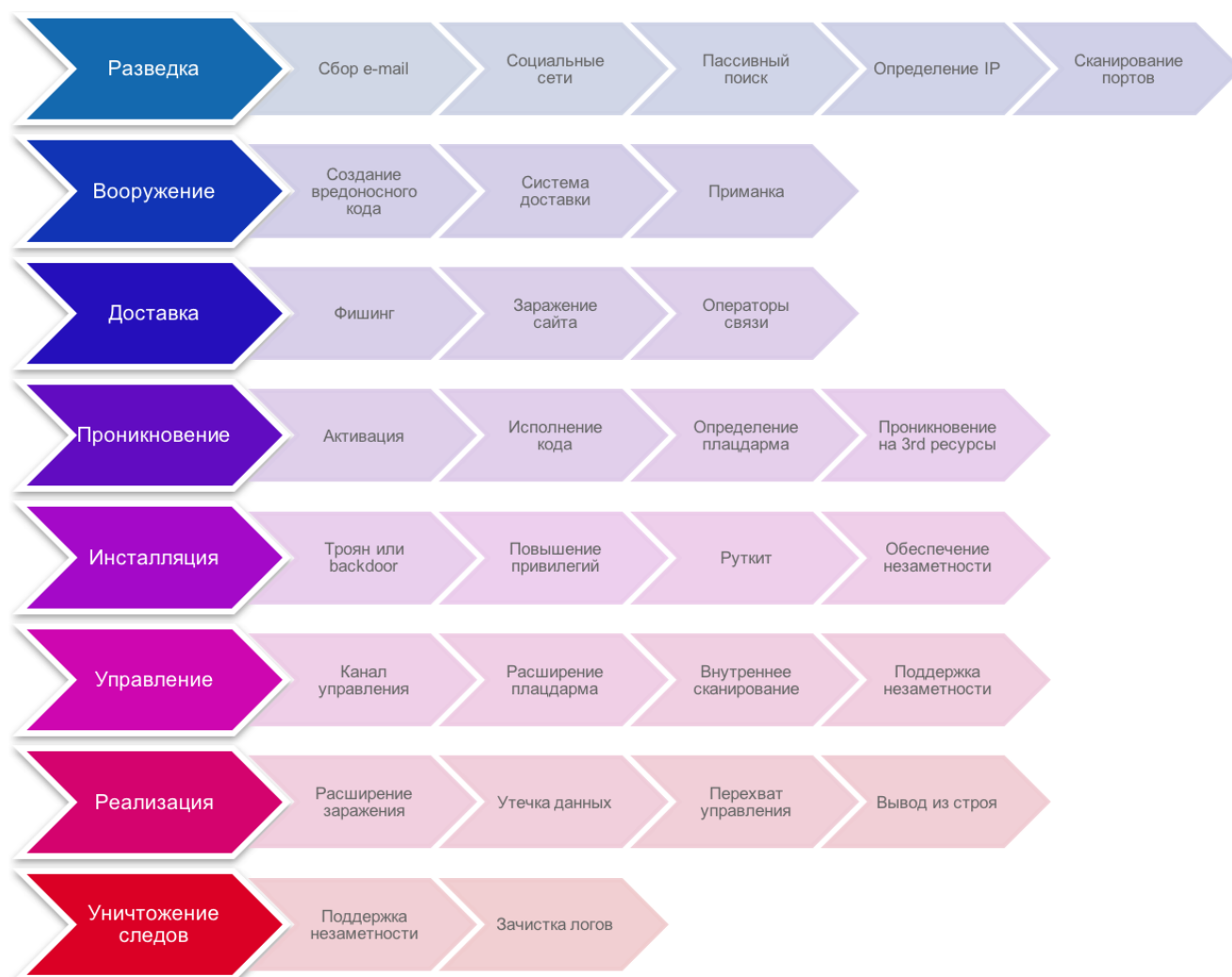


Рисунок 1.2 – Этапы вбивчого ланцюга

Алгоритмічні атаки можуть відстежувати дані, які автоматично надсилаються системою, наприклад, дані про енергію, яку споживає комп'ютер. Ця інформація може бути використана для вибору цілей атаки або для запуску хибних тривог. Алгоритмічні атаки також можуть пошкодити комп'ютери, використовуючи надмірну пам'ять або перевантажуючи процесор. Алгоритмічні атаки є більш складними, оскільки вони експлуатують елементи операційної системи, призначені для економії енергії, зменшення кількості системних збоїв і підвищення ефективності системи.

Нове покоління атак включає в себе інтелектуальне таргетування. Раніше об'єктами атак ставали найслабші або найбільш вразливі жертви. Однак підвищена увага до виявлення та ізоляції кібератак змусила кіберзлочинців бути більш

обережними. Вони не можуть ризикувати раннім виявленням, оскільки експерти з кібербезпеки знаходяться "на порозі" вразливостей. Як наслідок, найскладніші атаки відбуваються лише тоді, коли зловмисники можуть знайти типову ціль.

Інтегроване управління ідентифікацією використовується компаніями, які дозволяють користувачам отримувати доступ до мереж усіх компаній групи, використовуючи один і той самий ідентифікатор. Це збільшує масштаби та ймовірність каскадних ефектів у разі атаки.

Метою інтегрованого управління є автоматичний обмін обліковими даними в межах захищеної групи. Для окремого користувача це означає єдиний вхід в Інтернет.

Організаціям важливо ретельно продумувати ідентифікаційну інформацію, яку вони надають партнерам. Номери соціального страхування, імена та адреси можуть дозволити зловмисникам викрадати особисту інформацію партнерів для здійснення шахрайства. Найпоширеніший спосіб захистити інтегроване управління ідентифікаційними даними - пов'язати логіни з авторизованими пристроями.

1.2 Захист в кіберпросторі

На зорі кібернетичної ери захист від кібератак був низьким. Розумні старшокласники та аматори могли отримати доступ до систем. Сьогодні країни по всьому світу краще усвідомлюють загрозу кібератак. У більшості країн загроза кібератак зараз очолює список найбільш серйозних загроз національній та економічній безпеці.

Для захисту мереж, доменів та Інтернету використовується інструмент під назвою "Куб кібербезпеки". Перший вимір цього куба визначає мету кіберзахисту. Цілі, визначені в першому вимірі, є ключовими принципами. Три принципи - це конфіденційність, цілісність і доступність. Ці принципи слугують орієнтирами і

дозволяють фахівцям з кібербезпеки визначати пріоритетність дій при захисті будь-якої мережевої системи.

Конфіденційність означає запобігання розголошенню інформації несанкціонованим особам, ресурсам або процесам. Цілісність даних означає точність, узгодженість і надійність інформації. Нарешті, доступність гарантує, що інформація буде доступна авторизованим користувачам, коли вони її потребують.

Кіберпростір - це сфера, яка містить велику кількість важливих даних. Тому фахівці з кібербезпеки зосереджені на захисті даних. Другий вимір куба кібербезпеки зосереджений на проблемі захисту даних, які існують у кіберпросторі за різних обставин. Існує три можливі стани даних:

- дані в процесі передачі;
- дані в стані спокою або на зберіганні;
- дані що обробляються.

Кіберзахист вимагає, щоб фахівці з кібербезпеки забезпечували безпеку даних у всіх трьох ситуаціях.

Куб кібербезпеки визначає три типи навичок, що використовуються для забезпечення захисту. Перша навичка - це технології, пристрої та продукти, що використовуються для захисту інформаційних систем та стримування дій кіберзлочинців. Фахівці з кібербезпеки повинні бути знайомі зі спеціалізованими технічними засобами, процедури та інструкції і встановлювати надійні засоби захисту, які дозволяють кіберкористувачам залишатися в безпеці і дотримуватися принципів найкращих практик. Нарешті, кіберкористувачі повинні прагнути підвищувати обізнаність про кіберзагрози і розвивати культуру освіти та обізнаності з питань інформаційної безпеки. На рисунку 1.3 зображено куб кібербезпеки.

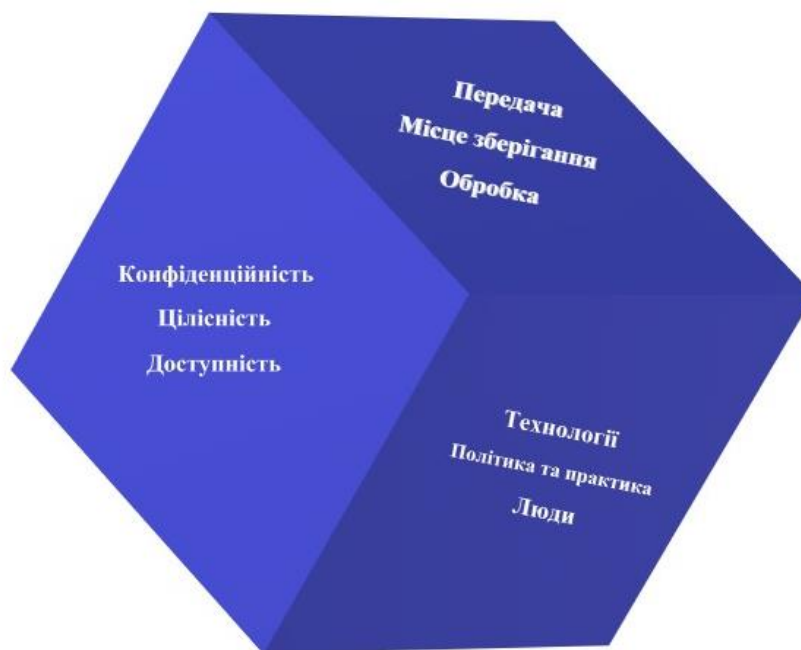


Рисунок 1.3 – Куб кібербезпеки

Організації зберігають великі обсяги даних. Більшість цих даних є загальнодоступними і не потребують захисту, наприклад, імена та номери телефонів співробітників. Однак деякі дані можуть потребувати спеціального захисту.

Конфіденційна інформація – це дані, захищені від несанкціонованого доступу для забезпечення безпеки окремих осіб або організацій. Існує три типи конфіденційної інформації:

персональна інформація – це інформація, тобто дані, які можуть бути використані для ідентифікації особи;

ділова інформація – це інформація, розголошення якої потенційно може спричинити проблеми для організації;

секретна інформація – це інформація, якою володіє державна установа і яка засекречена через її конфіденційний характер.

Контроль доступу визначає набір систем безпеки, які запобігають несанкціонованому доступу до комп'ютерів, мереж, баз даних та інших інформаційних ресурсів. Концепція ААО включає в себе три служби безпеки: автентифікацію, авторизацію та облік. Ці послуги забезпечують базову структуру контролю доступу.

Перша "А" в "ААО" означає "автентифікація". Автентифікація перевіряє особу користувача, щоб запобігти несанкціонованому доступу. Користувачі використовують ім'я користувача або ідентифікатор для підтвердження своєї особи[10].

Наприклад, щоб зняти готівку в банкоматі, вам потрібна банківська картка і PIN-код. Це ще один приклад багатофакторної автентифікації. Багатофакторна автентифікація вимагає різних типів автентифікації. Найпоширенішим типом автентифікації є використання пароля.

Авторизація визначає, до яких ресурсів користувачі можуть отримати доступ і які функції вони можуть виконувати за допомогою цих сервісів. Деякі системи реалізують це за допомогою списків контролю доступу, які визначають, чи мають авторизовані користувачі певні права доступу. Можливість підключитися до мережі компанії не означає, що користувач має право користуватися високошвидкісним кольоровим принтером. Автентифікація може також контролювати, коли користувачі можуть отримати доступ до певних ресурсів. Наприклад, користувачі можуть отримати доступ до бази даних продажів у робочий час, але система заблокує доступ у неробочий час.

Облік відстежує поведінку користувачів, включаючи дані, до яких вони отримують доступ, тривалість використання ресурсів та внесені зміни. Наприклад, банк відстежує кожен рахунок клієнта. Аудит цієї системи дозволяє виявити час і суму всіх транзакцій, а також працівників і системи, які здійснювали ці транзакції. Служби обліку кібербезпеки працюють подібним чином. Система відстежує всі операції з даними та надає результати аудиту. Щоб уможливити аудит системи, адміністратори можуть встановлювати комп'ютерні політики.

Концепція ААО схожа на використання кредитних карток. Кредитні картки визначають, хто може витратити, скільки користувач може витратити, а також реєструють товари та послуги, які користувач купує.

У кібербезпеці підрахунок відбувається в режимі реального часу - такі сайти, як Norse, відображають атаки в реальному часі на основі даних, зібраних в рамках системи підрахунку і відстеження.

Цілісність – це надійність даних протягом усього їхнього життєвого циклу. Іншими словами, цілісність – це якість. Дані проходять багато операцій, таких як збір, зберігання, пошук, оновлення та передача. Під час цих операцій дані повинні бути захищені від несанкціонованого втручання сторонніх осіб.

Методи забезпечення цілісності даних включають хешування, перевірку даних, узгодженість даних і контроль доступу. Системи забезпечення цілісності даних можуть включати один або декілька з перерахованих вище методів.

Цілісність даних є фундаментальним елементом інформаційної безпеки. Потреба в цілісності даних залежить від того, як організація використовує дані. Наприклад, Банки та фінансові установи цінують цілісність даних. Транзакції та рахунки клієнтів повинні бути точними. Для медичних організацій цілісність даних може бути питанням життя і смерті. Інформація про рецепти повинна бути точною.

Захист цілісності даних є постійним викликом для більшості організацій. Втрата цілісності даних може призвести до того, що всі дані стануть неточними або непридатними для використання.

Потребу в цілісності даних можна розділити на чотири типи важливості. Найважливішим рівнем є медичні та екстрені служби, де всі дані перевіряються, сертифікуються та визнаються достовірними. Прикладами є медичні документи та фінансові транзакції. Високий рівень - це електронна комерція та аналітика, де всі дані перевіряються, затверджуються і вважаються надійними. Бази даних є гарним прикладом високого рівня вимог до цілісності даних. Середній рівень - це онлайн-продажі та пошукові системи, наприклад, дані, зібрані з загальнодоступних форм, де існує мінімальна перевірка, а дані не викликають повної довіри. Найнижчий

рівень - блоги та сайти персональних публікацій, сервіси висловлення думок, де дані можуть бути неперевіреними, а отже, менш надійними.

Перевірка цілісності - це метод вимірювання узгодженості набору даних (файлів, зображень, записів). Перевірка цілісності використовує процедури, такі як хеш-функції, для безпосереднього створення "відбитка" даних. Щоб переконатися, що дані не були пошкоджені.

Контрольна сума - це приклад хеш-функції. Контрольні суми перевіряють цілісність файлу або рядка до і після його передачі з одного пристрою на інший через локальну мережу або Інтернет. Контрольні суми просто перетворюють кожен фрагмент інформації на значення і складають їх разом: якщо дві суми рівні, дані дійсні; якщо дві суми не рівні, дані недійсні; якщо вони не рівні, дані недійсні; якщо вони не рівні, десь у процесі передавання відбулася зміна.

Найпопулярнішими хеш-функціями сьогодні є MD5, SHA-1, SHA-256 і SHA-512. Хеш-значення використовуються для порівняння. Наприклад, після завантаження файлу користувач може перевірити його цілісність, порівнявши оригінальне хеш-значення з хеш-значенням, згенерованим хеш-калькулятором.

Організації використовують контроль версій, щоб запобігти випадковим змінам з боку авторизованих користувачів; два користувачі не можуть оновлювати один і той самий об'єкт. Об'єктом може бути файл, запис у базі даних або транзакція. Наприклад, перший користувач, який відкрив документ, має право змінювати цей документ; другий користувач має версію тільки для читання.

Належне резервне копіювання допомагає зберегти цілісність даних у разі їх пошкодження.

Авторизація визначає, хто може отримати доступ до ресурсів організації залежно від потреб. Наприклад, дозволи доступу до файлів, лише певні користувачі можуть змінювати дані. Адміністратор може встановити права доступу до файлу лише на читання. Як наслідок, користувачі, які мають доступ до цього файлу, не можуть вносити до нього жодних змін.

Доступність даних - це принцип, що використовується для опису необхідності постійно підтримувати доступність інформаційних систем і послуг.

Методи забезпечення доступності включають резервування системи, резервне копіювання системи, підвищену відмовостійкість системи, технічне обслуговування обладнання, оновлення операційних систем і програмного забезпечення, а також плани аварійного відновлення.

Зловмисні атаки, збої в роботі обладнання та стихійні лиха становлять загрозу для даних..

Люди використовують широкий спектр інформаційних систем у своєму повсякденному житті. Постійна доступність інформаційних систем є невід'ємною частиною сучасного життя. Термін "висока доступність" описує системи, призначені для запобігання простоїв. Висока доступність гарантує певний рівень продуктивності протягом більш тривалого періоду часу, ніж зазвичай. Системи високої доступності часто використовують три принципи побудови:

- усунути слабкі місця;
- важливо мати надійний план на випадок надзвичайних ситуацій;
- виявляйте помилки, коли вони виникають.

Мета полягає в тому, щоб забезпечити продовження роботи навіть в екстремальних умовах, наприклад, під час атаки. Однією з найпоширеніших технологій високої доступності є технологія five-nine. Назва five-nine пов'язана з тим, що ресурси доступні 99,999% часу. Це означає, що час простою становить менше 5,26 хвилин на рік.

Організації можуть забезпечити доступність шляхом регулярного проведення наступних заходів

- обслуговування обладнання;
- операційна система та оновлення системи;
- резервне копіювання та відновлення;
- готовність до стихійних лих;
- впровадження нових технологій;
- моніторинг аварійних ситуацій;
- тестування доступності.

Регулярне технічне обслуговування може значно збільшити час безвідмовної роботи системи. Технічне обслуговування охоплює заміну деталей, чищення та регулювання. Новітні операційні системи, додатки та програми постійно оновлюються для виправлення помилок і усунення вразливостей. Усі системи, додатки та програмне забезпечення мають регулярно оновлюватися. Фахівці з кібербезпеки можуть підписатися на повідомлення про нові оновлення. Забезпечте доступність системи шляхом резервного копіювання організаційних, конфігураційних і персональних даних. Системи резервного копіювання слід тестувати, щоб переконатися в їхній працездатності та можливості відновлення даних у разі їхньої втрати. Планування на випадок непередбачених обставин є ключовим елементом доступності системи. Співробітники та клієнти мають знати, як реагувати на надзвичайні ситуації. Команди кібербезпеки мають бути знайомі з процедурами відновлення критично важливих систем шляхом відпрацювання систем реагування та тестування резервних систем. Кіберзлочинці використовують новітні інструменти та хитрощі. Кіберпрофесіонали також повинні використовувати нові технології. Постійний моніторинг систем підвищує їхню доступність. Відстежуючи журнали подій, системні оповіщення та журнали доступу, фахівці з кібербезпеки можуть отримувати інформацію про систему в режимі реального часу. Ця інформація дає змогу виявляти атаки після того, як подія сталася, і дає змогу фахівцям із кібербезпеки відбивати атаки на місці. Усі системи мають бути перевірені на наявність вразливостей. Тестування включає в себе сканування портів, сканування вразливостей і тести на проникнення.

Збереження даних є складним завданням для організацій. Щоб покращити збереження даних, організації можуть покладатися на автоматизацію або централізоване резервне копіювання даних.

Сховище з прямим підключенням - один з найскладніших типів сховищ для моніторингу та управління. Воно більш вразливе до зловмисних атак на локальний комп'ютер. Дані, що зберігаються, можуть також містити резервні копії. Резервні копії можна створювати вручну або автоматично. Організації повинні обмежити

типи даних, що зберігаються на безпосередньо підключеному сховищі. Зокрема, не слід зберігати дуже конфіденційні дані.

Мережеві сховища є більш безпечним варіантом. Однак їхнє встановлення та керування складніше. Вони також обробляють більший обсяг даних, що створює більший ризик для організації в разі виходу пристрою з ладу. Якщо використовується мережеве сховище, особливу увагу слід приділити налаштуванню, тестуванню та моніторингу системи.

Захист даних під час передачі - одне з найскладніших завдань для фахівців з кібербезпеки. З розвитком мобільних і бездротових пристроїв фахівці з кібербезпеки несуть відповідальність за захист даних, які регулярно переміщуються через їхні мережі. Щоб захистити ці дані, фахівці з кібербезпеки повинні подолати кілька викликів:

Захист цілісності даних - кіберзлочинці можуть перехоплювати та пошкоджувати дані під час передачі. Щоб запобігти таким діям, фахівці з кібербезпеки впроваджують системи захисту цілісності даних, які перевіряють точність і автентичність переданих даних.

Захист доступності даних - кіберзлочинці можуть використовувати несанкціоновані або неавторизовані пристрої для порушення доступу до даних. Прості мобільні пристрої можуть маскуватися під локальні бездротові точки доступу та обманювати звичайних користувачів. Кіберзлочинці можуть переривати законні з'єднання із захищеними сервісами та пристроями. Щоб протистояти цьому процесу, може бути використана система взаємної автентифікації. Система взаємної автентифікації вимагає від користувача автентифікації на сервері, який, у свою чергу, автентифікує користувача.

