МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК.
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Метод забезпечення кібербезпеки в телекомунікаційних мережах» .

Виконавець: _____ Микита КРИВОЛАПОВ
(підпис)

Керівник: _____ Юлія ПЕТРОВА
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Андріан ЯВНЮК
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Віктор ГНАТЮК
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Криволапова Микити Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи (проекту): «Метод забезпечення кібербезпеки в телекомунікаційних мережах»
затверджена наказом ректора від «28» вересня 2023 р. №1965/ст
2. Термін виконання роботи: з 02.10.2023 р. по 31.12.2023 р.
3. Вихідні дані до роботи: FIREWALL, IDS/IPS, ENCRYPTION, VLAN, ROUTING PROTOCOLS, NETWORK TOPOLOGY, DDOS MITIGATION, INTRUSION DETECTION, ACCESS CONTROL,
4. Зміст пояснювальної записки: Розділ 1. Ознайомлення з основними принципами кібербезпеки телекомунікаційних мереж, Розділ 2. Аналіз основних загроз кібербезпеці телекомунікаційних мереж, Розділ 3. Розробка стратегій захисту телекомунікаційних систем від кібератак, Висновки
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: Топологічна схема мережі, Діаграми загроз та вразливостей, Схеми системи кіберзахисту, Скріншоти інтерфейсів ПЗ, Схеми стратегій захисту, Графіки та діаграми трафіку, Схеми сценаріїв кібератак, Ілюстрації заходів безпеки, Графіки ефективності та покращень

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	02.10.2023-04.10.2023	Виконано
2	Вступ	05.10.2023-08.10.2023	Виконано
3	Ознайомлення з основними принципами кібербезпеки телекомунікаційних мереж	09.10.2023-22.10.2023	Виконано
4	Аналіз основних загроз кібербезпеці телекомунікаційних мереж	23.10.2023-05.11.2023	Виконано
5	Розробка стратегій захисту телекомунікаційних систем від кібератак	06.11.2023-30.11.2023	Виконано
6	Охорона праці	01.12.2023-06.12.2023	Виконано
7	Охорона навколишнього середовища	07.12.2023-17.12.2023	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	18.12.2023-31.12.2023	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., професор Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.б.н., доц. Андріан ЯВНЮК		

8. Дата видачі завдання: “29" вересня 2023 р.

Керівник кваліфікаційної роботи _____ Юлія ПЕТРОВА
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Микита КРИВОЛАПОВ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Метод забезпечення кібербезпеки в телекомунікаційних мережах» містить 92 сторінки, 17 рисунків , 1 таблиць, 17 використаних джерел.

Телекомунікаційні мережі, Кібербезпека, Стратегії захисту, Топологія мережі, Ефективність, Тестування безпеки, Системи кіберзахисту, Проектування мереж, Наступне покоління, Рекомендації, Аналіз загроз, Інфраструктура телекомунікацій, Стійкість до кібератак, Стандарти безпеки, Аудит безпеки, Трафік мережі, Вразливості систем, Літературний огляд, Сучасні технологіїДокументація безпеки.

Об’єкт дослідження – телекомунікаційна мережа для розробки та впровадження стратегій кіберзахисту

Предмет дослідження – процеси та методи забезпечення кібербезпеки в телекомунікаційних мережах.

Мета дипломної роботи – розробка та впровадження ефективних стратегій кіберзахисту для телекомунікаційних мереж з метою запобігання кіберзагроз та забезпечення стійкості системи.

Метод дослідження – аналіз літературних джерел, аудит телекомунікаційної інфраструктури, тестування кібербезпеки, та розробку та впровадження стратегій захисту.