Засоби контролю, що використовуються для захисту конфіденційності, цілісності даних під час передачі, включають VPN, SSL, IPsec, шифрування/розшифрування, хешування та надмірність.

Третій стан даних - це дані, які обробляються. Це стан, в якому дані спочатку вводяться, змінюються, обчислюються та витягуються.

Захист цілісності даних починається з введення даних. Організації використовують різні методи збору даних, зокрема ручне введення, сканування форм, завантаження файлів і зчитування з датчиків. Прикладами пошкодження даних під час введення даних є помилки при введенні даних, відключення датчиків системи, несправності та не функціональність. Помилки введення даних також включають неправильне маркування та неправильні або неузгоджені формати даних.

Модифікація даних - це будь-яка зміна вихідних даних. Приклади включають, коли користувачі змінюють дані вручну, коли додатки редагують та оновлюють дані або коли дані змінюються через збій обладнання. Такі процеси, як кодування/декодування, стиснення/розпакування та шифрування/розшифрування, є прикладами модифікації даних. Шкідливий код може спричинити пошкодження даних.

Пошкодження даних також може статися під час процесу виведення даних. Виведення даних передбачає передачу даних на принтер, електронний дисплей або на інший пристрій. Точність вихідних даних дуже важлива, оскільки вихідна інформація впливає на прийняття рішень. Прикладами пошкоджених вихідних даних є використання неправильних обмежувачів даних, неправильні налаштування з'єднання та неправильні налаштування принтера.

Ретельно розроблені системи необхідні для захисту даних під час обробки. Експерти з кібербезпеки розробляють політики та процедури, які вимагають тестування, обслуговування та оновлення систем, щоб вони працювали з мінімальною кількістю помилок.

Заходи щодо захисту конфіденційності, цілісності та доступності оброблюваних даних включають контроль доступу, перевірку даних і копіювання даних.

Захист програмного забезпечення - це програми та сервіси, які захищають операційні системи, бази даних та інші сервіси, що працюють на робочих станціях, мобільних пристроях і серверах. Існує кілька програмних технологій, що використовуються для захисту даних організації:

Брандмауери контролюють віддалений доступ до систем. Брандмауери зазвичай входять до складу операційної системи, але користувачі можуть придбати або завантажити брандмауери від інших виробників.

Мережеві та портові сканери виявляють і контролюють відкриті порти на хостах і серверах.

Аналізатор протоколів - це пристрій, який збирає і досліджує мережевий трафік. Він виявляє проблеми з продуктивністю, неправильні конфігурації та несправні програми, визначає загальні та нормальні шаблони трафіку та вирішує проблеми зв'язку.

Сканер вразливостей - це комп'ютерна програма, призначена для оцінки вразливостей комп'ютерів і мереж.

Системи виявлення вторгнень на рівні хоста (IDS) перевіряють лише активність у системі хоста, вони створюють журнали (записи в системному журналі) та сповіщають про виявлення аномальної активності. Системи, які зберігають конфіденційні дані або надають критичні дані, можуть бути хорошими цілями для хост-систем виявлення вторгнень (IDS).

Існують різні апаратні технології, що використовуються для захисту даних організації:

- брандмауер (апаратне забезпечення) блокує небажаний трафік на основі правил, які визначають дозволений вхідний і вихідний трафік у мережі;
- системи виявлення вторгнень (IDS) виявляють ознаки атак або аномального трафіку в мережі та надсилають сповіщення;
- системи запобігання вторгненням (IPS) виявляють ознаки атак або аномального трафіку в мережі, генерують оповіщення і вживають коригувальних заходів;
- служби фільтрації контенту контролюють доступ і передачу небажаного або неприйняттого контенту.

Для захисту даних організації використовується кілька мережевих технологій:

- віртуальна приватна мережа (VPN) - захищена віртуальна мережа, яка використовує публічну мережу (Інтернет); безпека VPN базується на шифруванні вмісту пакетів між кінцевими точками;

- контроль доступу до мережі (NAC) - перед тим, як дозволити пристрою підключитися до мережі, необхідно виконати низку перевірок. Ці перевірки включають встановлення останньої версії антивірусного програмного забезпечення та оновлення операційної системи;

- безпека бездротової точки доступу досягається за допомогою автентифікації та шифрування.

Хмарні обчислення передають технічні елементи безпеки від організації до хмарного провайдера. Існує три основні типи послуг хмарних обчислень:

- програмне забезпечення як послуга дозволяє користувачам отримувати доступ до прикладного програмного забезпечення та баз даних;

- інфраструктура як послуга забезпечує віртуальні обчислювальні ресурси через Інтернет. Провайдер надає у користування апаратне та програмне забезпечення, сервери і компоненти зберігання;

- платформа як послуга забезпечує доступ до інструментів і служб розробки, які використовуються для створення застосунків.

Кіберзлочинці потрапляють до користувачів, встановлюючи шкідливе програмне забезпечення на їхні кінцеві точки.

Вірус - це шкідливий програмний код, приєднаний до виконуваного файлу, так само, як і легальна програма. Більшість вірусів вимагають, щоб користувач запустив заражену програму, а також можуть активуватися в певний час і дату. Комп'ютерні віруси зазвичай поширюються одним із трьох способів: через знімні носії, через завантаження з Інтернету або через вкладення в пошті. Віруси можуть бути нешкідливими, просто відображати зображення на екрані або змінювати, модифікувати чи видаляти дані. Віруси мутують, щоб уникнути виявлення. Комп'ютер може бути заражений вірусом просто тому, що користувач відкрив файл.

Черв'яки - це шкідливий код, який самостійно поширюється, використовуючи вразливості в мережевій інфраструктурі. Хробаки зазвичай уповільнюють роботу мережі. На відміну від вірусів, яким для запуску потрібна інфікована хост-програма, черв'яки можуть працювати незалежно. Після первинного зараження черв'як більше не потребує втручання користувача. Після зараження комп'ютера черв'як може швидко поширюватися мережею. Хробаки працюють за єдиним принципом, вони використовують певні вразливості, мають механізм розповсюдження і виконують певні шкідливі дії.

Черв'яки відповідальні за деякі з найбільш руйнівних атак в Інтернеті. Наприклад, у 2001 році черв'як Code Red заразив 658 серверів. Протягом 19 годин він заразив понад 300 000 серверів.

Троянський кінь - це шкідливе програмне забезпечення, яке виконує шкідливі дії, замасковані під звичайні функції, наприклад, онлайн-ігри. Цей шкідливий код використовує привілеї користувача, який його запускає. Троянські програми відрізняються від вірусів тим, що вони приєднуються до невиконуваних файлів, таких як файли зображень, аудіо файли та ігри.

Логічні бомби - це шкідливі програми, які використовують тригери для запуску шкідливого коду. Наприклад, активатором може бути дата, час, запуск іншої програми. Логічні бомби залишаються в сплячому режимі, поки не відбудеться подія, яка запустить код. Після запуску логічна бомба виконує шкідливий код і завдає шкоди комп'ютеру. Цей тип шкідливого програмного забезпечення може знищувати файли баз даних, видаляти файли або атакувати операційні системи та програми. Нещодавно експерти з кібербезпеки виявили новий тип логічної бомби, яка атакує та руйнує апаратні компоненти робочих станцій та серверів, а саме: вентилятори охолодження, процесори, пам'ять, жорсткі диски та блоки живлення. Ця логічна бомба змушує ці пристрої працювати в критичному стані, поки вони не перегріються або не вийдуть з ладу.

Програми-зидирники блокують комп'ютерну систему або дані на ній доти, доки жертва не заплатить викуп. Зазвичай програми-зидирники шифрують дані на

комп'ютері за допомогою невідомого користувачеві ключа. Користувач повинен заплатити зловмиснику викуп, щоб розблокувати замок.

Деякі версії програм-здірників використовують вразливості певних систем, щоб заблокувати їх. Вимагачі поширюються так само, як і трояни, використовуючи завантаження файлів і вразливості програмного забезпечення.

Платіж, який має здійснити жертва, зазвичай здійснюється через платіжну систему, яка не дозволяє ідентифікувати одержувача. Після того, як жертва сплачує викуп, зловмисник надає їй програму-здірник, яка розшифровує файли або надсилає код розблокування.

Бекдор - це програма або код, доданий зловмисником, який проник у систему. Бекдори обходять стандартну автентифікацію, яка використовується для доступу до системи. Найпоширенішими програмами цього типу є Netbus і Back Orifice, які надають віддалений доступ до системи неавторизованим користувачам. Мета бекдору - дозволити кіберзлочинцям отримати доступ до системи в майбутньому, навіть після того, як усунеться вразливість, що використовувалася для атаки на систему. Зазвичай для встановлення бекдору зловмисники використовують легітимного користувача, який несвідомо запускає на комп'ютері троянського коня.

Руткіт модифікує операційну систему, створюючи чорний хід. Потім зловмисник використовує бекдор для отримання віддаленого доступу до комп'ютера. Більшість руткітів використовують вразливості програмного забезпечення для отримання більших привілеїв та модифікації системних файлів. Підвищення привілеїв може відбуватися через помилки програмування або недоліки дизайну, що дозволяє зловмисникам отримати більший доступ до мережевих ресурсів і даних. Руткіти також модифікують перевірки стану системи та інструменти моніторингу, що значно ускладнює виявлення цього типу шкідливого програмного забезпечення. У багатьох випадках, щоб видалити руткіт, необхідно перевстановити операційну систему.

За допомогою кількох простих кроків ви можете захистити свій комп'ютер від усіх типів шкідливих програм.

Антивірусне програмне забезпечення - більшість антивірусних пакетів успішно виявляють найпоширеніші форми шкідливого програмного забезпечення. Однак кіберзлочинці щодня розробляють і впроваджують нові загрози. Тому ключем до ефективного захисту від вірусів є постійне оновлення бази даних вірусних сигнатур. Вірусні сигнатури схожі на відбитки пальців людини. Вірусні сигнатури можна використовувати для ідентифікації та розпізнавання особливостей шкідливого коду.

Актуальне програмне забезпечення - більшість шкідливих програм досягають своєї мети, використовуючи вразливості операційних систем і додатків. Якщо раніше вразливості операційних систем були основним джерелом проблем, то зараз найбільший ризик становлять вразливості додатків. Хоча розробники операційних систем стають все більш стійкими до нових загроз, розробники додатків в основному експлуатують вразливості додатків.

Електронна пошта - це універсальна послуга, якою користуються мільярди людей по всьому світу. Будучи однією з найпопулярніших послуг, електронна пошта є основною вразливістю для користувачів та організацій. Спам, також відомий як небажана електронна пошта, є широко вживаним терміном. Загалом, спам - це різновид реклами. Однак деякі види спау можуть також містити шкідливі посилання, шкідливе програмне забезпечення або оманливий вміст. Основною метою такого спау є отримання конфіденційної інформації користувача, наприклад, номерів соціального страхування або реквізитів банківських рахунків. Більшість спау надсилається з великої кількості комп'ютерів у мережі, заражених вірусом або інтернет-черв'яком. Ці заражені комп'ютери надсилають якомога більше електронних листів.

Впровадження функцій захисту від спау не усуває його повністю. Нижче наведено деякі загальні характеристики спау:

- тема листа відсутня;
- електронна пошта із запитом на оновлення облікового запису;
- у тексті листа є друкарські помилки та незрозумілі розділові знаки;
- посилання в листах довгі або незрозумілі;

- електронні листи, які виглядають як реальне листування з організаціями;
- у листі необхідно відкрити прикріплений файл.

Якщо ви отримали електронний лист, який відповідає одній або декільком з цих характеристик, не відкривайте його або вкладений файл. Політика електронної пошти організації зазвичай вимагає, щоб користувачі, які отримують такі листи, повідомляли про це команду кібербезпеки. Однак, на жаль, небажана пошта продовжує перевантажувати мережі та сервери одержувачів.

Шпигунське програмне забезпечення - це програмне забезпечення, яке дозволяє зловмисникам отримувати інформацію про діяльність користувача на комп'ютері. Шпигунські програми часто містять інструменти, які відстежують активність, символи клавіатури та перехоплюють дані. Щоб обійти заходи безпеки, шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто йдуть у комплекті з легальним програмним забезпеченням або поширюються як "троянський кінь". Багато веб-сайтів, які розповсюджують умовно-безкоштовне програмне забезпечення, містять шпигунські програми.

Зазвичай це рекламне ПЗ відображає набридливі спливаючі вікна і генерує рекламний дохід для своїх творців. Шкідливе програмне забезпечення може аналізувати інтереси користувачів, відстежуючи веб-сайти, які вони відвідують. Після цього шкідливе програмне забезпечення може показувати спливаючу рекламу, пов'язану з темами цих веб-сайтів. Деякі версії програмного забезпечення автоматично встановлюють рекламне ПЗ. Деякі рекламні програми дійсно показують лише рекламу, але вони часто поширюються разом зі шпигунськими програмами.

Scareware - це шкідливе програмне забезпечення, яке використовує страх користувача, щоб змусити його виконати певні дії. Scareware створює спливаючі вікна, які нагадують діалогові вікна операційної системи. Ці вікна містять фальшиві повідомлення про те, що системі загрожує небезпека або що для повернення до нормальної роботи необхідно запустити певну програму. Насправді ніякої

проблеми немає, і якщо користувач дозволить запустити певну програму, на його комп'ютері буде встановлено шкідливий код.

Фішинг - це різновид шахрайства. Кіберзлочинці, які видають себе за надійні організації або приватних осіб, використовують електронну пошту, миттєві повідомлення та соціальні мережі для збору інформації, наприклад, реєстраційних даних або даних облікового запису. Фішинг виникає, коли зловмисник надсилає фальшивий електронний лист, який виглядає як такий, що надійшов з надійного джерела. Мета повідомлення - обманом змусити одержувача встановити шкідливе програмне забезпечення на свій пристрій або надати особисту чи фінансову інформацію.

Спрямований фішинг - це цілеспрямована фішингова атака. Як звичайний фішинг, використовують електронну пошту для зв'язку з жертвою. Однак у випадку цільового фішингу персоналізовані електронні листи надсилаються конкретним особам. Перед відправкою такого листа зловмисник вивчає інтереси потенційної жертви. Коли жертва переходить за посиланням, на її комп'ютер ненавмисно встановлюється шкідливе програмне забезпечення.

Зловмисники заражають веб-браузери для показу спливаючих оголошень, збору персональних даних та встановлення рекламного, вірусного та шпигунського ПЗ. Шкідливий код може бути встановлений у виконуваних браузерах, компонентах і доповненнях до браузерів.

Плагіни Flash і Shockwave від Adobe можна використовувати для створення привабливої графіки та анімації і значно покращити зовнішній вигляд веб-сайтів. Плагіни відображають вміст, створений за допомогою відповідного програмного забезпечення.

До недавнього часу добавки мали відмінні показники безпеки. Однак зі зростанням популярності Flash-контенту зловмисники звернули свою увагу на доповнення та програмне забезпечення Flash, виявляючи вразливості, якими можна скористатися. Успішна атака може призвести до краху системи або дозволити зловмиснику отримати контроль над нею. Очікується, що втрати даних

зростатимуть, оскільки злочинці продовжують досліджувати найпопулярніші плагіни та протоколи на предмет вразливостей.

Браузерні викрадачі - це шкідливе програмне забезпечення, яке змінює налаштування веб-браузера комп'ютера і перенаправляє користувачів на платні веб-сайти. Браузерні викрадачі зазвичай встановлюються без дозволу користувача під час автоматичного завантаження. Приховане завантаження - це програми, які автоматично завантажуються на комп'ютер, коли користувач відвідує певні веб-сайти або переглядає електронну пошту у форматі HTML. Щоб уникнути подібних загроз, завжди уважно читайте умови та положення при завантаженні програми.

Заходи боротьби зі спамом включають фільтрацію електронної пошти, навчання користувачів розпізнавати підозрілі листи та використання фільтрів хост/сервер.

Хоча повністю зупинити спам складно, можна зменшити його вплив. Наприклад, більшість інтернет-провайдерів блокують спам ще до того, як він потрапляє до поштової скриньки користувача. Крім того, більшість антивірусних програм та програм захисту електронної пошти автоматично фільтрують електронні листи. Це означає, що вони виявляють і видаляють небажані повідомлення з поштових скриньок користувачів.

Організації також повинні попереджати працівників про ризики, пов'язані з відкриттям вкладень, які можуть містити віруси або інтернет-черв'яків. Не думайте, що вкладення в електронному листі є безпечним, навіть якщо воно надійшло з надійного джерела. Комп'ютер відправника може бути використаний для розповсюдження вірусу несвідомо. Завжди перевіряйте вкладення, перш ніж відкривати їх.

Регулярні оновлення всього програмного забезпечення гарантують, що всі системи мають виправлення для усунення відомих вразливостей.

1.3 Типи кібератак

Атака на відмову в обслуговуванні (DoS-атака) - це тип мережевої атаки, при якій DoS-атака перериває доступ користувача, пристрою або програми до мережевих сервісів. Існує два основних типи DoS-атак:

- надмірний трафік - зловмисники надсилають так багато даних на таких високих швидкостях, що мережа, хост або додаток не встигають їх вчасно обробити. Це сповільнює передачу даних, іноді призводячи до збоїв у роботі пристроїв і сервісів;
- неправильно відформатовані пакети зловмисник надсилає неправильно відформатовані пакети даних на хост або додаток, і одержувач не може їх обробити. Наприклад, програма не може розпізнати пакети, які містять помилки. Це може призвести до того, що пристрій-одержувач працюватиме дуже повільно або навіть повністю перестане працювати.

DoS-атаки є серйозним ризиком, оскільки вони можуть легко порушити обмін інформацією та призвести до значних втрат часу та грошей. Ці атаки можуть бути відносно легко здійснені некваліфікованими зловмисниками.

Мета атаки на відмову в обслуговуванні - відмовити в доступі авторизованим користувачам через недоступність мережевої інфраструктури три основні принципи безпеки: конфіденційність, цілісність і доступність.

Розподілені атаки типу "відмова в обслуговуванні" (DDoS) схожі на DoS-атаки, але походять із кількох скоординованих джерел. Наприклад, DDoS-атака може відбуватися таким чином:

Зловмисники створюють мережі заражених комп'ютерів, так звані ботнети, що складаються з комп'ютерів-зомбі. Зомбі - це заражені комп'ютери. Зловмисник керує зомбі за допомогою спеціальної системи управління. Комп'ютери-зомбі постійно сканують мережу, заражаючи інші вузли і створюючи нових зомбі. Після такої підготовки хакер направляє ботнет на проведення DDoS-атаки через систему управління.

Шпигунство (sniffing) дуже схоже на стеження за кимось у реальному світі. Хакери вивчають весь мережевий трафік, що проходить через мережеву інтерфейсу карту, незалежно від того, кому він призначається. Злочинці аналізують мережевий трафік, використовуючи програмне забезпечення, обладнання або комбінацію того й іншого. Деякі мережеві аналізатори досліджують весь трафік і можуть змінювати частину або весь трафік. Мережеві адміністратори можуть використовувати такі інструменти для аналізу мережевого трафіку, виявлення проблем з пропускнуою здатністю та усунення інших проблем мережевої інфраструктури.

Фізичний захист необхідний для того, щоб гарантувати, що аналізатори трафіку не будуть встановлені у внутрішній мережі організації.

Підміна (Spoofing) - це атака, яка використовує довірчі відносини між двома системами: якщо дві системи підтримують автентифікацію з єдиним входом, користувачеві, який увійшов в одну систему, може не знадобитися повторно проходити процес автентифікації, щоб отримати доступ до іншої системи. Завдяки довірчим відносинам між системами цільова система може виконати запит без автентифікації.

Існує кілька типів спуфінг-атак.

Підміна MAC-адреси відбувається, коли комп'ютер отримує пакет даних, адресований на MAC-адресу іншого комп'ютера.

IP-спуфінг надсилає IP-пакети з фальшивої IP-адреси джерела, щоб замаскувати справжню адресу.

Протокол дозволу адрес (ARP) - це протокол, який перетворює IP-адреси в MAC-адреси для передачі даних. При атаці підміни ARP зловмисник надсилає фальшиве ARP-повідомлення через локальну мережу, пов'язуючи його MAC-адресу з легітимним користувачем в мережі за допомогою мапування IP-адрес.

Система доменних імен (DNS) пов'язує доменні імена з IP-адресами. Підробка DNS - це модифікація DNS-серверів для переправлення певних доменних імен на інші IP-адреси, контрольовані зловмисником.

Злочинці, які здійснюють атаки типу "людина посередині", перехоплюють повідомлення, якими обмінюються комп'ютери, і викрадають інформацію, що

надсилається мережею. Оскільки хости не знають, що повідомлення були змінені, зловмисник може маніпулювати повідомленнями і передавати неправдиві дані між хостами. Ця атака дозволяє зловмиснику отримати контроль над пристроєм без відома користувача.

Атака "Людина в мобільному" - це різновид атаки "Людина посередині" (Man-in-the-Mobile). Зловмисник отримує контроль над мобільним пристроєм. Заражений мобільний пристрій надсилає зловмиснику конфіденційну інформацію користувача.

При повторній атаці зловмисник перехоплює частину даних, що передаються між двома хостами, і ретранслює записане повідомлення. Таким чином є можливість обійти механізм автентифікації.

Атака нульового дня - це атака на комп'ютер, яка намагається використати вразливість програмного забезпечення, невідому або приховану виробником програмного забезпечення. Термін "нульова година" описує момент, коли хтось виявляє шкідливий програмний код. Поки виробники програмного забезпечення розробляють і випускають виправлення, мережі залишаються вразливими до експлуатації. Щоб захиститися від цих атак, фахівці з мережевої безпеки повинні більш ретельно продумувати архітектуру своєї мережі. Сьогодні практично неможливо запобігти численним вторгненням в систему з різних точок одночасно. На рисунку 1.2 показані основні типи кібератак.

Основні типи кібератак

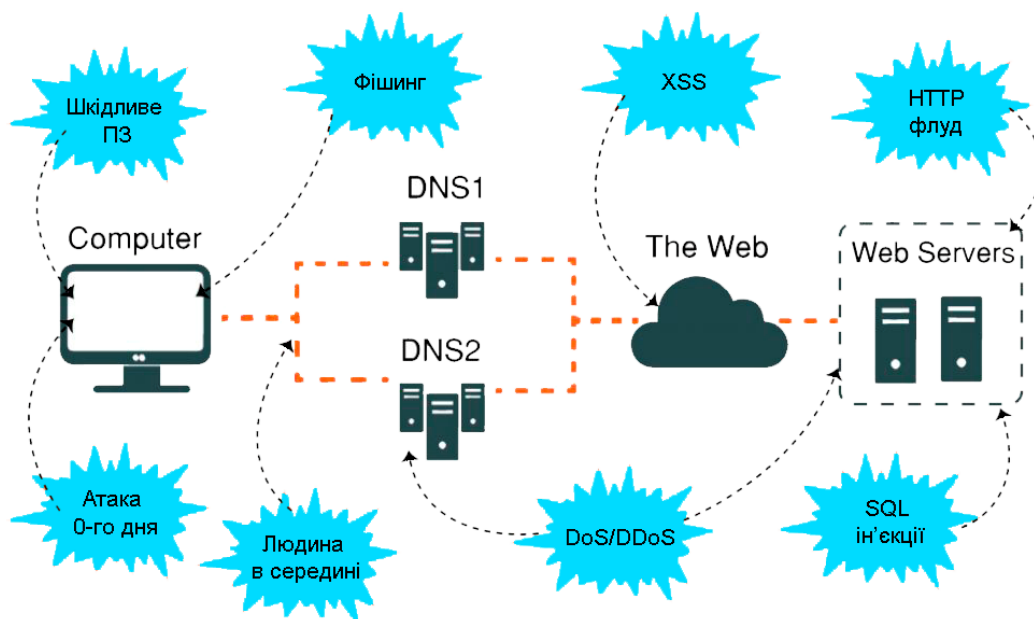


Рисунок 1.2 – Основні типи кібератак

1.4 Висновки до розділу 1

У цьому розділі описано різні типи кібератак, які здійснюють кіберзлочинці, і пояснено загрозу шкідливого програмного забезпечення та шкідливого коду. У ньому також розглядаються типи атак на дротові та бездротові мережі та описуються вразливості, які атаки створюють у додатках. Розуміючи типи загроз, які можуть виникнути, організації можуть виявити вразливості, які можуть стати мішенню для атаки. Це дозволяє їм захистити себе від кібер-шахрайства та зловживань.

2 ІНСТРУМЕНТИ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ДАНИХ.

2.1 Технологія виявлення та запобігання мережевим вторгненням

Організації, які прагнуть максимізувати доступність системи та даних, можуть вжити спеціальних заходів для мінімізації або усунення втрати даних. Мета - звести до мінімуму час простою критично важливих процесів. Якщо співробітники не можуть виконувати свої звичайні обов'язки, організація може втратити дохід.

Цей розділ описує різні підходи, які організації можуть застосовувати для досягнення своїх цілей щодо доступності. Резервування забезпечує додаткові елементи для створення резервних копій і забезпечення доступності комп'ютерних систем і мереж. Елементи резервування включають апаратне забезпечення, таке як диски, сервери, комутатори та маршрутизатори, а також програмне забезпечення, таке як операційні системи, додатки та бази даних. У цьому розділі також обговорюється відмовостійкість, тобто здатність сервера, мережі або центру обробки даних швидко відновлюватися і залишатися працездатними.

Висока доступність ґрунтується на тому, що система або компонент завжди увімкнений протягом певного періоду часу. Для того, щоб забезпечити високу доступність, необхідно:

- усунення окремих точок відмови;
- проектування для надійності;
- виявлення помилок по мірі їх виникнення.

Підтримка високої доступності за стандартом 99,999% призводить до збільшення витрат і використання багатьох ресурсів. Збільшення витрат пов'язане з придбанням додаткового обладнання, такого як сервери та компоненти. Організації додають компоненти, що, в свою чергу, збільшує складність конфігурації. На жаль, зі збільшенням складності конфігурації зростає і фактор

ризик. Чим більше рухомих частин, тим більша ймовірність виходу якогось компонента з ладу.

99% готовності означає 87 годин 36 хвилин простою на рік; 99,5% означає 43 години 48 хвилин простою на рік; 99,95% означає 4 години 23 хвилини простою на рік; 99,99% означає 53 хвилини простою на рік; 99,999% означає 5 хвилин простою на рік.

Вартість підтримки високої доступності може бути високою в деяких галузях, але для деяких організацій п'ять дев'яток можуть бути критично важливими.

Фінансова індустрія повинна підтримувати високу доступність для поточних транзакцій, зберігаючи при цьому довіру клієнтів.

Медичні заклади потребують високої доступності, щоб лікувати пацієнтів цілодобово.

До сектору громадської безпеки належать організації, які забезпечують безпеку та надають послуги громаді, державі чи нації.

Роздрібні торговці покладаються на ефективний ланцюг поставок, щоб доставити товари споживачам. Втрати можуть бути значними, особливо в періоди підвищеного попиту, наприклад, під час свят.

Люди очікують, що новини подаватимуть факти такими, якими вони є. Цикл новин постійно рухається 24/7.

Наступні загрози становлять високий ризик для доступності даних та інформації:

- якщо неавторизований користувач успішно проникає в основну базу даних організації та компрометує її;
- або якщо dos-атака є успішною та серйозно впливає на операційну діяльність;
- або організація зазнає значної втрати конфіденційних даних;
- або критично важливе програмне забезпечення перестає функціонувати;
- або адміністратори або привілейовані користувачі скомпрометовані;

- або виявлено незаконний обмін файловими серверами;
- або веб-сайт організації не працює, що впливає на зусилля зі зв'язків з громадськістю;
- або сильні шторми, такі як урагани та торнадо;
- катастрофічні події, такі як терористичні атаки, вибухи;
- тривалі перебої в наданні послуг;
- пошкодження водою внаслідок повені.

Стихійні лиха включають: землетруси, урагани, торнадо, повені та пожежі. Людські помилки, в тому числі несподівана помилка працівника при введенні даних або коли працівник впустив ноутбук. Апаратні проблеми, включаючи несправний жорсткий диск або неправильно налаштований брандмауер. Несанкціоноване втручання, що включає встановлення зловмисником бекдору або видалення файлів за допомогою хробака. Програмні атаки включають віруси, хробаки та DoS-атаки.

Програмні помилки - це помилки в програмному забезпеченні, які заважають програмам завантажуватися належним чином. Злодії можуть вкрати ноутбуки та обладнання з незамкнених приміщень. Відключення електроенергії може перервати надання комунальних послуг.

Висока доступність передбачає три ключові принципи для досягнення мети сталого доступу до даних і послуг:

- усунення або зменшення кількості точок відмови;
- гнучкість системи;
- відмовостійкість.

Важливо розуміти, як працювати з єдиною точкою відмови. Єдиною точкою відмови може бути хост-маршрутизатор або комутатор, мережеві служби або виділений ІТ-персонал. Важливо, що втрата однієї системи, процесу або людини може призвести до значних збоїв у роботі всієї системи. Також важливими є процеси, ресурси та компоненти, які зменшують кількість окремих точок відмови. Кластери високої доступності - це один із способів забезпечити надмірність. Кластер складається з групи комп'ютерів, які мають спільний простір для

зберігання даних і однакову мережеву конфігурацію. Всі сервери беруть участь в обробці сервісів одночасно. Зовні кластер серверів виглядає як один пристрій. Якщо один сервер у кластері виходить з ладу, інші сервери продовжують обробляти ті ж самі сервіси, що й несправний пристрій.

Відмовостійкість системи - це здатність підтримувати доступність даних і процесів, незважаючи на атаку або збій. Загалом, системи повинні бути надлишковими з точки зору пропускну здатності та обробки даних, щоб у разі виходу з ладу однієї системи, інша система могла продовжувати працювати без перерви в обслуговуванні. Стійкість системи - це не лише її загартування, але й забезпечення доступності даних та послуг у разі атаки.

Відмовостійкість дозволяє системі продовжувати працювати, навіть якщо один або кілька компонентів вийшли з ладу. У разі "збою", коли пристрій, наприклад, контролер диска, виходить з ладу, система дзеркалювання надає необхідні дані, не перериваючи роботу користувача.

Єдина точка відмови - це єдина точка в критично важливій функції, якщо вона вийде з ладу, то вийде з ладу вся функція. Стійкість системи - це здатність системи підтримувати доступність у разі збою. Відмовостійкість - це здатність системи продовжувати працювати, навіть якщо один або кілька компонентів вийшли з ладу.

Резервування $N+1$ забезпечує доступність системи у випадку відмови одного з компонентів. Компонент (N) повинен мати принаймні один резервний компонент ($+1$). Наприклад, автомобіль має чотири шини (N) і запасну шину в багажнику на випадок проколу ($+1$).

У центрі обробки даних $N+1$ означає, що система спроектована таким чином, щоб витримати втрату компонента, де N відноситься до різних компонентів, з яких складається центр обробки даних, таких як сервери, джерела живлення, комутатори та маршрутизатори, а $+1$ відноситься до додаткових компонентів, які працюють у разі потреби, і відноситься до систем резервного копіювання.

Прикладом резервування N+1 в дата-центрі є генератор, який вмикається, коли щось трапляється з електропостачанням з мережі; система N+1 містить резервне обладнання, але не є повністю резервованою системою.

Резервування підвищує доступність інфраструктури, захищаючи мережу від єдиної точки відмови, наприклад, від'єданого мережевого кабелю або несправності комутатора. Коли фізичне резервування закладено в мережу, можуть виникати петлі і дублювання кадрів, що може мати серйозний негативний вплив на комутаційну мережу.

Протокол Spanning Tree Protocol (STP) вирішує цю проблему, основна функція STP полягає в тому, щоб забезпечити відсутність петель в мережах, коли комутатори з'єднані декількома шляхами, STP запобігає виникненню петель на надлишкових фізичних каналах. Він гарантує, що існує тільки один логічний шлях, що з'єднує всі пункти призначення в мережі; STP навмисно виключає надлишкові шляхи, які можуть викликати петлі.

Виключення надлишкових шляхів є важливим для уникнення мережевих петель. Фізичні шляхи все ще існують для забезпечення надмірності, але STP відключає ці шляхи, щоб запобігти виникненню петель. Якщо мережевий кабель або комутатор виходить з ладу, STP перераховує шлях, розблоковує необхідні порти і вмикає резервний шлях.

Шлюзом за замовчуванням зазвичай є маршрутизатор, який забезпечує доступ до всієї мережі або Інтернету. Якщо як шлюз за замовчуванням використовується тільки один маршрутизатор, існує тільки одна точка відмови. Організації можуть встановити додаткові маршрутизатори в режимі очікування.

Маршрутизатори переадресації та резервні маршрутизатори використовують протоколи резервування, щоб визначити, який маршрутизатор повинен відігравати активну роль у переадресації трафіку. Кожен маршрутизатор має фізичну IP-адресу та віртуальну IP-адресу. Кінцеві пристрої використовують віртуальну IP-адресу як шлюз за замовчуванням. Маршрутизатори, що надсилають трафік, очікують, що дані надійдуть на адресу 192.0.2.100. Маршрутизатор-передавач і резервний маршрутизатор періодично надсилають повідомлення, використовуючи свої

фізичні IP-адреси. Ці повідомлення допомагають переконатися, що обидва маршрутизатори доступні і залишаються на зв'язку. Якщо резервний маршрутизатор не отримує ці періодичні повідомлення від основного маршрутизатора, резервний маршрутизатор перебирає на себе функцію переадресації.

Здатність мережі динамічно відновлюватися після відмов шлюзів називається резервуванням першого рівня.

На рисунку 2.1 представлено перелік технологій для забезпечення безпеки мережевої інфраструктури.

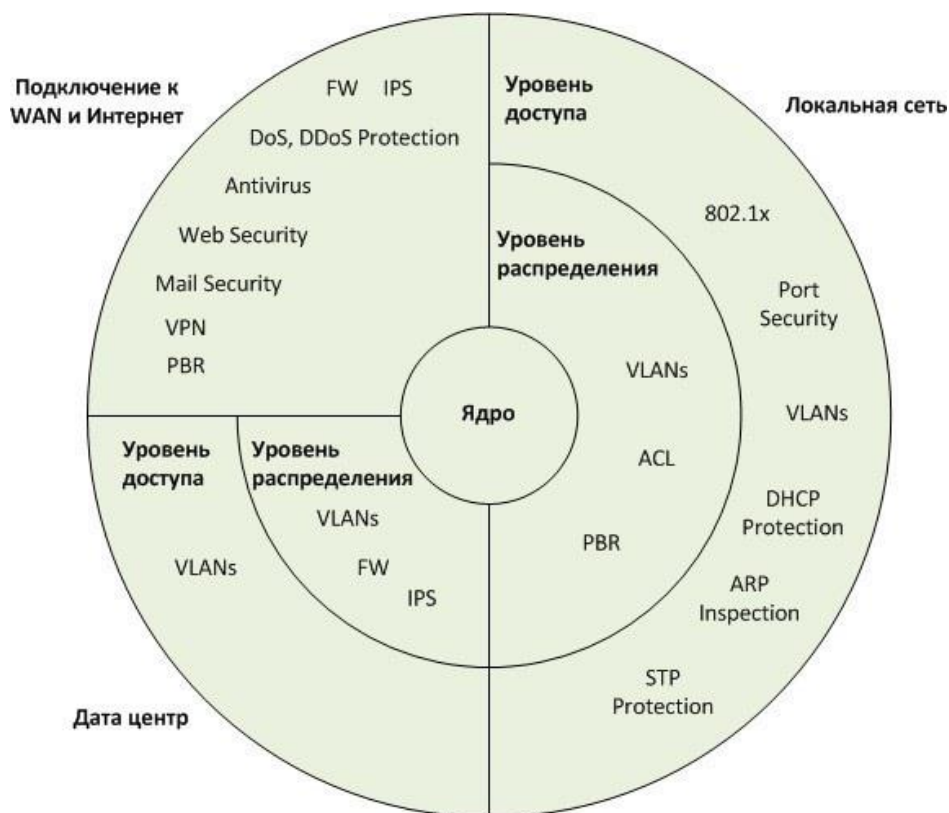


Рисунок 2.1 Перелік технологій для забезпечення безпеки мережевої інфраструктури.

Наступний список визначає доступні варіанти резервування маршрутизатора на основі протоколів, які забезпечують зв'язок між мережевими пристроями:

Протокол гарячого резервування маршрутизаторів (Hot Standby Router Protocol) - забезпечує високу доступність мережі, надаючи надлишкову

маршрутизацію першого переходу. Групи маршрутизаторів використовують HSRP для вибору активних і резервних пристроїв. У групі інтерфейсів пристроїв активний пристрій - це пристрій, який пересилає пакети, а резервний пристрій - це пристрій, який перебирає на себе функції, коли активний пристрій виходить з ладу. Резервний маршрутизатор HSRP відстежує робочий стан групи HSRP і швидко перебирає на себе пересилання пакетів, якщо активний маршрутизатор виходить з ладу.

Протокол резервування віртуального маршрутизатора (VRRP) - маршрутизатор працює за протоколом VRRP з одним або декількома іншими маршрутизаторами, підключеними до локальної мережі, обраний маршрутизатор стає основним віртуальним маршрутизатором, а інші маршрутизатори стають резервними маршрутизаторами в разі виходу з ладу основного маршрутизатора.

Протокол балансування навантаження шлюзу (GLBP) - захищає трафік даних від збоїв маршрутизатора і ланцюга, таких як HSRP і VRRP, і забезпечує балансування (розподіл) навантаження між резервними членами групи маршрутизаторів.

Організаціям можуть знадобитися резервні сайти для задоволення своїх потреб. Нижче описано три типи резервних позицій.

а) синхронна:

- 1) синхронізує обидва місця в режимі реального часу;
- 2) вимагає високої пропускної здатності;
- 3) щоб зменшити затримку, мають бути розташовані близько один до одного;

б) асинхронне копіювання:

- 1) не синхронізовано в реальному часі;
- 2) вимагає меншої пропускної здатності;
- 3) може бути розміщена на більшій відстані, оскільки затримка не є проблемою;

с) відтворення в певний час:

- 1) забезпечує регулярне оновлення резервних копій даних;

- 2) цей метод не вимагає постійного з'єднання і економить більшу частину пропускної здатності.

Правильний баланс між вартістю та доступністю визначить правильний вибір для вашої організації.

Відмовостійкість відноситься до методів і конфігурацій, що використовуються для забезпечення стійкості системи або мережі до збоїв. Наприклад, у деяких мережах можуть бути надлишкові канали між комутаторами, що працюють за технологією STP. STP забезпечує альтернативний шлях через мережу, коли канал виходить з ладу, але якщо конфігурація не є оптимальною, перемикання може відбутися не одразу.

Протоколи маршрутизації також забезпечують відмовостійкість, але їх вдосконалення може спростити переходи і зробити їх непомітними для користувачів мережі. Адміністраторам слід розглянути можливість використання нестандартних налаштувань у тестовій мережі, щоб побачити, чи зможуть вони покращити час відновлення мережі.

Відмовостійкий дизайн - це не лише про надмірність. Важливо розуміти бізнес-потреби організації, а потім використовувати надмірність для створення відмовостійкої мережі.

Стійкість програмного забезпечення - це здатність програми реагувати на проблему з одним зі своїх компонентів під час виконання без переривання роботи. Простої пов'язані зі збоями, спричиненими помилками програми або збоями в інфраструктурі. Адміністратори повинні врешті-решт зупинити програму, щоб застосувати виправлення, оновити версії або впровадити нову функціональність. Простої також можуть бути спричинені пошкодженням даних, відмовою обладнання, збоєм програми або людською помилкою.

Багатьом організаціям важко збалансувати вартість досягнення відмовостійкості програмної інфраструктури з вартістю втрати клієнтів і бізнесу через збої в роботі додатків. Забезпечення високої доступності додатків є складним і дорогим завданням. Чим вищий коефіцієнт доступності будь-якого рішення, тим більша складність і вартість.

Відмовостійке обладнання (найскладніше і найдорожче) - це система, побудована шляхом копіювання всіх критично важливих компонентів на один комп'ютер. Кластерна архітектура - це група з декількох серверів, що працюють як єдина система. Резервне копіювання копіює файли, щоб відновити їх у разі втрати даних.

Cisco Internetwork Operating System (Cisco IOS) на маршрутизаторах і комутаторах має функцію постійної конфігурації. Ця функція дозволяє швидко відновитися після зловмисного або випадкового форматування флеш-пам'яті або видалення оригінального файлу конфігурації. Ця функція зберігає копію файлу образу маршрутизатора IOS, який безпечно працює, і копію поточного файлу конфігурації. Користувачі не можуть видалити ці захищені файли (також відомі як оригінальний завантажувальний набір).

Перша команда, `secure boot-image`, захищає операційний образ; друга команда, `secure boot-config`, захищає файл. Команда `show secure bootset` увімкне збереження образу iOS.