Матеріали дипломної роботи рекомендується використовувати при проектуванні мереж наступного покоління.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

1. **IPv4:** Інтернет-протокол четвертої версії.
2. **IPv6:** Інтернет-протокол шостої версії.
3. **PyCharm:** Інтегроване середовище розробки для мови програмування Python.
4. **Suricata:** Система виявлення і запобігання вторгнень (IDS/IPS).
5. **КПО:** Природне освітлення.
6. **МФУ:** Мультіфункціональний пристрій.
7. **ДБА:** Децибел ампер.
8. **НАПБ:** Нормативи пожежної безпеки.
9. **ВП-5:** Портативний порошковий вогнегасник.
10. **SSL:** Протокол безпеки, що забезпечує шифрування ідентифікаційних даних в Інтернеті.
11. **TLS:** Протокол транспортного рівня.
12. **БВПП:** Багатофункціональний вимірювальний прилад.
13. **МІОД:** Максимально допустимий рівень шуму.
14. **ДМВП:** Допустимий рівень вібрації приміщення.
15. **IDS**: Система виявлення вторгнень
16. **IPS**: Система запобігання вторгнень.
17. **SSL**: Протокол безпеки рівня сесій
18. **TLS**: Протокол транспортного рівня безпеки

ВСТУП

Актуальність теми. Забезпечення кібербезпеки в телекомунікаційних мережах стає критичним завданням у зв'язку з постійним розвитком цифрових технологій та зростанням обсягів обміну даними. З кожним новим етапом розвитку телекомунікацій виникають нові виклики та загрози, що потребують ефективних та інноваційних методів захисту.

Актуальність даної теми зумовлена не лише зростанням кількості кіберзагроз, але й розвитком нових технологій, таких як Інтернет речей (IoT), 5G, хмарні обчислення та інші. Це ставить під загрозу безпеку та конфіденційність інформації, а також функціонування критичних інфраструктур.

Розробка методів забезпечення кібербезпеки в телекомунікаційних мережах є актуальним завданням, оскільки вона спрямована на вдосконалення та адаптацію захисних стратегій до сучасних викликів. Постійний розвиток кіберзлочинності вимагає вдосконалення методів захисту для забезпечення стійкості та безпеки телекомунікаційних систем, які відіграють критичну роль у всіх аспектах нашого життя

Мета і завдання дослідження - Дослідження присвячене розробці ефективних методів забезпечення кібербезпеки в телекомунікаційних мережах. Метою є створення стратегії захисту від кібератак для забезпечення високої надійності, конфіденційності та доступності інфраструктури телекомунікацій. Завдання включають комплексний аналіз загроз, вразливостей, розробку стратегій захисту, використання стандартів, дослідження технологічних рішень та розробку конкретних рекомендацій. Завершеним дослідженням буде звіт із зазначенням настанов для подальшого вдосконалення кібербезпеки в телекомунікаціях.

Об’єкт дослідження – технічні та безпекові аспекти телекомунікаційних мереж з метою розробки стратегій захисту від кібератак.

Предмет дослідження – процеси та системи забезпечення кібербезпеки в телекомунікаційних мережах, з фокусом на їхній ефективності та захисті від потенційних кіберзагроз.

Апробація отриманих результатів. Отримані результати можуть бути використані для розробки і впровадження нових методів захисту інформації в телекомунікаційних мережах

РОЗДІЛ 1 ОЗНАЙОМЛЕННЯ З ОСНОВНИМИ ПРИНЦИПАМИ КІБЕРБЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1. Кібербезпека: Вступ та Основні Концепції

Кібербезпека є важливою галуззю, яка вивчає та реалізує заходи для захисту інформаційних систем від потенційних загроз та несанкціонованого доступу. Заснована на основних концепціях конфіденційності, цілісності та доступності, кібербезпека спрямована на забезпечення високого рівня безпеки в цифровому просторі.

Перша ключова концепція – конфіденційність – ставить перед собою завдання гарантувати, що лише авторизовані користувачі отримують доступ до конфіденційної інформації. Це важливо для захисту від несанкціонованого витоку чутливих даних та збереження їх конфіденційності.

Друга концепція – цілісність – націлена на забезпечення того, що дані залишаються недоторканими та не піддаються несанкціонованій зміні. Це важливо для гарантування надійності інформації та попередження будь-яких спроб її неправомірної модифікації.

Третя концепція – доступність – визначає готовність системи витримувати атаки та забезпечувати неперервний доступ до інформації. Це означає стійкість системи до різноманітних загроз і здатність швидко відновлювати роботу після можливих інцидентів.