Приклади виконання команд для захисту IOS, показані на рисунку 2.2.

```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:..runcfg-20200218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2020
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2020
Secure archive flash0:..runcfg-20200218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

Рисунок 2.2 – Приклади виконання команд для захисту IOS

Контроль доступу до мережі (NAC) дозволяє доступ до мережі авторизованим користувачам із сумісними системами. Сумісна система - це система, яка відповідає всім вимогам політики організації. Наприклад, ноутбук, підключений до домашньої бездротової локальної мережі, не зможе віддалено підключитися до корпоративної мережі. NAC оцінює пристрої на відповідність мережевим політикам, також ізолює невідповідні системи та керує відновленням невідповідних систем.

Система NAC використовує наявну мережеву інфраструктуру та додаткове програмне забезпечення для впровадження політик безпеки на всіх кінцевих точках. Крім того, пристрої NAC контролюють доступ до мережі, оцінюють відповідність і застосовують політики безпеки. Загальні елементи керування системою NAC включають:

- оновлення антивірусних програм;
- ремонт та оновлення операційної системи;
- інтегрований захист паролем.

Системи виявлення вторгнень (IDS) пасивно відстежують трафік у мережі; пристрої з підтримкою IDS копіюють потоки трафіку і аналізують скопійований трафік, а не пакети, які насправді пересилаються. Працюючи в автономному режимі, IDS порівнює перехоплений потік трафіку з відомими сигнатурами зломисників. В автономному режимі роботи має кілька наслідків:

- IDS працює пасивно;
- пристрій IDS фізично знаходиться в мережі і повинен відбивати трафік, щоб досягти його;
- мережевий трафік не пройде через IDS, якщо його не відбити;
- пасивний означає, що IDS відстежує трафік і повідомляє про нього, але не виконує жодних дій.

Перевагою реплікації трафіку є те, що IDS не впливає на потік пакетів переадресованого трафіку. Недоліком реплікації трафіку є те, що вона не запобігає зломисній одно пакетній атаці, яка досягає своєї мети до того, як IDS встигне

відреагувати на атаку. Для протидії атакам IDS часто потребують допомоги інших мережових пристроїв, таких як маршрутизатори та брандмауери.

Найкращим рішенням є використання пристрою, який може негайно виявити та зупинити атаки. Це функція системи запобігання вторгненням (IPS).

В основі IPS лежить технологія IDS. Однак пристрої IPS працюють в режимі online. Це означає, що весь вхідний і вихідний трафік повинен проходити через IPS для обробки; IPS не дозволяє пакетам потрапляти в захищену частину мережі, поки пакети не будуть проаналізовані. Це дозволяє негайно виявляти і вирішувати мережові проблеми.

IPS відстежує мережовий трафік, він аналізує вміст пакетів і корисне навантаження, щоб виявити більш складні атаки в мережі, які можуть містити шкідливі дані. Деякі системи використовують комбінацію методів виявлення, таких як виявлення вторгнень на основі сигнатур, профілів і протоколів. Такий глибший аналіз дозволяє IPS виявляти, зупиняти і блокувати атаки, які в іншому випадку могли б пройти повз традиційний брандмауер. Якщо пакет надходить до IPS через інтерфейс, довірене джерело або інтерфейс не прийме пакет, доки IPS не проаналізує його. На рисунку 2.3 показано розташування IPS в мережі.

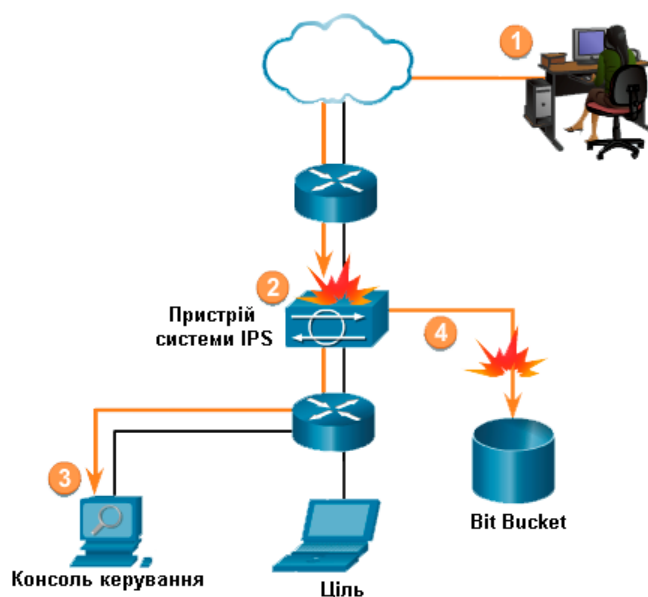


Рисунок 2.3 – Приклад розташування IPS в мережі

Перевага роботи в інтегрованому режимі полягає в тому, що IPS може зупиняти атаки на окремі пакети ще до того, як вони досягнуть цілі. Недоліком є те, що погано налаштований IPS може негативно вплинути на потік пакетів переадресованого трафіку.

Найбільша різниця між IDS та IPS полягає в тому, що IPS реагує негайно і не пропускає шкідливий трафік, в той час як IDS пропускає шкідливий трафік до тих пір, поки проблема не буде вирішена.

NetFlow - це технологія Cisco IOS, яка надає статистику про пакети, що проходять через маршрутизатори та багаторівневі комутатори Cisco. NetFlow є стандартом для збору оперативних даних з мереж.

Організації можуть виявити ознаки атак за допомогою журналів оповіщень системи безпеки та системних звітів:

- блокування облікового запису;
- всі події в базі даних;
- створення та видалення активів;
- зміни конфігурації системи.

Розширений аналіз загроз - це тип даних про події та профілі, які допомагають у моніторингу безпеки та реагуванні на них. Оскільки кіберзлочинці стають все більш витонченими, важливо розуміти як працює шкідливе програмне забезпечення. Підвищена видимість методів атак дозволяє організаціям швидше реагувати на інциденти.

Операційні системи відіграють важливу роль у роботі комп'ютерних систем і є об'єктом багатьох атак. Безпека операційних систем має каскадний вплив на безпеку всієї комп'ютерної системи.

Адміністратори змінюють налаштування за замовчуванням, щоб керувати операційною системою і зробити її більш захищеною від зовнішніх загроз. Цей процес також включає видалення небажаних програм і служб. Ще однією ключовою вимогою для підвищення безпеки операційної системи є застосування патчів та оновлень для вразливостей. Компанії випускають патчі та оновлення для усунення вразливостей і виправлення помилок у своїх продуктах.

Організації повинні організувати свій організаційний підхід до оновлення наступним чином:

- встановити процедури моніторингу інформації, пов'язаної з безпекою;
- оцінювати впровадження оновлень;
- та планувати розгортання виправлень та оновлень додатків;
- встановлювати оновлення за задокументованим планом.

Ще однією важливою вимогою до безпеки операційної системи є виявлення потенційних вразливостей. Цього можна досягти, встановивши базову лінію. Визначення базової лінії дозволяє адміністратору порівняти поточну продуктивність системи з базовою лінією.

До шкідливих програм належать віруси, хробаки, троянські програми, клавіатурні шпигуни, шпигунські та рекламні програми. Всі вони можуть порушувати конфіденційність, викрадати інформацію, пошкоджувати системи, видаляти або пошкоджувати дані.

Для захисту комп'ютера та мобільних пристроїв важливо використовувати надійне антивірусне програмне забезпечення. Існують такі типи програмного забезпечення

- антивірусний захист - програма постійно моніторить наявність вірусів, при виявленні вірусу програма попередить користувача і спробує помістити вірус в карантин або видалити його;
- захист від шкідливих програм - постійно шукає програми, які показують рекламу на вашому комп'ютері;
- захист від фішингу - ця програма блокує IP-адреси відомих фішингових сайтів і попереджає користувачів про підозрілі сайти;
- захист від шпигунських програм - ця програма шукає клавіатурні шпигуни та інші шпигунські пристрої;
- довірені/надійні джерела - програми, які попереджають користувачів про спроби встановити шкідливе програмне забезпечення або шкідливі веб-сайти до того, як вони їх відвідають.

Щоб видалити всі шкідливі програми, може знадобитися кілька різних програм. Одночасно слід запускати лише одну антивірусну програму.

Деякі провідні організації з безпеки, такі як McAfee, Symantec і ESET, пропонують комплексний захист від шкідливого програмного забезпечення для ПК.

Під час роботи в Інтернеті слід остерігатися появи шкідливих і фальшивих антивірусів. Більшість таких шахрайських антивірусів показують рекламу або спливаючі вікна, які виглядають як попереджувальні вікна Windows. Зазвичай це означає, що шкідливе програмне забезпечення заразило комп'ютер, і радить користувачеві видалити його. Клацання в будь-якому місці вікна фактично запускає завантаження та інсталяцію шкідливого програмного забезпечення.

Несумісне програмне забезпечення - це не лише програми, які користувачі встановлюють на комп'ютери помилково, це також може бути програмне забезпечення, яке користувач навмисно встановлює. Таке програмне забезпечення може порушувати політики безпеки, навіть якщо воно не є зловмисним. Цей тип програмного забезпечення може скомпрометувати програмне забезпечення або мережеві служби компанії.

Серверні рішення - це програмне забезпечення, яке працює на локальному комп'ютері та захищає його. Разом з операційною системою це програмне забезпечення допомагає запобігти атакам.

Програмний брандмауер - це програма, яка працює на комп'ютері і дозволяє або забороняє трафік між комп'ютером та іншими підключеними пристроями. Програмний брандмауер застосовує набір правил до трафіку даних, перевіряючи та фільтруючи пакети даних брандмауер Windows є прикладом програмного брандмауера, він встановлюється за замовчуванням в операційних системах Windows як інстальований.

Користувачі можуть контролювати тип даних, що надсилаються на комп'ютери та з них, відкриваючи та блокуючи окремі порти. Брандмауер блокує вхідні та вихідні мережеві з'єднання, якщо не встановлено виняток для відкриття або закриття портів, необхідних для роботи програми.

Користувачі вибирають правило входу і визначають тип трафіку, дозволеного в системі. Налаштування правил входу допомагає захистити систему від небажаного трафіку.

Система виявлення вторгнень на хост (HIDS) - це програмне забезпечення, яке працює на хості та відстежує його на предмет підозрілої активності. Це програмне забезпечення має бути встановлене на всіх серверних або настільних системах, які потребують захисту. HIDS відстежує системні виклики і доступ до файлової системи, щоб переконатися, що ці запити не є результатом зловмисних дій. Програма також може контролювати налаштування системного реєстру. Реєстр містить інформацію про конфігурацію комп'ютера.

На рисунку 2.4 показано кількість днів, необхідних для виявлення та усунення витоку даних за галузями[6].

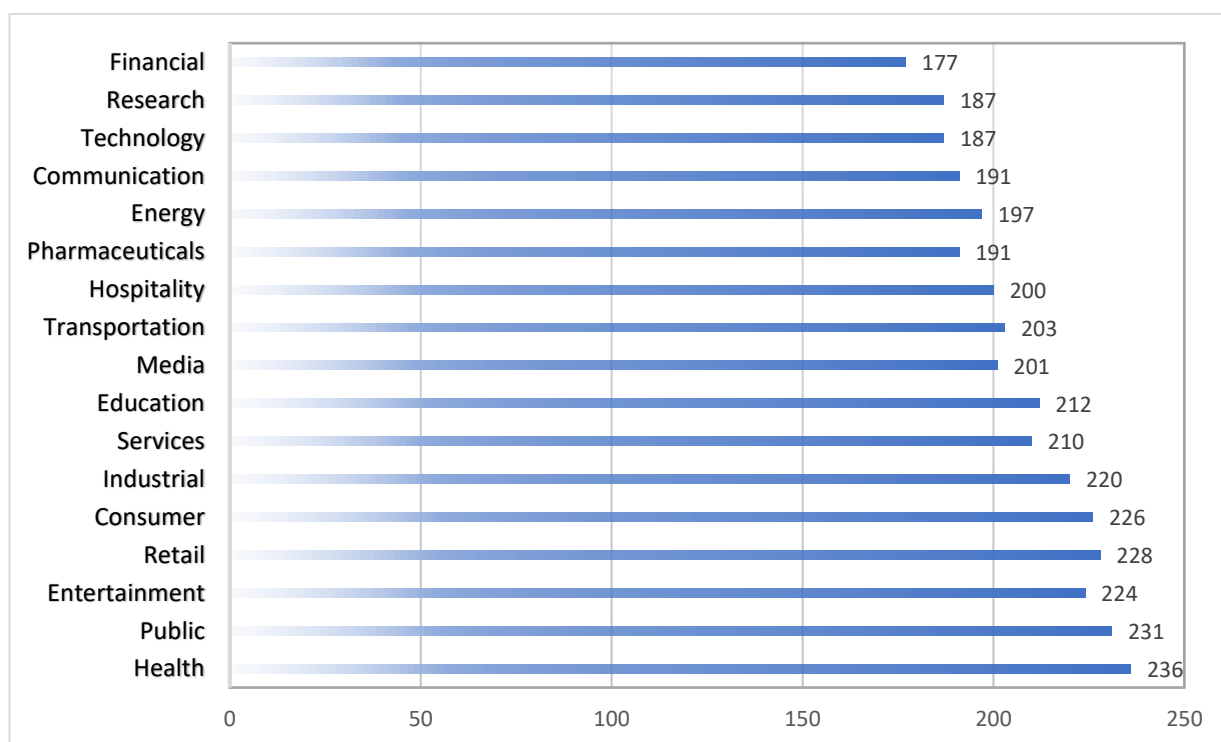


Рисунок 2.4 – Кількість днів, необхідних для виявлення та усунення витоку даних, за галузями

HIDS зберігає всі дані журналу локально. Цей процес вимагає багато ресурсів і може вплинути на продуктивність системи. Системи виявлення вторгнень на

основі хостів не можуть відстежувати мережевий трафік, який не досягає хост-системи, але можуть відстежувати операційну систему і важливі системні процеси, характерні для цього хоста.

Коли ви підключаєтеся до локальної мережі для обміну файлами, зв'язок між комп'ютерами залишається всередині мережі. Комп'ютери від'єднанні від інших мереж і не підключені до Інтернету, тому дані захищені. Для спілкування та обміну ресурсами через незахищені мережі користувачі використовують віртуальні приватні мережі (VPN).

VPN - це приватна мережа, яка з'єднує віддалені сайти і користувачів через загальнодоступну мережу, таку як Інтернет. Найпоширеніший тип VPN - це доступ до корпоративної приватної мережі. VPN з корпоративної приватної мережі до віддаленого користувача - це виділене і безпечне з'єднання, що маршрутизується через Інтернет. Підключаючись до корпоративної приватної мережі, користувачі стають членами цієї мережі і мають доступ до всіх служб і ресурсів так, ніби вони фізично підключені до корпоративної локальної мережі.

Віддалений доступ вимагає наявності VPN-клієнта, встановленого на комп'ютері користувача для створення захищеного з'єднання з приватною мережею компанії. Програмне забезпечення VPN-клієнта шифрує дані і відправляє їх через Інтернет в приватну мережу компанії на VPN-шлюз, який створює, управляє і контролює VPN-з'єднання, також відоме як VPN-тунель.

Операційна система зазвичай містить VPN-клієнт, який користувач налаштовує для підключення до VPN.

Програмне забезпечення для контролю контенту обмежує доступ користувачів до певних типів контенту у веб-браузерах. Програми для контролю вмісту може блокувати веб-сайти, які містять певні типи матеріалів, наприклад, порнографію або суперечливі з релігійної чи політичної точки зору матеріали. Батьки можуть встановити таке програмне забезпечення на комп'ютери, якими користуються їхні діти.

Адміністратори можуть використовувати такі типи фільтрів

- браузерні фільтри через сторонні розширення для браузерів;

- фільтрація листів на основі клієнтських або серверних фільтрів;
- фільтр на стороні клієнта, встановлений на комп'ютері;
- контент-фільтр на базі маршрутизатора, який блокує трафік на вході в мережу;
- фільтрація контенту на основі пристрою та фільтрація на основі маршрутизатора;
- хмарна фільтрація контенту.

Пошукові системи, такі як Google, надають можливість увімкнути фільтри безпеки для блокування небажаних посилань у результатах пошуку.

Віддалений доступ - це поєднання апаратного та програмного забезпечення, яке дозволяє користувачам віддалено отримувати доступ до локальної мережі.

В операційних системах Windows технічні фахівці можуть використовувати віддалений робочий стіл. Віддалений робочий стіл дозволяє технічним фахівцям переглядати та керувати комп'ютерами з віддаленого місця. Дистанційна допомога дозволяє технічним фахівцям допомагати клієнтам вирішувати проблеми віддалено. Це також дозволяє клієнтам бачити на екрані процес ремонту та оновлення в режимі реального часу.

Secure Shell (SSH) - це протокол, який забезпечує зашифровані адміністративні з'єднання з віддаленими пристроями. Для безпечного керування віддаленими з'єднаннями SSH має замінити Telnet, застарілий протокол, який використовує незахищені передачі, що не шифрують дані та параметри автентифікації (ім'я користувача та пароль), які передаються між пристроями, що взаємодіють. SSH - це автентифікація пристроїв. Забезпечує безпечні віддалені з'єднання шляхом шифрування даних (імені користувача та пароля) і даних, що передаються між пристроями, які взаємодіють SSH використовує 22-й порт TCP; Telnet використовує 23-й порт TCP.

Secure Copy Protocol (SCP) безпечно передає комп'ютерні файли між двома віддаленими системами; SCP використовує SSH для передачі даних і забезпечує автентичність і конфіденційність передачі даних.

Кіберзлочинці використовують служби, що працюють в системі, оскільки знають, що на більшості пристроїв запущено більше служб і додатків, ніж їм потрібно. Менеджер аналізує кожну послугу, визначає її необхідність та оцінює ризики. Непотрібні послуги видаляються.

Простий метод, який використовується багатьма адміністраторами для захисту своїх мереж від несанкціонованого доступу, полягає у відключенні всіх невикористовуваних портів на комутаторі. Наприклад, якщо комутатор має 24 порти і 3 з'єднання Fast Ethernet, рекомендується відключити всі невикористовувані порти.

Процес увімкнення та вимкнення портів займає багато часу, але він підвищує безпеку мережі і вартий того.

У більшості мереж з комп'ютерами Windows адміністратор налаштовує Active Directory у домені на Windows Server. Комп'ютери Windows є членами домену. Адміністратори налаштовують політики безпеки домену, які застосовуються до всіх комп'ютерів у мережі. Правила облікових записів автоматично встановлюються під час входу користувача до Windows.

Якщо комп'ютер не належить до домену Active Directory, користувач встановлює політику відповідно до локальної політики безпеки Windows. У всіх версіях Windows, окрім Home Edition, введіть `secpol.msc` у меню "Виконати". Після цього з'явиться інструмент локальної політики безпеки.

Користувачі повинні змінювати свій пароль кожні 90 днів і використовувати новий пароль не менше одного дня. Паролі мають складатися з восьми символів і трьох із чотирьох категорій: верхній регістр, нижній регістр, цифри та символи. Нарешті, користувачі можуть повторно використовувати паролі після 24 унікальних паролів. На рисунку 2.5 показано список найпоширеніших і, отже, найменш безпечних паролів.



Рисунок 2.5 – Найпоширеніші паролі

Політики блокування облікових записів блокують комп'ютери на певний час у разі великої кількості несанкціонованих спроб входу. Наприклад, ця політика дозволяє користувачеві п'ять разів ввести неправильне ім'я користувача або пароль; після п'яти спроб обліковий запис користувача буде заблоковано на 30 хвилин; через 30 хвилин кількість спроб буде обнулено, і користувач зможе знову спробувати увійти в систему.

Додаткові параметри безпеки доступні, якщо розгорнути папку локальних політик аудиторські політики створюють журнали безпеки, які використовуються для моніторингу подій.

Постачання та споживання енергії є ключовими елементами безпеки інформаційних систем. Стабільне електроживлення необхідне для сучасних серверних масивів і сховищ даних. Загальні правила створення ефективної системи електропостачання такі:

- центри обробки даних потребують іншого джерела енергії, ніж інші будівлі;
- резервне джерело живлення: джерело живлення з двома або більше лініями, що живляться від двох або більше підстанцій;
- часто потрібне використання резервної системи електроживлення;
- для належного вимкнення системи має бути доступне джерело безперебійного живлення.

При проектуванні системи електропостачання організаціям необхідно захистити себе від різних проблем.

а) надмірна потужність:

- 1) різкий стрибок: миттєва висока напруга;
- 2) стрибок: тривала висока напруга;

б) втрата потужності:

- 1) переривання: короткочасна втрата потужності;
- 2) блокування: повна втрата потужності;

с) зниження потужності:

- 1) падіння: миттєво низька напруга;
- 2) провал напруги: більш тривале зниження напруги;
- 3) пусковий струм: початковий стрибок потужності.

Віртуальні локальні мережі (VLAN) - забезпечують спосіб групування пристроїв у локальній мережі або на окремих комутаторах. Віртуальні локальні мережі використовують логічні, а не фізичні з'єднання. Окремі порти на комутаторі можуть бути призначені до певної VLAN. Інші порти можна використовувати для фізичного з'єднання комутаторів між собою, щоб трафік можна було перенаправляти між кількома VLAN.

Пристрої в VLAN поведуться так, ніби вони знаходяться у власній незалежній мережі, навіть якщо вони поділяють інфраструктуру з іншими VLAN. VLAN можуть ізолювати групи з конфіденційними даними від інших мереж, зменшуючи ймовірність витоку даних.

Існують різні типи вразливостей та атак на VLAN. Вони можуть включати в себе атаки на VLAN і протоколи "Trunking". Хакери також можуть здійснювати атаки на продуктивність і доступність VLAN. Загальний захист від цих загроз включає моніторинг змін і метрик VLAN, додаткову конфігурацію і регулярне оновлення IOS.

Брандмауер - це апаратне або програмне рішення, яке забезпечує дотримання політик мережевої безпеки. Брандмауери фільтрують несанкціонований або потенційно шкідливий трафік і запобігають вторгненню в мережеву інфраструктуру. Прості брандмауери використовують списки контролю доступу (ACL) для забезпечення базових функцій фільтрації трафіку. Адміністратори використовують списки ACL, щоб зупинити трафік у мережі або дозволити лише певний трафік. ACL - це нерозривний список дозволів або заборон, що застосовується до адрес або протоколів. Списки ACL - це потужний спосіб контролювати те, що входить і виходить з мережі. Брандмауери запобігають атакам на приватні мережі, а загальною метою хакерів є проникнення через захист брандмауерів. Основними загрозами для брандмауерів є крадіжка, злом, віддалений доступ, ACL-атаки або атаки, спрямовані на зниження продуктивності та доступності пристрою. Стандартні заходи безпеки брандмауера включають оновлення фізичного захисту, додаткову конфігурацію, безпечний віддалений доступ і автентифікацію, а також відповідні системні оновлення та виправлення за потреби.

Маршрутизатори є основою Інтернету і сполучною ланкою між різними мережами. Маршрутизатори спілкуються один з одним і визначають найкращий спосіб надсилання трафіку між різними мережами. Маршрутизатори приймають рішення за допомогою протоколів маршрутизації. Маршрутизатори також можуть інтегруватися з іншими сервісами, такими як комутатори та брандмауери. Як наслідок, маршрутизатори є першочерговими цілями для зловмисників. Основними загрозами для мережевих маршрутизаторів є крадіжка, злом, віддалений доступ, атаки на протоколи маршрутизації, такі як RIP/OSPF, або атаки, спрямовані на зниження продуктивності та доступності пристрою. Типові заходи

безпеки для мережевих маршрутизаторів включають підвищену фізичну безпеку, додаткову конфігурацію, використання захищених протоколів маршрутизації з автентифікацією, а також відповідні системні оновлення та патчі, якщо це необхідно.

Кіберзлочинці використовують вразливі мережеві служби для атак на ваш пристрій або використовують їх як частину атаки. Щоб перевірити наявність вразливих мережевих служб, скористайтеся сканером портів, щоб знайти відкриті порти на пристрої. Сканер портів - це програма, яка перевіряє відкриті порти на пристрої, надсилаючи повідомлення на кожен порт і чекаючи на відповідь. Відповідь показує, як використовується порт. Це та сама мета, з якою кіберзлочинці використовують сканери портів. Щоб забезпечити безпеку мережевих сервісів, слід використовувати лише необхідні порти, які можна сканувати.

2.2 Загальний регламент про захист даних

У травні 2018 року Європейський Союз запровадив Загальний регламент про захист даних (GDPR), який передбачає значні штрафи до 4% річного обороту компанії або 20 мільйонів євро (залежно від того, яка сума більша) за порушення регламенту та вимагає прямої згоди користувачів на обробку персональних даних. Запроваджено можливість відкликання дозволу на обробку персональних даних. Суб'єкти даних мають право бути поінформованими протягом 72 годин з моменту порушення даних, право на доступ до своїх даних - суб'єкти даних можуть отримати інформацію від будь-якої організації про те, чи обробляються їхні дані, які дані обробляються і з якою метою. Право на забуття - право на повне видалення даних про особу з систем оператора, право на припинення використання даних, право на повідомлення інших третіх осіб, пов'язаних з даними про особу, про припинення їх використання, а також право на отримання всіх даних про особу, що зберігаються оператором.

GDPR - це правова база, яка встановлює правила збору та обробки персональних даних особами, які проживають в Європейському Союзі (ЄС). GDPR застосовується незалежно від того, де знаходиться веб-сайт, і тому поширюється на всіх європейських відвідувачів, навіть якщо вони не продають конкретні товари або послуги резидентам ЄС.

Згідно з цим регламентом, веб-сайт повинен інформувати вас про дані, зібрані від вас, і ви повинні дати явну згоду на збір інформації, наприклад, натиснувши на кнопку "Я згоден". Ця вимога приблизно описує запит на загальний дозвіл на збір файлів cookie (невеликих файлів, що містять особисту інформацію, наприклад, уподобання користувача).

Веб-сайт також повинен своєчасно інформувати відвідувачів у разі порушення персональних даних, що зберігаються на веб-сайті. Ці вимоги ЄС можуть бути суворішими, ніж ті, що вимагаються в юрисдикції, де знаходиться веб-сайт.

GDPR також вимагає від веб-сайтів не персоналізувати або замінити особистість користувача псевдонімом персональні дані, які вони збирають, щоб додатково захистити вас. Псевдонімізація дозволяє компаніям проводити більш глибокий аналіз даних. Наприклад, можна проводити розрахунки, які виходять за рамки первинної мети зібраних даних для оцінки кредитоспроможності позики, оцінювати середній коефіцієнт заборгованості клієнтів у певному регіоні.

GDPR впливає не лише на збір коштів від клієнтів, але й на їхні дані. Мабуть, найважливіше, що він стосується кадрових записів працівників.

У деяких країнах GDPR зазнав критики. Обов'язок призначати відповідального за захист даних та оцінювати потребу в такій посаді вважається надмірним адміністративним тягарем для деяких компаній. Інші скаржаться на те, що керівні принципи занадто розпливчасті щодо того, як найкраще поводитися з даними співробітників.

Крім того, існують побоювання, що витрати, пов'язані з GDPR, з часом зростатимуть, частково через збільшення потреби в навчанні клієнтів і співробітників щодо загроз захисту даних і заходів протидії. Існують також

сумніви щодо того, чи зможуть органи захисту даних в ЄС та інших країнах реально узгодити свої програми та інтерпретації з регламентом, щоб забезпечити рівні умови для всіх гравців.

2.3 Висновки до розділу 2

Пояснюються технології захисту даних, такі як VPN, ACL, VLAN і HIDS, а також загальний регламент захисту даних - ключовий правовий документ, який визначає підхід ЄС до захисту даних користувачів.

3 ПРОЕКТУВАННЯ БАНКІВСЬКОЇ МЕРЕЖІ

3.1 Налаштування середовища проектування

Для моделювання високопродуктивної банківської мережі було використано сервіси Google Cloud Platform. Це набір хмарних сервісів, які надають інструменти для управління, обчислень, зберігання та аналізу даних. У даній роботі використано компонент Google Compute Engine. Цей компонент дозволяє запускати віртуальні машини на інфраструктурі Google; при створенні екземпляра ВМ можна вибрати її тип, який визначає кількість обчислювальних процесорів і обсяг оперативної пам'яті. Для цілей цього розділу виберемо вісім обчислювальних процесорів і 30 ГБ оперативної пам'яті для комфортної роботи. На рисунку 3.1 показано, як створити екземпляр ВМ у Compute Engine.

Google Cloud Platform EVE-PRO

← Создать экземпляр

Название [?]
eve-ng

Регион [?] Зона [?]
us-east1 (Южная Каролина) us-east1-b

Конфигурация машины [?]

Семейство машин
Стандартные Большой объем памяти
Оптимизированные для вычислений

Экономичные и гибкие типы машин для стандартных рабочих нагрузок.

Series
N1
На базе платформы ЦП Skylake или платформы предыдущего поколения

Тип машины
n1-standard-8 (8 ВЦП, 30 ГБ памяти)

ВЦП	Память
8	30 ГБ

Рисунок 3.1 – Створення екземпляру VM в Compute Engine

Для початку створимо екземпляр у власному образі дистрибутива Ubuntu. Сервіс також дозволяє вибрати тип і ємність завантажувального диска. Тут ми виберемо SSD, який значно швидший за HDD, і встановимо ємність диска у 100 ГБ. На рисунку 3.2 показано початкові налаштування диска.

Завгрузочный диск

Чтобы создать диск, выберите образ или снимок. Вы также можете подключить существующий диск.

Образы ОС Образы приложений Пользовательские образы Снимки Существующие диски

Показать образы из проекта
EVE-PRO

☒ nested-virt-ubuntu

Тип загрузочного диска [?] Размер (ГБ) [?]
Постоянный SSD-диск 100

Рисунок 3.2 – Налаштування завантажувального диску

Після того, як ви створили віртуальну машину, підключіться до неї за допомогою SSH. У командному рядку по черзі виконайте наступні команди, щоб завантажити та оновити лабораторію розробки EVE-NG:

```
wget -O - http://www.eve-ng.net/repo/install-eve.sh | bash -i
apt update
apt upgrade
```

На рисунку 3.3 наведена робота з консоллю в Google Cloud Platform.

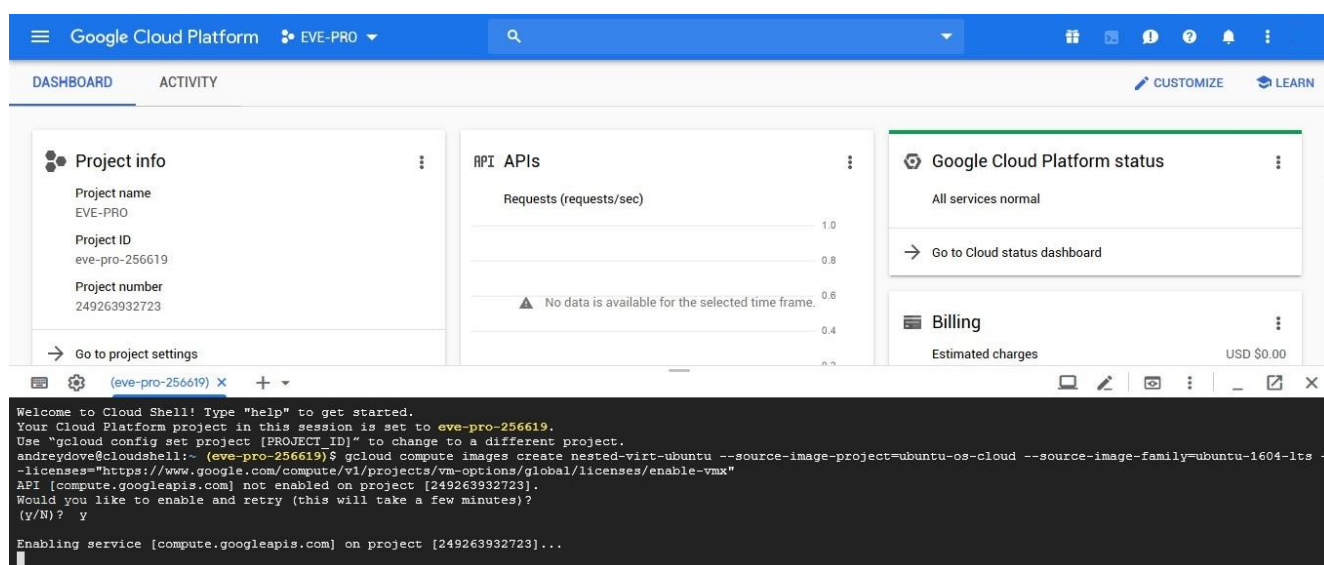


Рисунок 3.3 – Робота з консоллю в Google Cloud Platform

Увійдемо до EVE-NG з логіном (root) і паролем (eve) за замовчуванням і встановить новий логін і пароль. Під час конфігурування залишимо мережеві налаштування, такі як отримання IP-адреси через DHCP, за замовчуванням.

Після налаштування мережі віртуальна машина перезавантажиться. Після того, як EVE-NG знову запрацює, перевіримо, чи підключений віртуальна машина до Інтернету. Для цього виконайте команду `ping` і введіть `www.google.com`. перевіримо чи зв'язок. На рисунку 3.4 показано, що команда `ping` була успішно виконана.

```

root@eve-ng:~# ping www.google.com
PING www.google.com (172.217.16.36) 56(84) bytes of data.
64 bytes from muc03s08-in-f36.1e100.net (172.217.16.36): icmp_seq=1 ttl=128 time=18.3 ms
64 bytes from muc03s08-in-f36.1e100.net (172.217.16.36): icmp_seq=2 ttl=128 time=18.4 ms
64 bytes from muc03s08-in-f36.1e100.net (172.217.16.36): icmp_seq=3 ttl=128 time=18.3 ms
^C
--- www.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 18.302/18.369/18.407/0.120 ms
root@eve-ng:~#

```

Рисунок 3.4 – Виконання команди ping

3.2 Розробка центральної частини мережі банку

Тепер, коли ми налаштували середовище розробки для цього завдання, перейдемо до проектування EVE-NG у браузері. Відкривши браузер, введемо в адресний рядок IP-адресу віртуальної машини EVE, як показано у вікні екземпляра віртуальної машини Computer Engine VM. Відкриється сторінка автентифікації, як показано на зображенні. Якщо автентифікація пройшла успішно, ми будемо авторизовані за допомогою логіна і пароля адміністратора EVE. На рисунку 3.5 показано коротку інформацію про VM.

☒	Назва	Зона	Рекомендація	Используется	Внутренний IP-адрес	Внешний IP-адрес	Подключиться
☒	main	us-east1-b			10.142.0.3 (nic0)	35.211.99.15	SSH

Рисунок 3.5 – Коротка інформація про VM

За допомогою FTP-клієнта FileZilla додаємо потрібні для роботи на віртуальній машині образи обладнання: завантажемо їх до папки `opt/unetlab/addons/qemu/`. Спосіб роботи з FileZilla показано на рисунку 3.6.

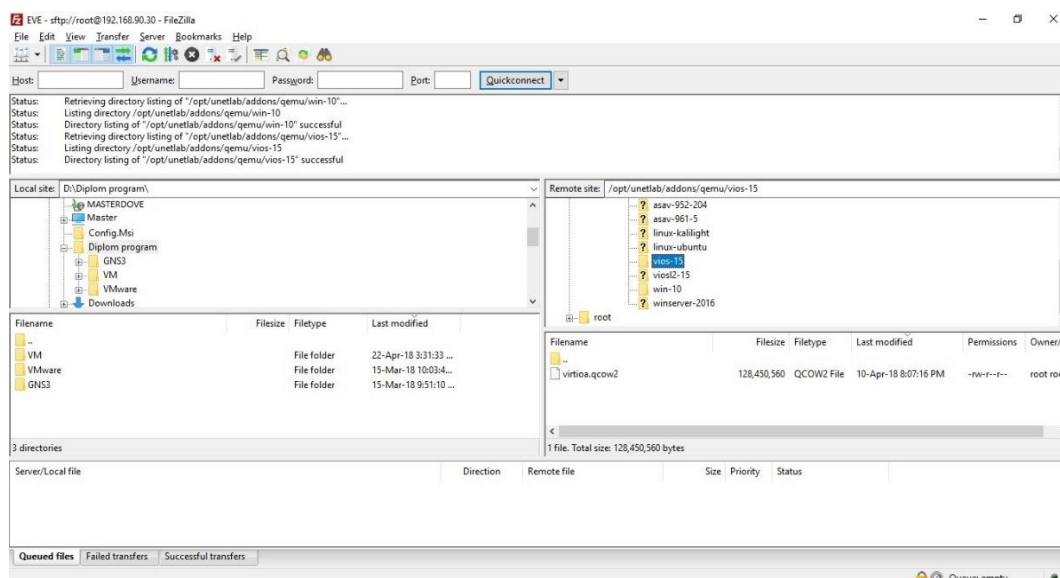


Рисунок 3.6 – Робота з FileZilla

Повернувшись до веб-інтерфейсу EVE, створюємо проект і додаємо необхідні креслення для представлення обладнання. На рисунку 3.7 показано блок-схему банківської мережі. Ця схема складається з двох відділень (Відділення №1 та Відділення №2), одного офісу (Головний офіс) та двох центрів обробки даних (ЦОД №1 та ЦОД №2).

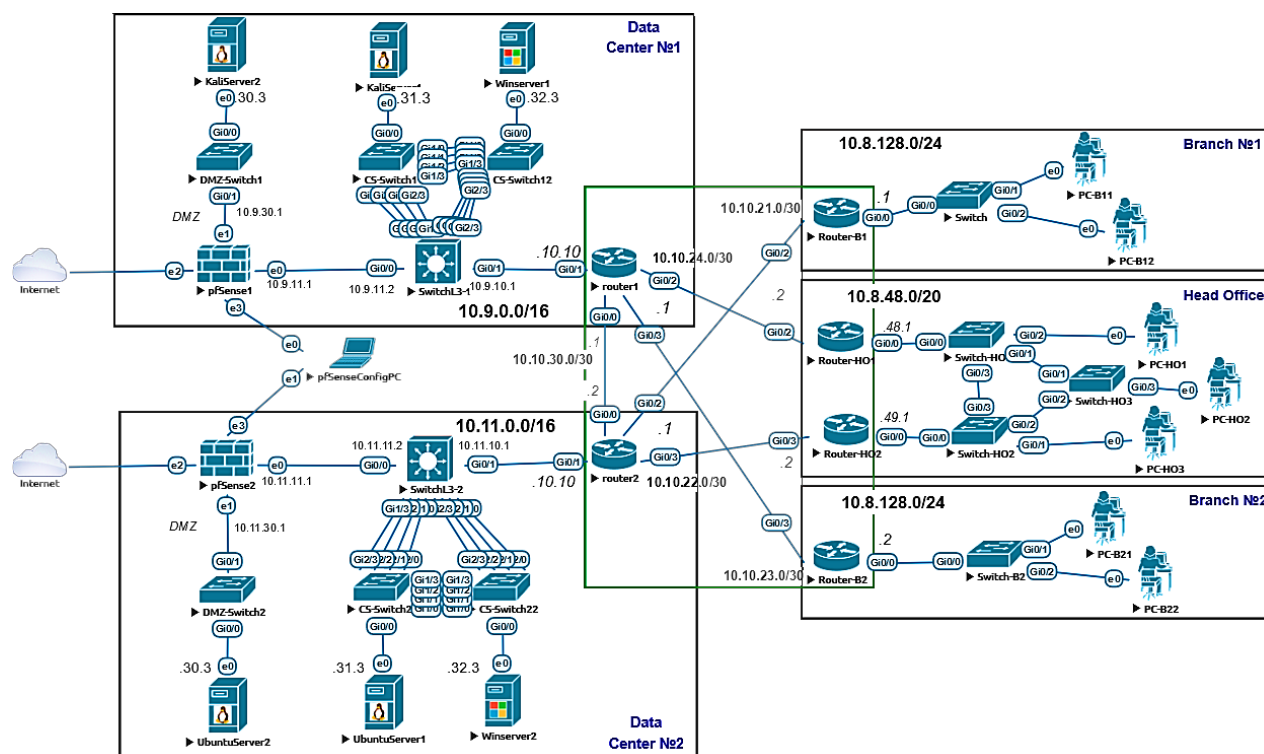


Рисунок 3.7 – Структурна схема мережі банку

Тепер перейдемо до найважливішого - мережевого обладнання та конфігурації хоста. На рисунку 3.8 показано конфігурацію мережевого адаптера для сервера під управлінням Windows, а на рисунку 3.9 - конфігурацію для сервера під управлінням Linux. В обох випадках налаштовано статичну IP-адресу. У таблиці 3.1 наведено статичні адреси пристроїв.

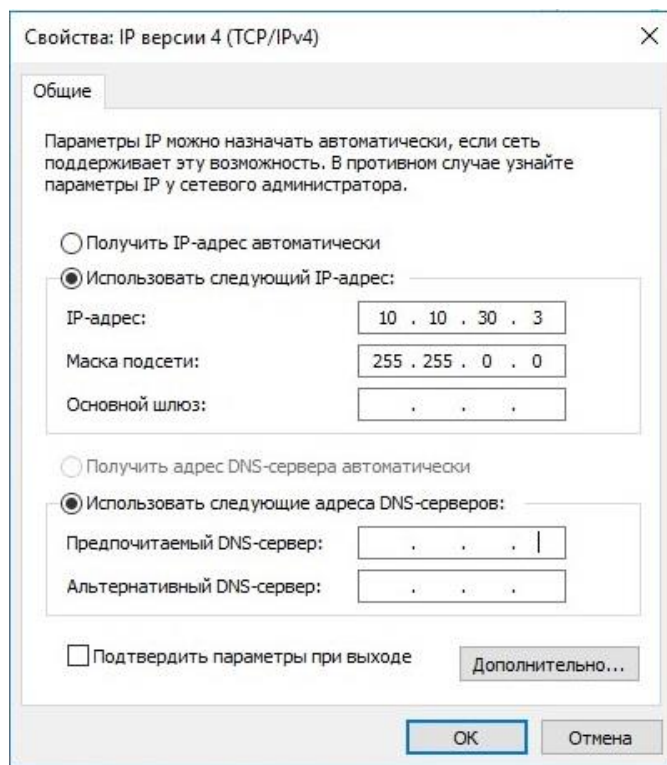


Рисунок 3.8 – Налаштування мережевого адаптера Windows



Рисунок 3.9 – Налаштування мережевого адаптера Linux

Таблиця 3.1 – Статичні адреси пристроїв

Ім'я пристрою	Інтерфейс	ІР-адреса
Winserver1	e0	10.9.32.3
Winserver2	e0	10.11.32.3
KaliServer2	e0	10.9.30.3
KaliServer1	e0	10.9.31.3
UbuntuServer2	e0	10.11.30.3
UbuntuServer1	e0	10.11.31.3
SwitchL3-1	Gi0/0	10.9.11.2
	Gi0/1	10.9.10.1
SwitchL3-2	Gi0/0	10.11.11.2
	Gi0/1	10.11.10.1
router1	Gi0/0	10.10.30.1
	Gi0/1	10.9.10.10
	Gi0/2	10.10.24.1
	Gi0/3	10.10.23.1
router2	Gi0/0	10.10.30.2
	Gi0/1	10.11.10.10
	Gi0/2	10.10.21.1
	Gi0/3	10.10.22.1
Router-B1	Gi0/0	10.8.128.1
	Gi0/2	10.10.21.2
Router-B2	Gi0/0	10.8.128.2
	Gi0/3	10.10.23.2
Router-HO1	Gi0/0	10.8.48.1
	Gi0/2	10.10.24.2
Router-HO2	Gi0/0	10.8.49.1
	Gi0/3	10.10.22.2
pfSense1	G0/0	10.9.11.1
	G0/1	10.9.30.1
pfSense2	G0/0	10.11.11.1
	G0/1	10.11.30.1

Всі сервери налаштовані з логіном і паролем. Під час розробки було встановлено, що дані для автентифікації мають бути однаковими, але в реальності це далеко не завжди можливо. Облікові дані для входу наступні: логін - admin, пароль - Qazxsw123. Пароль для входу в обліковий запис на робочому комп'ютері у відділенні: passw0rd!

Для входу в консоль маршрутизатора введіть команду en. Для входу в режим конфігурації використовуйте команду conf t. Щоб зберегти конфігурацію пристрою після перезавантаження, конфігурація пристрою повинна бути збережена в пам'яті. Це можна зробити за допомогою команди wr mem. Щоб встановити IP-адресу в режимі конфігурації, використовуйте команду int для вибору порту, який потрібно встановити. Потім за допомогою команди ip addr вкажіть IP-адресу і маску, необхідні для цього інтерфейсу. Після цього скористайтеся командою no sh, щоб "підняти" інтерфейс, тобто увімкнути його. На рисунку 3.10 показано приклад налаштування IP-адреси для порту маршрутизатора.