Кібербезпека, будучи комплексною областю, намагається забезпечити баланс між цими концепціями, забезпечуючи повноцінний захист інформаційних систем в умовах сучасного цифрового середовища.

Усі країни мають політику регулювання телекомунікаційних операцій, а також політику щодо забезпечити розумне використання телекомунікаційних платформ на благо своїх суспільств і урядів і оператори/компанії зв’язку. Однак різниця полягає в тому, наскільки ефективні ці політики і наскільки ефективно та результативно

реалізуються ці політики. Ці відмінності створити простір для злочинців для вчинення шахрайства за допомогою телекомунікаційних платформ, використовуючи слабкі місця в політиці або відсутність бажання впроваджувати політику з боку регуляторів. Однак телекомунікаційне шахрайство здебільшого розглядається в ширшому контексті як кіберзлочин правильно розміщене, у більшості випадків ускладнює його виокремлення та вирішення цього питання як окремої проблеми публічних дискусіях і в літературі. Знову ж таки, більшість шахрайств, вчинених шахраями або кіберзлочинці подібні до тих, що вчиняються в телекомунікаційній галузі, але з незначною мірою варіації.

У телекомунікаційній галузі компанії також беруть участь в обмані урядів і держав. Це робиться шляхом ухилення від сплати податків [33]. Також беруть участь постачальники телекомунікаційних послуг у слеммінгу (коли телефонні оператори незаконно змінюють телефонні послуги клієнтів без їх дозволу [22], [50]) і зубріння (коли телефонні оператори незаконно додають плату за телефонні рахунки клієнтів за послуги, які вони не авторизували. Клієнтів часто обманюють прийняти ці збори під час підписання рекламних матеріалів або через соціальні мережі інженерні методи, такі як маркетинг негативних опцій [22], [51]) шахрайство, таким чином обман абонентів [14], [35], [36], [37]. Телекомунікаційні шахраї стають все більш інноваційними техніки, послуги та продукти, на які вони націлені. Постачальники послуг зв'язку іноді забувають, що високоорганізовані шахраї насправді ведуть власний бізнес і мають своїх «клієнтів» [15]. Незважаючи на зниження у відсотках, як повідомляє Communications Fraud Опитування Control Association (CFCA) у 2015 році, фактичні фінансові, інформаційні та репутаційної шкоди країнам, телекомунікаційним компаніям та іншим підприємствам, а також індивідуумів все ще величезний і має серйозний негативний вплив у всьому світі [32]. Основні проблеми в Гані та інших країнах, що розвиваються, у сфері телекомунікацій шахрайство, а згодом і кібершахрайство – це політика, технологія та політична воля для виконання або запровадити ці політики [2], [14]. Політика щодо телекомунікаційного шахрайства або кібер шахрайство або не продумане, неефективне або не виконується послідовними уряди [14]. Це пояснюється тим, що

інформаційна безпека часто не вважається пріоритетом як на парламентському, так і на виконавчому рівнях наступних урядів, а отже Інформаційна безпека часто є запізнілою думкою, яка часто є реактивною, а не проактивною [14]

Аутентифікація та авторизація є ключовими аспектами в галузі кібербезпеки і використовуються для забезпечення безпеки систем та даних. Давайте розглянемо кожен з цих процесів більш детально:

1. Аутентифікація:

- Означення: Це процес перевірки ідентичності користувача, який намагається отримати доступ до системи чи ресурсів.
- Методи: Включають щось, що користувач знає (паролі), що він має (картки доступу, ключі) або хто він є (біометричні дані).
- Мета: Забезпечення впевненості у тому, що особа або сутність, яка намагається отримати доступ, є тією, за кого себе видає.

2. Авторизація:

- Означення: Це процес визначення прав доступу після того, як користувач успішно пройшов аутентифікацію.
- Методи: Встановлення рівнів доступу, ролей або правил, які контролюють, які ресурси або операції може використовувати користувач.
- Мета: Забезпечення обґрунтованого та гнучкого контролю за тим, що користувач може робити в системі чи з ресурсами.