```
Router(config)#int g0/2
Router(config-if)#ip addr 10.10.21.1 255.255.255.252
Router(config-if)#no sh
```

Рисунок 3.10 – Налаштування IP-адреси на порту маршрутизатора

Коротку інформацію про IP-адресу, налаштовану на порту, можна вивести на екран консолі за допомогою команди show ip int br. Приклад команди показано на рисунку 3.11.

```
Router#show ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.10.30.2	YES	manual	up	up
GigabitEthernet0/1	10.11.10.10	YES	manual	up	up
GigabitEthernet0/2	10.10.21.1	YES	manual	up	up
GigabitEthernet0/3	10.10.22.1	YES	manual	up	up

Рисунок 3.11 – Виконання команди show ip int br

У цьому дослідженні використовувалося тільки обладнання Cisco, оскільки компанія має дуже хорошу репутацію на ринку, а її обладнання використовується

найбільшими банками країни. Використання протоколу EIGRP для динамічної маршрутизації між маршрутизаторами, розроблений компанією Cisco для власного обладнання. Цей протокол налаштовується за допомогою команди `router eigrp` в режимі конфігурації. У цій команді необхідно вказати номер автономної системи, який повинен бути однаковим для всіх маршрутизаторів в домені маршрутизації. У цьому прикладі цей номер дорівнює 10. Команда `network` використовується для ввімкнення протоколу на інтерфейсі маршрутизатора в наступній підмережі. На рисунку 3.12 показано налаштування протоколу EIGRP на маршрутизаторі.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 10.10.21.0 255.255.255.252
Router(config-router)#network 10.10.22.0 255.255.255.252
Router(config-router)#network 10.10.30.0 255.255.255.252
Router(config-router)#network 10.11.0.0 255.255.0.0
Router(config-router)#end
```

Рисунок 3.12 – Налаштування протоколу EIGRP

На рисунку 3.13 показано команду `show ip route`. Ця команда покаже мережі, відомі цьому маршрутизатору.

```

S      10.0.0.0/8 is variably subnetted, 28 subnets, 6 masks
S      10.8.0.0/16 [1/0] via 10.9.10.10
S      10.8.48.0/20 is directly connected, GigabitEthernet0/1
D      10.8.48.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.8.49.0/24 [90/3584] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.8.128.0/25 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.8.128.128/25
        [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
C      10.9.10.0/24 is directly connected, GigabitEthernet0/1
L      10.9.10.1/32 is directly connected, GigabitEthernet0/1
C      10.9.11.0/24 is directly connected, GigabitEthernet0/0
L      10.9.11.2/32 is directly connected, GigabitEthernet0/0
S      10.9.30.0/24 [1/0] via 10.9.11.1
D      10.9.31.0/24 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.9.32.0/24 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
S      10.10.0.0/16 [1/0] via 10.9.10.10
D      10.10.21.0/30 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.10.22.0/30 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
S      10.10.23.0/24 [1/0] via 10.9.10.10
D      10.10.23.0/30 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
S      10.10.24.0/24 [1/0] via 10.9.10.10
D      10.10.24.0/30 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
S      10.10.30.0/24 [1/0] via 10.9.10.10
D      10.10.30.0/30 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
S      10.11.0.0/16 is directly connected, GigabitEthernet0/1
D      10.11.10.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.11.11.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.11.30.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.11.31.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.11.32.0/24 [90/3328] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
R      192.168.1.0/24 [120/1] via 10.9.11.1, 00:00:15, GigabitEthernet0/0
```

Рисунок 3.13 – Виконання команди `show ip route`

Для збільшення масштабованості мережі та усунення необхідності вручну встановлювати IP-адреси для хостів у мережі, протокол DHCP використовується для автоматичного призначення адрес на основі конфігурації обладнання. Цей протокол може бути налаштований на сервері або, як в даному випадку, на маршрутизаторі. При налаштуванні протоколу діапазон IP-адрес визначається мережевими командами. Щоб вказати адресу, яка не використовується при призначенні адреси, використовуйте команду `ip dhcp excluded-address`. Використовуйте команду `default-router`, щоб вказати IP-адресу інтерфейсу маршрутизатора, на якому буде запущено протокол. Щоб вказати доменне ім'я мережі, скористайтеся командою `domain-name`. На рисунку 3.14 показано приклад налаштування протоколу DHCP на маршрутизаторі.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp excluded-address 10.8.128.1 10.8.128.149
Router(config)#ip dhcp pool BRANCH2
Router(dhcp-config)#network 10.8.128.0 255.255.255.0
Router(dhcp-config)#default-router 10.8.128.2
Router(dhcp-config)#domain-name branch2.com
Router(dhcp-config)#end
Router#
```

Рисунок 3.14 – Налаштування протоколу DHCP

Ви можете контролювати конфігурацію мережевого адаптера на комп'ютері, ввівши команду `ipconfig` на консолі комп'ютера. Ця команда дозволяє керувати роботою протоколу DHCP. На рисунку 3.15 після запуску команди `ipconfig` видно, що комп'ютер автоматично отримує IP-адресу, маску та адресу шлюзу, оскільки вони не були встановлені вручну, що свідчить про те, що DHCP налаштовано правильно.

```
C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : head_office.com
    Link-local IPv6 Address . . . . . : fe80::f513:1737:d185:2442%7
    IPv4 Address. . . . . : 10.8.49.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.8.49.1
```

Рисунок 3.15 – Виконання команди ipconfig

VLAN використовується для реалізації політик доступу та безпеки, які враховують інтереси різних користувачів. За допомогою команди `vlan` створюємо нову віртуальну мережу і вказуємо її номер. Потім за допомогою команди `name` вказуємо її ім'я. Команда `switchport mode access` на інтерфейсі комутатора вказує на те, що порт знаходиться у режимі доступу, а команда `switchport access vlan` вказує, через який `vlan` відбувається доступ. На Рисунку 3.16 показано приклад конфігурації VLAN на комутаторі.

```
Switch(config)#vlan 10
Switch(config-vlan)#name administration
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name users
Switch(config-vlan)#exit
Switch(config)#int g0/1
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
```

Рисунок 3.16 – Налаштування VLAN

Крім того, між двома вузлами створюється VPN-тунель. Безпека передачі інформації в загальнодоступній мережі забезпечується шифруванням, створюючи канал обміну інформацією, закритий для сторонніх. Технологія VPN дозволяє об'єднати кілька географічно віддалених мереж і окремих клієнтів в одну,

використовуючи неконтрольований канал зв'язку між їх мережами. Між дата-центром і маршрутизаторами філій було створено VPN-тунель. Конфігурація була виконана з використанням групи протоколів IPsec. Використання цієї технології гарантує, що дані передаються в зашифрованому вигляді між місцем зберігання і точкою використання. Це, безсумнівно, важлива деталь мережі банку. Шифрування базується на алгоритмі md5. На рисунку 3.17 показано створення VPN-тунелю між маршрутизаторами за допомогою набору протоколів IPsec.

```
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#au
Router(config-isakmp)#authentication p
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit
Router(config)#crypto isakmp key PASS address 10.10.23.2
Router(config)#crypto ipsec transform-set LAN1 esp-3des esp-md5-hmac
Router(cfg-crypto-trans)#
*Apr 21 13:14:29.745: %PLATFORM-5-SIGNATURE_VERIFIED: Image 'flash0:/vios-advent
erprise9-m' passed code signing verification
Router(cfg-crypto-trans)#mode tunnel
Router(cfg-crypto-trans)#exit
Router(config)#crypto map MAP1 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 10.10.23.2
Router(config-crypto-map)#set tr
Router(config-crypto-map)#set transform-set LAN1
Router(config-crypto-map)#match ad
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#exit
Router(config)#access-list 100 permit gre host 10.10.23.1 host 10.10.23.2
Router(config)#int g0/3
Router(config-if)#cr
Router(config-if)#crypto map MAP1
```

Рисунок 3.17 – Налаштування VPN-тунелю

Списки контролю доступу (ACL) використовуються для обмеження доступу з однієї мережі в іншу. Типові ACL налаштовуються на маршрутизаторах за допомогою стандартної команди `ip access-list`, в кінці команди вказується номер списку, який потрібно створити. Команда `deny` або `permit` з необхідною IP-адресою потім використовується для заборони або дозволу доступу з вказаної мережі до поточної мережі. Створений список потрібно призначити інтерфейсу. Це робиться за допомогою команди `ip access-group`, в якій вказується кількість списків, що призначаються, і спосіб їх роботи: якщо вказано `in`, список фільтрує пакети, що

надходять на інтерфейс; якщо вказано out, список фільтрує пакети, що виходять з нього. На рисунку 3.19 показано приклад створення списку ACL.

```
Router(config)#ip access-list s
Router(config)#ip access-list standard 1
Router(config-std-nacl)#deny 10.8.128.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#int g0/2
Router(config-if)#ip acc
Router(config-if)#ip acce
Router(config-if)#ip access-group 1 in
Router(config-if)#end
```

Рисунок 3.19 – Створення ACL-списку

Статична адресація використовується для явного інформування пристрою про віддалену мережу. Маршрутизатор можна налаштувати за допомогою команди `ip route`. При виконанні цієї команди потрібно вказати мережу, про яку ви хочете, щоб роутер "сповіщав", а також IP-адресу наступного пристрою, підключеного до пристрою, який ви налаштовуєте, і через нього отримати доступ до мережі за замовчуванням. Такий тип маршрутизації використовується в центрах обробки даних. У цьому випадку немає необхідності використовувати динамічну маршрутизацію, оскільки масштабованість не потрібна, оскільки в дата-центрі не завжди з'являється нове обладнання. Статична маршрутизація також є більш безпечною, ніж динамічна. На Рисунку 3.20 показано приклад конфігурації для статичної маршрутизації.

```
SwitchL3-2(config)#ip route 10.11.30.0 255.255.255.0 10.11.11.1
SwitchL3-2(config)#ip route 10.10.30.0 255.255.255.0 10.11.10.10
SwitchL3-2(config)#ip route 10.10.22.0 255.255.255.0 10.11.10.10
SwitchL3-2(config)#ip route 10.10.21.0 255.255.255.0 10.11.10.10
```

Рисунок 3.20 – Налаштування статичної маршрутизації

Щоб забезпечити максимально стабільний зв'язок між сервером і зовнішнім світом та збільшити пропускну здатність між комутаторами, дата-центри конфігуруються з агрегацією каналів. Це забезпечує резервування каналів зв'язку,

тобто, якщо один канал виходить з ладу, інший залишається доступним. Агрегація каналів контролюється протоколом LACP. Під час налаштування портів комутатора два фізичні інтерфейси об'єднуються в один логічний інтерфейс. На рисунку 3.21 показано приклад конфігурації агрегації каналів.

```

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP        Gi1/0(P)   Gi1/1(P)

Switch11#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch11(config)#int range g1/2-3
Switch11(config-if-range)#channel-protocol lacp
Switch11(config-if-range)#channel-group 2 mode active
Creating a port-channel interface Port-channel 2

```

Рисунок 3.21 – Налаштування агрегування каналів комутатора

Якщо занадто багато широкомовних кадрів потрапляє в петлю 2-го рівня між трьома комутаторами і використовує всю смугу пропускання, виникає так званий "широкомовний шторм", що означає, що для корисного трафіку більше немає смуги пропускання і мережа не може бути використана для обміну даними. Протокол STP використовується для уникнення цієї ситуації. Команда `spanning tree cost` в маршрутизаторі повинна використовуватися для визначення вартості інтерфейсу, чим менше значення вартості, тим вищий пріоритет для маршрутизації трафіку на цей порт.

На рисунку 3.23 показано приклад визначення пароля для доступу до консолі маршрутизатора і режиму конфігурування. Команда `service password-encryption` також може використовуватися для шифрування паролів, що зберігаються в пам'яті, і запобігання їх зчитуванню під час фізичного доступу до роутера. На рисунку 3.24 показано, як паролі зберігаються у зашифрованому вигляді у пам'яті пристрою. Під час розгортання всі паролі маршрутизатора встановлено на один і той самий пароль: він має значення `Qazxsw123`.

```

Router(config)#enable secret Qazxsw123
Router(config)#line console 0
Router(config-line)#password Qazxsw123
Router(config-line)#login
Router(config-line)#line vty 0 15
Router(config-line)#password Qazxsw123
Router(config-line)#login
Router(config-line)#exit
Router(config)#service password-encryption
Router(config)#end
Router#

```

Рисунок 3.23 – Налаштування паролів на маршрутизаторі

```
enable secret 5 $l$D3iq$gWcAw/myw7kbbk8MW18kcb1
```

```

line con 0
 password 7 08104D54110A12464058
 login
line aux 0
line vty 0 4
 password 7 0035121C1C481C575D72
 login
 transport input none
line vty 5 15
 password 7 06370E3B545D1E485744
 login
 transport input none

```

Рисунок 3.24 – Вигляд зашифрованих паролів.

Далі налаштуємо pfSense - дистрибутив на базі операційної системи FreeBSD, який використовується як віртуальний брандмауер і маршрутизатор. Він дозволить вам фільтрувати вихідний і вхідний трафік, створювати VPN-мережі типу site-to-site і point-to-point, а також підвищити надійність і відмовостійкість мережі. Основне завдання pfSense - фільтрувати трафік всередині мережі за допомогою функції маршрутизації. Він також може блокувати або обмежувати виклики ззовні на внутрішні хости, дозволяючи при цьому спілкування зсередини назовні. Під час першого запуску pfSense запропонує вам налаштувати vlans і призначити інтерфейси. Призначення інтерфейсу надасть порту адресу локальної мережі за замовчуванням 192.168.1.1. На Рисунку 3.24 показано приклад конфігурації інтерфейсу pfSense.

```

Enter the Optional 6 interface name or 'a' for auto-detection
(vtnet7 vtnet8 vtnet9 a or nothing if finished): vtnet7

Enter the Optional 7 interface name or 'a' for auto-detection
(vtnet8 vtnet9 a or nothing if finished): vtnet8

Enter the Optional 8 interface name or 'a' for auto-detection
(vtnet9 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet3
OPT1 -> vtnet1
OPT2 -> vtnet2
OPT3 -> vtnet4
OPT4 -> vtnet5
OPT5 -> vtnet6
OPT6 -> vtnet7
OPT7 -> vtnet8

```

Рисунок 3.24 – Призначення інтерфейсів pfSense

NAT-трансляція використовується для підтримки публічних IPv4-адрес. Це досягається шляхом використання приватних IPv4-адрес для внутрішньої мережевої комунікації і перетворення їх на публічні адреси лише за необхідності. Додатковою перевагою NAT є підвищений рівень конфіденційності та безпеки мережі. Це пов'язано з тим, що цей механізм приховує внутрішні IPv4-адреси від зовнішніх мереж.

За замовчуванням політика Linux щодо IPv4 вимикає переадресацію IP-адрес і не дозволяє маршрутизаторам діяти як роутери. Щоб увімкнути переадресацію IP-адрес, змініть рядок `net.ipv4.ip_forward = 0` у файлі `/etc/sysctl.conf` з 0 на 1. Щоб зміни набули чинності, виконайте `sysctl -p /etc/sysctl.conf`. Дозволивши переадресацію пакетів через внутрішні інтерфейси, захищені брандмауером, вузли локальної мережі можуть спілкуватися один з одним, але все ще не можуть отримати доступ до зовнішніх вузлів в Інтернеті. Щоб дозволити вузлам локальної мережі з приватними IP-адресами зв'язуватися із зовнішньою мережею, ви повинні налаштувати підміну IP-адрес на брандмауері і приховати вузли локальної мережі під IP-адресою зовнішнього інтерфейсу брандмауера (в даному випадку `pnet9`): `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`.

Це правило використовує таблицю зіставлення пакетів NAT (-t nat) вибирає вбудований ланцюжок POSTROUTING для NAT (-A POSTROUTING) на зовнішньому мережевому інтерфейсі брандмауера. Ланцюжок POSTROUTING дозволяє змінювати пакети, що виходять із зовнішнього пристрою брандмауера. Параметр -j MASQUERADE використовується для приховування приватної IP-адреси хоста за IP-адресою зовнішнього брандмауера/шлюзу.

Правило iptables також може спрямовувати трафік на певний комп'ютер, наприклад, на виділений сервер у демілітаризованій зоні (DMZ), яка є локальною підмережею, призначеною для серверів, відкритих для зовнішніх мереж, таких як Інтернет. Наступне правило дозволяє NAT отримати доступ до таблиці PERROUTING для пересилання пакетів за призначенням, так що вхідні HTTP-запити перенаправляються на виділений сервер за IP-адресою 10.9.30.3 (поза локальною мережею): iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \ --to-destination 10.0.4.2:80 [7].

На рисунку 3.25 наведено результати конфігурації NAT інтерфейсу.

```
default-lease-time 600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

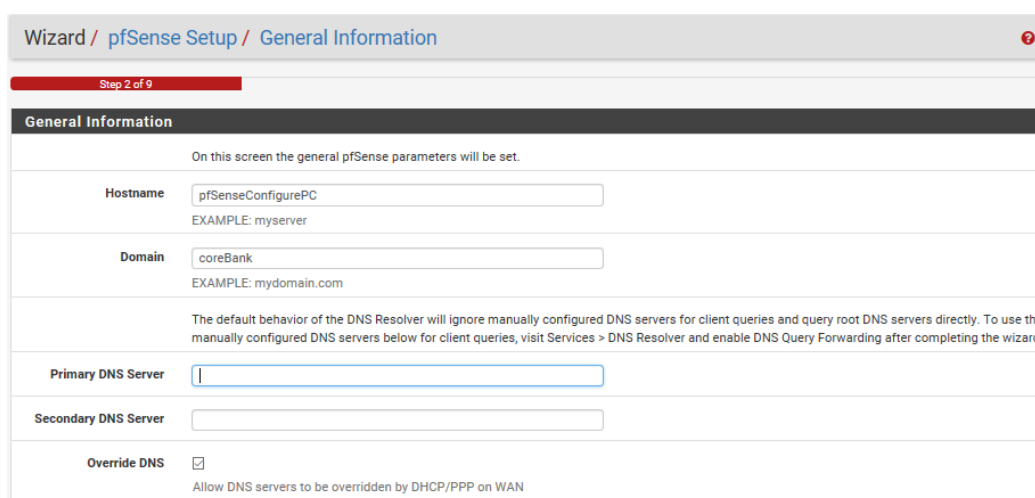
subnet 198.18.18.0 netmask 255.255.255.0 {
    range 198.18.18.50 198.18.18.230;
    interface pnet9;
    default-lease-time 600;
    max-lease-time 7200;
    option domain-name "my.bank.org";
    option domain-name-servers 8.8.8.8;
    option broadcast-address 198.18.18.255;
    option subnet-mask 255.255.255.0;
    option routers 198.18.18.1;
}
```

Рисунок 3.25 – Результати налаштування NAT інтерфейсу

Ця команда перенаправляє всі HTTP-з'єднання із зовнішньої мережі на сервер, ізольований від внутрішньої мережі. Така мережева ізоляція може бути

безпечнішою, ніж дозвіл на HTTP-з'єднання з комп'ютерами у локальній мережі. Якщо HTTP-сервер налаштовано на безпечні з'єднання, порт 443 також має бути пере направлено.

Потім відкриємо браузер і введемо IP-адресу pfSense, 192.168.1.1, в поле пошуку. Відкриється вікно автентифікації pfSense, в якому потрібно буде ввести логін і пароль адміністратора pfSense. Після цього слід виконати початкові кроки налаштування брандмауера. На Рисунку 3.26 показано одне з вікон конфігурації pfSense.



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSenseConfigurePC
EXAMPLE: myserver

Domain: coreBank
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: []

Secondary DNS Server: []

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Рисунок 3.26 – Вікно налаштування pfSense

Після завершення процесу налаштування з'явиться вікно із загальною інформацією про брандмауер. Потім у меню "Інтерфейс" виберіть і встановіть IP-адреси портів OPT1 і OPT2. 10.9.11.1 і 10.9.30.1 відповідно. На рисунку 3.27 показано приклад інформації про систему для pfSense.

The screenshot displays two panels from the pfSense web interface. The left panel, titled 'System Information', provides detailed system data. The right panel, titled 'Netgate Services And Support', shows a status for retrieving support information and a table of network interfaces.

System Information			
Name	pfSenseConfigurePC.coreBank		
User	admin@192.168.1.13 (Local Database)		
System	pfSense Netgate Device ID: 8b80c631c67e61c84da0		
BIOS	Vendor: Bochs Version: Bochs Release Date: Sat Jan 1 2011		
Version	2.4.4-RELEASE-p3 (amd64) built on Wed May 15 18:53:44 EDT 2022 FreeBSD 11.2-RELEASE-p10 The system is on the latest version.		
CPU Type	QEMU Virtual CPU version 1.0 AES-NI CPU Crypto: No		
Kernel PTI	Enabled		
Uptime	00 Hour 25 Minutes 18 Seconds		
Current date/time	Sun Oct 27 0:19:28 EEST 2022		
DNS server(s)	• 127.0.0.1		
Last config change	Sun Oct 27 0:18:20 EEST 2022		
State table size	0% (193/97000) Show states		
MBUF Usage	0% (2786/1000000)		
Load average	0.62, 0.48, 0.37		
CPU usage	12%		

Netgate Services And Support			
Retrieving support information			
Refresh			
Interfaces			
WAN	↑	10Gbase-T <full-duplex>	0.0.0.0
LAN	↑	10Gbase-T <full-duplex>	192.168.1.1

Рисунок 3.27 – Зведена системна інформація pfSense

3.3 Діагностика протоколу EIGRP

Діагностичні можливості протоколу EIGRP не тільки визначають правильність роботи, але й виявляють слабкі місця в маршрутизації та безпеці мережі.

Команда `show ip protocols` може бути використана для відображення конфігурації протоколу EIGRP, як показано на Рисунку 3.28.

```

Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    Soft SIA disabled
    NSF-aware route hold timer is 240
    Router-ID: 10.11.10.10
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    10.10.21.0/30
    10.10.22.0/30
    10.10.30.0/30
    10.11.0.0/16
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.10.22.2             90          00:46:56
    10.10.21.2             90          00:46:58
    10.10.30.1             90          00:46:58
  Distance: internal 90 external 170

```

Рисунок 3.28 – Виконання команди show ip protocols

Результати виконання команди show ip eigrp neighbours, показані на рисунку 3.29, можна використовувати для відображення списку сусідів маршрутизатора.

```

Router-DC2#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)

```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
2	10.10.22.2	Gi0/3	12	00:39:59	218	1308	0	4
1	10.10.21.2	Gi0/2	11	00:40:07	246	1476	0	4
0	10.10.30.1	Gi0/0	12	00:40:08	248	1488	0	13

```

Router-DC2#

```

Рисунок 3.29 – Виконання команди show ip eigrp neighbors

Результат виконання команди show ip eigrp interfaces, показаний на рисунку 3.30, дозволяє побачити, які інтерфейси використовуються eigrp.

```
Router-DC2#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(10)
```

Interface	Peers	Xmit Queue Un/Reliable	PeerQ Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Gi0/2	1	0/0	0/0	246	0/0	50	0
Gi0/3	1	0/0	0/0	218	0/0	50	0
Gi0/0	1	0/0	0/0	248	0/0	50	0
Gi0/1	0	0/0	0/0	0	0/0	0	0

Рисунок 3.30 – Виконання команди show ip eigrp interfaces

Команда show ip eigrp topology, показана на рисунку 3.31, може бути використана для перегляду списку підмереж, відомих цьому маршрутизатору, шлюзів, підключених до цих підмереж, метрик тощо.

```

      via 10.10.30.1 (3072/2816), GigabitEthernet0/0
P 10.8.128.128/25, 1 successors, FD is 3072
      via 10.10.21.2 (3072/2816), GigabitEthernet0/2
P 10.8.49.0/24, 1 successors, FD is 3072
      via 10.10.22.2 (3072/2816), GigabitEthernet0/3
P 10.9.30.0/24, 1 successors, FD is 3072
      via 10.10.30.1 (3072/2816), GigabitEthernet0/0
P 10.10.21.0/30, 1 successors, FD is 2816
      via Connected, GigabitEthernet0/2
P 10.8.128.0/25, 1 successors, FD is 3072
      via 10.10.21.2 (3072/2816), GigabitEthernet0/2
P 10.11.10.0/24, 1 successors, FD is 2816
      via Connected, GigabitEthernet0/1
P 10.8.48.0/24, 1 successors, FD is 3328
      via 10.10.30.1 (3328/3072), GigabitEthernet0/0
```

Рисунок 3.31 – Виконання команди show ip eigrp topology

Команда show eigrp traffic, показана на рисунку 3.32, може бути використана для перегляду статистики передачі пакетів eigrp.

```
Router-DC2#sh ip eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS(10)
  Hellos sent/received: 2768/2077
  Updates sent/received: 15/16
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: 14/6
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 334
  PDM Process ID: 245
  Socket Queue: 0/10000/9/0 (current/max/highest/drops)
  Input Queue: 0/10000/9/0 (current/max/highest/drops)
```

Рисунок 3.32 – Виконання команди show ip eigrp traffic

Протокол EIGRP використовує композитну метрику для визначення кращого шляху до мережі, яка розраховується на основі рівняння (3.1) :

$$M = \left[\left(K_1 \cdot BW + \frac{K_2 \cdot BW}{256 - L} + K_3 \cdot D \right) \cdot \frac{K_5}{K_4 + R} \right] \cdot 256, \quad (3.1)$$

де BW (BandWidth) - безрозмірне значення смуги пропускання, розраховане відповідно до рівняння (3.2):

$$BW = \left[\frac{10^7}{\min(BW_1, \dots, BW_n)} \right], \quad (3.2)$$

де BW_i - значення пропускної здатності i -го інтервалу шляху, Кбіт/с; за замовчуванням дорівнює фізичній пропускній здатності інтерфейсу. Це найнижча пропускна здатність серед усіх інтерфейсів передачі на шляху від джерела до одержувача;

N – кількість ділянок маршруту;

L (Load) - навантаження інтерфейсу (від 1 до 255), вказане для поточного стану інтерфейсу. Воно являє собою найгірше навантаження на канал між джерелом і призначенням і розраховується на основі швидкості передачі пакетів і налаштованої пропускної здатності інтерфейсу;

D (Delay) - сума всіх затримок з'єднання на шляху (в десятках мікросекунд), розрахована за формулою (3.3):

$$D = \sum_{i=1}^N \left[\frac{D_i}{10} \right], \quad (3.3)$$

де D_i – значення затримки для i -ї ділянки маршруту, мкс; встановлені стандартні значення затримок;

N – кількість ділянок маршруту;

R (Reliability) – Надійність інтерфейсу (1-255) вказується для поточного стану інтерфейсу. Вказує на найгірший випадок надійності шляху між відправником та отримувачем на основі повідомлень keep-alive,

K1, K2, K3, K4, K5 – вагові коефіцієнти для розрахунку метрики, які можуть бути 0 або 1

Надійність між мережевого навантаження також може бути використана в розрахунках, але це не рекомендується, оскільки зазвичай призводить до частого перерахунку таблиці топології.

Метод розрахунку метрики (значення k) і номер автономної системи EIGRP сусіднього вузла EIGRP повинні збігатися. Якщо вони не збігаються, маршрутизатор не встановить суміжність.

Значення k за замовчуванням можна змінити за допомогою команди режиму налаштування metric weights маршрутизатора:

```
Router(config-router) # metric weights tos k1 k2 k3 k4 k5
```

Змінювати метричні ваги зазвичай не рекомендується, але важливо узгодити метричні ваги, щоб встановити зв'язок близькості з сусідніми пристроями. Якщо метричні ваги змінено на одному маршрутизаторі, але не на іншому, зв'язок близькості не може бути сформований.

Щоб перевірити значення k, скористайтесь командою show ip protocols. Нижче наведено вивід цієї команди для маршрутизатора R1. Зауважте, що значення k для маршрутизатора R1 встановлено за замовчуванням.

Значення швидкості передачі та затримки можна отримати, виконавши команду show ip int g0/0, результати якої показано на рисунку 3.33 (g0/0 - це інтерфейс, на якому розраховуються вимірювання).

```
Router-DC2#show int g0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is iGbE, address is 5000.0006.0000 (bia 5000.0006.0000)
  Internet address is 10.10.30.2/30
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
```

Рисунок 3.33 – Результат виконання команди show ip int g0/0

Перевіримо значення коефіцієнтів для розрахунку метрики за допомогою команди `show ip protocols`, показано на рисунку 3.34.

```
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(10)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
```

Рисунок 3.34 – Значення коефіцієнтів в результаті виконання `show ip protocols`

Оскільки всі маршрутизатори в цьому дослідженні використовують однакові стандартні коефіцієнти, формула для метрики EIGRP виглядає наступним чином

$$M = (K_1 \cdot BW + K_3 \cdot D) \cdot 256.$$

Виконаємо розрахунки:

$$\begin{aligned} M &= (K_1 \cdot BW + K_3 \cdot D) \cdot 256 = \left(K_1 \cdot \left[\frac{10^7}{\min(BW_1, \dots, BW_n)} \right] + K_3 \cdot \sum_{i=1}^N \left[\frac{D_i}{10} \right] \right) \cdot 256 = \\ &= \left(1 \cdot \left[\frac{10^7}{10^6} \right] + 1 \cdot \frac{20}{10} \right) \cdot 256 = 3072. \end{aligned}$$

Перевірити правильність розрахунку метрики можна за допомогою команди `show ip route`. Дивлячись на рисунок 3.35, можна побачити, що для маршруту, який проходить через два інтерфейси, розрахована вручну метрика дорівнює 3072, а значення адміністративної відстані, яка відповідає значенню внутрішнього маршруту, також дорівнює 90.

```
D      10.9.31.0/24 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
D      10.9.32.0/24 [90/3072] via 10.9.10.10, 00:02:39, GigabitEthernet0/1
```

Рисунок 3.35 – Метрика EIGRP та адміністративна відстань

Розрахуємо метрики для маршруту через чотири інтерфейси, наприклад, маршрут від другого дата-центру до штаб-квартири через перший дата-центр:

$$M = (K_1 \cdot BW + K_3 \cdot D) \cdot 256 = (K_1 \cdot \left[\frac{10^7}{\min(BW_1, \dots, BW_n)} \right] + K_3 \cdot \sum_{i=1}^N \left[\frac{D_i}{10} \right]) \cdot 256 = \\ = \left(1 \cdot \left[\frac{10^7}{10^6} \right] + 1 \cdot \frac{40}{10} \right) \cdot 256 = 3584.$$

Використовуйте команду метричних ваг <TOS> <K1> <K2> <K3> <K4> <K5> для зміни вагових коефіцієнтів EIGRP. Для команди TOS (Type Of Service) діапазон значень 0-8, а K1-K5 - це нові значення коефіцієнтів (діапазон значень для кожного коефіцієнта 0-255). Для шляху від другого дата-центру до головного офісу змінимо коефіцієнти протоколу EIGRP таким чином, щоб всі вони були рівні 1. Це означає, що метрика тепер враховує не тільки значення пропускної здатності і затримки, але також надійність і завантаженість інтерфейсу. Розрахунок метрики виглядає так:

$$M = \left[\left(K_1 \cdot BW + \frac{K_2 \cdot BW}{256-L} + K_3 \cdot D \right) \cdot \frac{K_5}{K_4+R} \right] \cdot 256 = (K_1 \cdot \left[\frac{10^7}{\min(BW_1, \dots, BW_n)} \right] + \frac{K_2 \cdot BW}{256-L} + \\ + K_3 \cdot \sum_{i=1}^N \left[\frac{D_i}{10} \right]) \cdot \frac{K_5}{K_4+R} \cdot 256 = \left(1 \cdot \left[\frac{10^7}{10^6} \right] + \frac{1 \cdot \frac{10^7}{10^6}}{256-1} + 1 \cdot \frac{40}{10} \right) \cdot \frac{1}{1+255} \cdot 256 = 14.$$

Це означає, що зміна коефіцієнтів EIGRP може змінити маршрути в мережі, але важливо пам'ятати, що суміжність не може бути встановлена, якщо коефіцієнти сусідніх маршрутизаторів, на яких налаштовано EIGRP, не однакові.

3.4 Висновки до розділу 3

Таким чином, у цій главі представлено процес розгортання та побудови локальних банківських мереж, включаючи середовище розгортання, динамічну маршрутизацію між маршрутизаторами, NAT для доступу до Інтернету, агрегацію каналів між комутаторами, міжмережеві екрани pfSense, VPN-тунелі та DHCP, а також розглянуто роботу протоколу EIGRP.

4 ДІАГНОСТИКА РОЗРОБЛЕНОЇ МЕРЕЖІ

4.1 Використання протоколу netflow

Моніторинг мережі надає інформацію, яка допомагає адміністраторам ефективно керувати мережею та створювати статистичні звіти про використання мережі для інших фахівців. Активність з'єднань, рівень помилок і стан каналу - це лише деякі з факторів, які допомагають адміністраторам оцінити стан і використання мережі. Збираючи та переглядаючи цю інформацію з плином часу, адміністратори можуть аналізувати та прогнозувати розвиток проекту, а також виявляти та замінювати пошкоджені ділянки до того, як вони вийдуть з ладу.

NetFlow - це власний відкритий протокол, розроблений компанією Cisco для моніторингу мережевого трафіку. NetFlow надає можливість аналізувати мережевий трафік на рівні сеансів, створюючи запис кожної TCP/IP-транзакції.

Архітектура системи базується на датчиках, колекторах та аналізаторах:

- датчики збирають статистику про трафік, що проходить через них. Є сенс розміщувати датчики у "вузлах" мережі, наприклад, на граничних маршрутизаторах сегментів мережі;
- колектор збирає інформацію з датчиків. Отримані дані зберігаються у файлах для подальшої обробки. Різні колектори зберігають дані в різних форматах;

– аналітичні інструменти (системи обробки) зчитують ці файли і створюють звіти у форматі, придатному для читання людиною. Ця система повинна бути сумісною з форматом даних, наданих колектором. У сучасних системах збирачі та аналізатори часто інтегровані в єдину систему.

Щоб увімкнути NetFlow на інтерфейсі, скористайтеся командою `ip route-cache flow`. Як показано на рисунку 4.1, команда `show ip cache verbose flow` може бути використана для отримання детальної інформації про трафік показано на рисунку 4.2; команда `show ip flow interface` може бути використана для відображення списку інтерфейсів, які є сенсорами NetFlow. Ця команда показана на рисунку 4.3. команда `show ip flow top-talkers` може бути використана для отримання інформації про відвідувані інтернет-ресурси за категоріями.

```
Router-DC1(config)#int g0/0
Router-DC1(config-if)#ip route-cache flow
Router-DC1(config-if)#exit
Router-DC1(config)#int g0/2
Router-DC1(config-if)#ip route-cache flow
```

Рисунок 4.1 – Увімкнення NetFlow на інтерфейсах

```
Router-DC1#show ip cache verbose flow
IP packet size distribution (152 total packets):
 1-32  64  96 128 160 192 224 256 288 320 352 384 416 448 480
 .000 .625 .151 .164 .013 .006 .006 .000 .000 .000 .032 .000 .000 .000 .000

 512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
 3 active, 4093 inactive, 13 added
 671 ager polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
 last clearing of statistics never
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
ICMP	5	0.0	5	100	0.0	2.2	15.4
IP-other	5	0.0	4	58	0.0	9.4	15.5
Total:	10	0.0	4	81	0.0	5.8	15.5

SrcIf Port Msk AS	SrcIPAddress	DstIf Port Msk AS	DstIPAddress NextHop	Pr TOS	Flgs B/Pk	Pkts Active
Gi0/0 0000 /0 0	10.10.30.2	Null 0000 /0 0	224.0.0.10 0.0.0.0	58 C0	10	31
					80	131.1
Gi0/1 0000 /0 0	10.9.10.1	Null 0000 /0 0	224.0.0.10 0.0.0.0	58 C0	10	41
					74	170.9
Gi0/2 0000 /0 0	10.10.24.2	Null 0000 /0 0	224.0.0.10 0.0.0.0	58 C0	10	37
					76	153.2

Рисунок 4.2 – Детальна інформація про трафік

```

Router-DC1#show ip flow interface
GigabitEthernet0/0
  ip route-cache flow
  ip flow ingress
GigabitEthernet0/1
  ip route-cache flow
  ip flow ingress
GigabitEthernet0/2
  ip route-cache flow
  ip flow ingress

```

Рисунок 4.3 – Перелік інтерфейсів, які є NetFlow сенсорами

4.2 Інструменти для перевірки мережі та усунення вразливостей

Всі інструменти мережевої безпеки призначені для усунення конкретних загроз системі. Однак кожен інструмент безпеки має свої переваги та недоліки, і лише поєднання їх може забезпечити високий рівень безпеки.

Брандмауери створюють бар'єр проти шкідливого трафіку, але вони не є на 100% безпечними. IDS діють як механізм для моніторингу та спостереження за активністю. Вони стають невід'ємною частиною інфраструктури безпеки в багатьох компаніях. pfSense виконує функції IDS, який також є брандмауером. Аналітики безпеки можуть підключатися до pfSense за допомогою ноутбука і проводити мережеві дослідження за допомогою браузера.

Налаштувавши проксі Squid у pfSense, ви можете отримувати інформацію про веб-сайти, які ви відвідуєте. Звіти показують, хто, коли і як часто відвідував певний сайт - приклади звітів про використання Squid показано на рисунку 4.4 - за місяць.

Звіт по використанню Інтернет, проксі-сервер Squid.

Користувач: 192.168.1.100 (?)
Дата: 09 Лис 2022

№	Відвідані сайти	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Всього
	Всього	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.1	-	-	0.1	-	0.0	0.0	0.0	-	319 287
1	packages.dmd.metaservices.microsoft.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.1	-	-	0.1	-	-	-	-	-	148 177
2	dmd.metaservices.microsoft.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	-	-	0.0	-	0.0	0.0	0.0	-	59 416
3	ctldl.windowsupdate.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	-	-	0.0	-	0.0	0.0	0.0	-	33 660
4	d1lxhc4jvstzrp.cloudfront.net	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	25 043
5	go.microsoft.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	-	-	0.0	-	0.0	0.0	0.0	-	11 088
6	ocsp.digicert.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	0.0	10 575
7	tile-service.weather.microsoft.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	0.0	9 477
8	www.msftconnecttest.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	-	-	0.0	-	-	0.0	-	-	6 190
9	ww42.speedtest.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	5 457
10	ocsp.pki.goog	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	4 221
11	ocsp.msocsp.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	2 572
12	speedtest.net	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	888
13	moodle.zp.edu.ua	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	660
14	speedtest.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	623
15	www.gstatic.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	511
16	netacad.com	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	477
17	aval.ua	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.0	252
	Всього	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0.1	-	-	0.1	-	0.0	0.0	0.0	-	319 287

Рисунок 4.4 – Звіт по використанню Інтернету за місяць

Також можна реєструвати пакети, що проходять через pfSense. Під час налаштування перехоплення пакетів ви можете вибрати, які інтерфейси запускати, які протоколи перехоплювати, а також фільтрацію на основі порту або IP-адреси одержувача. Під час перехоплення ви можете бачити, яка кінцева точка зв'язується з яким протоколом, як контролюється контрольна сума і довжина пакета. На рисунку 4.5 показано приклад відображення інформації про перехоплені пакети.

Packets Captured
<pre> o365filtering.com. NS ns4a.o365filtering.com. ar: ns1a.o365filtering.com. A 157.56.110.11, ns2a.o365filtering.com. A 157.56.116.52, ns3a.o365filtering.com. A 104.47.124.7, ns4a.o365filtering.com. A 157.56.116.52, . OPT UDPsize=4096 DO (208) 23:00:36.879572 76:0a:7e:db:57:ce > 50:00:00:09:00:02, ethertype IPv4 (0x0800), length 102: (tos 0x0, ttl 49, id 51454, offset 0, flags [none], proto UDP (17), length 88) 72.246.46.67.53 > 198.18.18.53.14187: [udp sum ok] 57881*- q: A? a18-67.akam.net. 1/0/1 a18-67.akam.net. A 95.101.36.67 ar: . OPT UDPsize=4096 DO (60) 23:00:36.879618 76:0a:7e:db:57:ce > 50:00:00:09:00:02, ethertype IPv4 (0x0800), length 101: (tos 0x0, ttl 49, id 13506, offset 0, flags [none], proto UDP (17), length 87) 72.246.46.67.53 > 198.18.18.53.25915: [udp sum ok] 54308*- q: A? a4-67.akam.net. 1/0/1 a4-67.akam.net. A 72.246.46.67 ar: . OPT UDPsize=4096 DO (59) 23:00:36.879663 76:0a:7e:db:57:ce > 50:00:00:09:00:02, ethertype IPv4 (0x0800), length 102: (tos 0x0, ttl 49, id 14064, offset 0, flags [none], proto UDP (17), length 88) 23.211.133.67.53 > 198.18.18.53.10570: [udp sum ok] 14445*- q: A? a28-67.akam.net. 1/0/1 a28-67.akam.net. A 95.100.173.67 ar: . OPT UDPsize=4096 DO (60) 23:00:36.880140 76:0a:7e:db:57:ce > 50:00:00:09:00:02, ethertype IPv4 (0x0800), length 228: (tos 0x0, ttl 236, id 52877, offset 0, flags [DF], proto UDP (17), length 214) 157.56.116.52.53 > 198.18.18.53.56793: [udp sum ok] 30721*- q: A? ns2a.o365filtering.com. 1/4/4 ns2a.o365filtering.com. A 157.56.116.52 ns: o365filtering.com. NS ns2a.o365filtering.com., o365filtering.com. NS ns3a.o365filtering.com., o365filtering.com. NS ns4a.o365filtering.com., o365filtering.com. NS ns1a.o365filtering.com. ar: ns1a.o365filtering.com. A 157.56.110.11, ns3a.o365filtering.com. A 104.47.124.7, ns4a.o365filtering.com. A 157.56.116.52, . OPT UDPsize=4096 DO (186) 23:00:36.880337 50:00:00:09:00:02 > 76:0a:7e:db:57:ce, ethertype IPv4 (0x0800), length 94: (tos 0x0, ttl 64, id 39516, offset 0, flags [none], proto UDP (17), length 82) </pre>

Рисунок 4.5 – Інформація про перехоплені пакети

pfSense постачається з попередньо встановленим Snort, безкоштовним пакетом системи виявлення та запобігання мережевим вторгненням. Цей IPS/IDS може виконувати перехоплення пакетів і аналіз трафіку в IP-мережах у режимі реального часу. Приклад конфігурації інтерфейсу Snort, що використовується для моніторингу трафіку, показано на рисунку 4.6.

The screenshot displays the 'Edit Interface' configuration page for a Snort instance in pfSense. The breadcrumb trail at the top reads 'Services / Snort / Edit Interface / None'. The page is divided into three main sections: 'General Settings', 'Alert Settings', and 'Detection Performance Settings'.

General Settings:

- Enable:** A checkbox labeled 'Enable interface' is checked.
- Interface:** A dropdown menu is set to 'WAN (vtnet2)'. Below it, a note says 'Choose the interface where this Snort instance will inspect traffic.'
- Description:** A text field contains 'WAN'. Below it, a note says 'Enter a meaningful description here for your reference.'
- Snap Length:** A text field contains '1518'. Below it, a note says 'Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.'

Alert Settings:

- Send Alerts to System Log:** A checkbox is unchecked. A note below it says 'Snort will send Alerts to the firewall's system log. Default is Not Checked.'
- Block Offenders:** A checkbox is unchecked. A note below it says 'Checking this option will automatically block hosts that generate a Snort alert.'

Detection Performance Settings:

This section is currently empty.

Рисунок 4.6 – Приклад налаштування інтерфейсу Snort

pfSense дозволяє виконувати трасування маршрутів, щоб зрозуміти потік трафіку у вашій мережі. Для цього скористайтеся функцією traceroute, показаною на рисунку 4.7.

The screenshot shows a web interface for Traceroute. At the top, it says "Diagnostics / Traceroute". Below this is a "Traceroute" section with several input fields and checkboxes:

- Hostname:** 10.9.30.3
- IP Protocol:** IPv4 (dropdown menu)
- Source Address:** LAN (dropdown menu)
- Maximum number of hops:** 18 (dropdown menu)
- Reverse Address Lookup:** ☐ (checkbox)
- Use ICMP:** ☐ (checkbox)

Below these fields is a blue button labeled "Traceroute". Below the button is a "Results" section showing the output of the traceroute:

Hop	IP Address	RTT 1	RTT 2	RTT 3
1	10.9.30.3	4.211 ms	3.354 ms	4.912 ms

Рисунок 4.7 – Робота з Traceroute

Операційна система KaliLinux дозволяє проводити діагностику мережі за допомогою деяких вбудованих інструментів. Наприклад, за допомогою команди `nmap` у терміналі операційної системи можна побачити, які порти відкриті на певному комп'ютері. Це дозволяє визначити, які невикористовувані порти відкриті, а отже, вразливі. На рисунку 4.8 показано приклад команди `nmap`.

```
admin@osboxes:~$ nmap 10.9.30.1

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-09 17:41 EST
Nmap scan report for 10.9.30.1
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
```

Рисунок 4.8 – Виконання команди `nmap`

За допомогою одного з інструментів цієї операційної системи також було виявлено, що DHCP, налаштований на маршрутизаторі філії, вразливий до

спуфінгу (маніпуляції з даними та видавання себе за іншого з метою отримання несанкціонованих переваг). Щоб вирішити цю проблему, на маршрутизаторі необхідно налаштувати DHCP snooping (процес моніторингу мережевого трафіку IGMP). Як показано на рисунку 4.9, команда `ip dhcp snooping` може бути використана для ввімкнення snooping на певному vlan. Команда `ip dhcp snooping limit rate` використовується для обмеження кількості DHCP-пакетів на секунду на порт, і якщо вказане значення буде перевищено, то він буде вимкнений.

Результат виконання команди `show dhcp snooping` показано на рисунку 4.10. За допомогою цієї команди можна переглянути конфігурацію snooping; для перегляду бази даних DHCP скористайтеся командою `show ip dhcp binding`.

```
Switch-B1(config)#ip dhcp snooping
Switch-B1(config)#ip dhcp snooping vlan 10 20
Switch-B1(config)#int g0/1
Switch-B1(config-if)#ip dhcp snooping trust
Switch-B1(config-if)#ip dhcp snooping limit rate 100
Switch-B1(config-if)#end
```

Рисунок 4.9 – Виконання команди `ip dhcp snooping`

```
Switch-B1#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleanig is disabled
DHCP snooping is configured on following VLANs:
10-20
DHCP snooping is operational on following VLANs:
10-20
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 5000.0025.0000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
```

Interface	Trusted	Allow option	Rate limit (pps)
GigabitEthernet0/1	yes	yes	100

Custom circuit-ids:

Рисунок 4.10 – Результат виконання команди `show dhcp snooping`

4.3 Висновки до розділу 4

Таким чином, в цьому розділі описується робота протоколу NETFLOW, моделюється і досліджується аномальна і шкідлива активність в мережі, розгорнута різними способами, а також виправляються вразливості і баги на основі емпіричних даних.

ВИСНОВКИ

Тому під час підготовки цієї дипломної роботи було поставлено завдання розгорнути центральну комп'ютерну мережу банку разом з його відділеннями, проаналізувати аномальні дії в цій мережі та усунути вразливості. Результати аналізу.

У теоретичній частині бакалаврської роботи було досліджено банківські інформаційні процеси, сучасні загрози безпеці комп'ютерних мереж у світі, види кібератак, технології хмарних обчислень та їх вразливості, способи забезпечення відмовостійкості мережі, безпеку операційної системи, різні технології комп'ютерних мереж та нормативно-правові акти щодо захисту даних в цілому.

У практичній частині дипломної роботи описано розгортання магістралі та гілок комп'ютерної мережі банку, моделювання та дослідження аномальної та зловмисної активності в мережі та нейтралізація вразливостей досліджуваної мережі на основі емпіричних даних.

Загалом, для досягнення мети роботи зроблено наступне

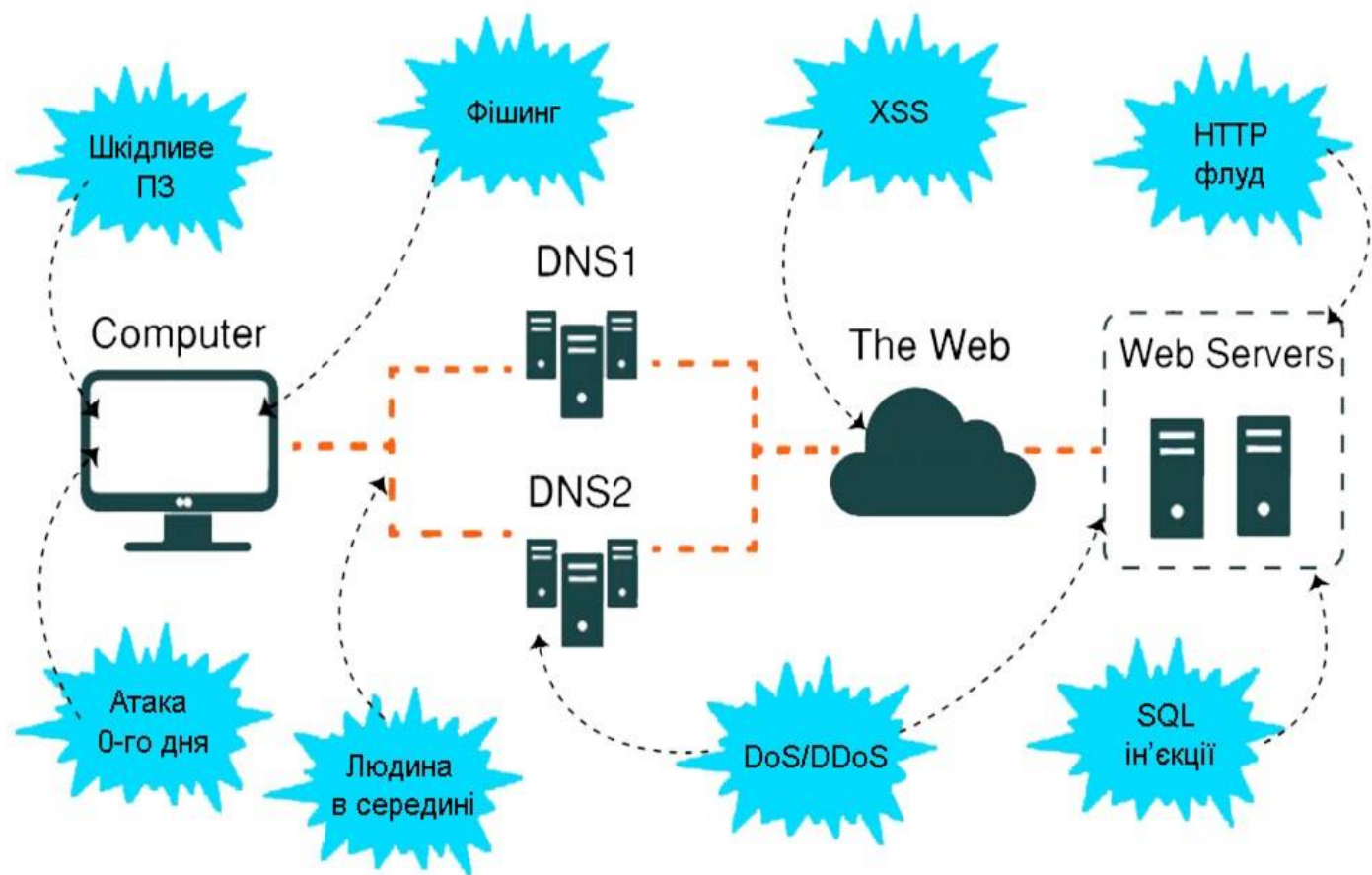
- розвинути навички самостійної роботи, закріпити та поглибити теоретичні та практичні знання за фахом;
- набуті вміння систематизувати та аналізувати літературу з досліджуваної теми;
- навчитися формулювати проблеми та обирати підходи і методи їх вирішення;
- систематизувати, закріпити та поглибити теоретичні та практичні знання у спеціалізованій галузі комп'ютерної інженерії та застосувати їх для вирішення конкретних завдань.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. IBM: Cost of a Data Breach Report 2019. Computer fraud & security. 2019. Vol. 2019, no. 8. P. 21. URL: <https://www.ibm.com/downloads/cas/RDEQK07R>.
2. Ланцюжок Kill Chain: від моделювання до проектування захищеного периметра. Інформаційна безпека. URL: <https://ipiskunov.blogspot.com/2016/11/kill-chain.html>
3. Кібербезпека-загрози, вразливості і атаки - Mind Map. Mind mapping, concept mapping, outlining and Gantt Charts. URL: <https://www.mindomo.com/ru/mindmap/mind-map-195edc656ae98deff2305cda39a611f0>
4. Найпопулярніші види кібератак у 2021 році. Громадська онлайн платформа | SPILNO. URL: <https://spilno.org/news/naipopulyarnishi-vydy-kiberatak-u-2021-rotsi>
5. Smith R. Global cyber losses expected to hit \$6 trillion by 2021 – report. UK Insurance News for Professionals | Insurance Business UK. URL: <https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-losses-expected-to-hit-6-trillion-by-2021--report-177552.aspx>
6. IBM: Cost of a Data Breach Report 2019. Computer fraud & security. 2019. Vol. 2019, no. 8. P. 54. URL: <https://www.ibm.com/downloads/cas/RDEQK07R>.
7. Налаштування інтернет-шлюзу з NAT та port forwarding на centos 7 - INFOIT.COM.UA. URL: <https://infoit.com.ua/linux/nastrojka-internet-shlyuza-s-nat-i-port-forwarding-na-centos-7/>
8. Учасники проектів Вікімедіа. EIGRP – Вікіпедія. Вікіпедія. URL: <https://uk.wikipedia.org/wiki/EIGRP>
9. Як настроїти гнучкий моніторинг трафіку за допомогою Flexible NetFlow на маршрутизаторі Cisco. Блог Університету SEDICOMM. URL: <https://blog.sedicom.com/2021/09/03/kak-nastroit-gibkij-monitoring-trafika-s-pomoshhyu-flexible-netflow-na-marshrutizatore-cisco/>

10. Безпека інформаційно-комунікаційних систем М.В. Грайворонський, О.М. Новіков – К. : Вид.група ВHV, 2009. 698 с

Основні типи кібератак



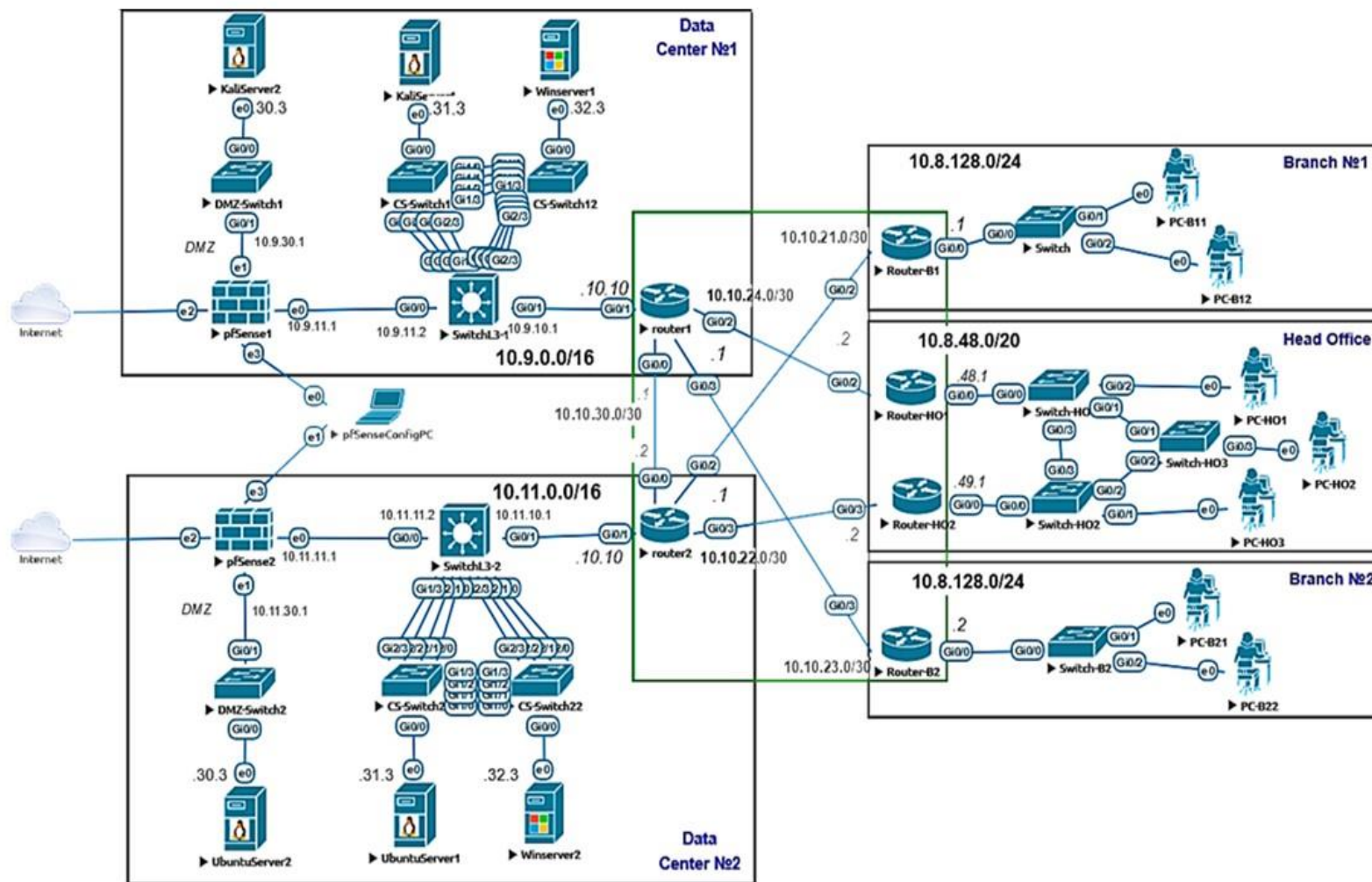
					13.02070849.00008 ПЛІ				
					Розробка центральної частини комп'ютерної мережі банку Основні типи кібератак	Літ.		Маса	Масштаб
Зам.	Лист	№ докум.	Підп.	Дата					
Розроб.		Казанський О.А.	log						
Перев.		Скрупський С.Ю.	SM						
Т.контр.									
						Лист 1		Листів 1	
Н.контр.		Щербак Н.В.	Щ			НУ «Запорізька політехніка» KHT-519			
Затвердж.		Кудерметов Р.К.	РК						

Куб кібербезпеки



					13.02070849.00008 ПЛ2				
					Розробка центральної частини комп'ютерної мережі банку <i>Куб кібербезпеки</i>	Літ.		Маса	Масштаб
Зам.	Лист	№ докум.	Підп.	Дата					
Розроб.		Казанський О.А.	<i>О.А. Казанський</i>						
Перев.		Скрупський С.Ю.	<i>С.Ю. Скрупський</i>						
Т.контр.						Лист 1		Листів 1	
					НУ «Запорізька політехніка» <i>КНТ-519</i>				
Н.контр.		Щербак Н.В.	<i>Н.В. Щербак</i>						
Затвердж.		Кудерметов Р.К.	<i>Р.К. Кудерметов</i>						

Структурна схема мережі банку



					13.02070849.00008 ПЛЗ				
					Розробка центральної частини комп'ютерної мережі банку <i>Структурна схема мережі банку</i>	Літ.		Маса	Масштаб
Зам.	Лист	№ докум.	Підп.	Дата					
Розроб.		Казанський О.А.							
Перев.		Скруський С.Ю.							
Т.контр.						Лист 1		Листів 1	
						НУ «Запорізька політехніка» KHT-519			
Н.контр.		Щербак Н.В.							
Затвердж.		Кудерметов Р.К.							