Використання обох цих процесів дозволяє створити надійний механізм контролю доступу, що допомагає уникнути несанкціонованого доступу, забезпечуючи в той же час зручність для легітимних користувачів

Аудит відіграє важливу роль у сфері кібербезпеки, допомагаючи виявляти та реагувати на потенційні загрози. Давайте розглянемо, як аудит відіграє цю роль:

1. Фіксація Подій:

- Означення: Аудиторська система реєструє події та дії, що відбуваються в інформаційній системі.
- Приклади: Успішні та неуспішні спроби входу, зміни в конфігураціях, створення/вилучення облікових записів тощо.

2. Аналіз Даних:

- Означення: Система аудиту може аналізувати зібрані дані для виявлення аномалій або невідповідностей в шаблонах поведінки користувачів чи системи.
- Приклади: Надмірні зміни прав доступу, спроби несанкціонованого доступу, зміни вірусних сигнатур тощо.

3. Виявлення Інцидентів:

- Означення: Аналіз аудитованих даних дозволяє вчасно виявляти можливі інциденти безпеки.
- Приклади: Виявлення зловживання правами доступу, атак на інформаційну систему, незвичайних даних, які покидають мережу.

4. Реагування на Інциденти:

- Означення: Аудиторські дані служать основою для розслідування інцидентів та вжиття заходів щодо їхнього усунення.
- Приклади: Заблокування акаунтів, відновлення змін, вивчення та застосування заходів безпеки.

5. Вдосконалення Системи Безпеки:

- Означення: Результати аудиту використовуються для удосконалення політик безпеки та заходів контролю доступу.
- Приклади: Модифікації прав доступу, впровадження нових заходів безпеки на основі аналізу аудиту.

Криптографія виступає як потужний інструмент для захисту інформації, застосовуючи методи шифрування для забезпечення конфіденційності та цілісності даних. Вона використовується для перетворення інформації у такий спосіб, щоб вона залишалася безпечною та незрозумілою для неавторизованих осіб, що є важливим аспектом в умовах постійно зростаючих кіберзагроз.

Безпека Мережі:

1. Брандмауери (Firewalls):

- Опис: Брандмауери контролюють трафік між комп'ютерами мережі, блокуючи чи дозволяючи доступ відповідно до визначених правил.
- Застосування: Захист від несанкціонованого доступу та зовнішніх атак.

2. Віртуальні Приватні Мережі (VPN):

- Опис: VPN створюють шифроване з'єднання через неприхильні мережі, забезпечуючи конфіденційність та безпеку даних.
- Застосування: Захист конфіденційності та безпеки під час передачі даних через мережі.

3. Ідентифікація та Аутентифікація:

- Опис: Використання методів ідентифікації (логіни, імена користувачів) та аутентифікації (паролі, біометричні дані) для визначення доступу користувачів.
- Застосування: Запобігання несанкціонованому доступу до мережі.

Безпека Програмного Забезпечення:

1. Оновлення та Патчі:

- Опис: Регулярне оновлення програм та встановлення патчів для закриття вразливостей.
- Застосування: Зменшення ризику атак, використовуючи вразливості програм.

2. Антивірусне та Анти-Malware ПЗ:

- Опис: Використання програм, які виявляють та видаляють шкідливі програми та коди.
- Застосування: Захист від вірусів, троянців та інших видів шкідливих програм.

3. Шифрування Даних:

- Опис: Застосування шифрування для захисту конфіденційних даних під час їхнього зберігання та передачі.
- Застосування: Захист від несанкціонованого доступу до конфіденційної інформації.

4. Тестування на Проникнення:

- Опис: Спроби виявлення та експлуатації вразливостей для забезпечення їхнього усунення.
- Застосування: Підвищення стійкості шляхом виявлення та виправлення слабких місць.

Завдяки цим концепціям, кібербезпека стає необхідною в сучасному світі, де зростає кількість кіберзагроз. Розуміння та впровадження цих принципів є критичним для ефективного захисту інформаційних активів у різних галузях, включаючи корпоративний сектор, державні структури та особисті комп'ютерні системи. Сприйняття кібербезпеки як комплексного підходу дозволяє забезпечити стійкість та надійність в інформаційному просторі.

1.2. Трансформація IPv4 на IPv6: Виклики та Заходи Кіберзахисту

Основні переваги IPv6:

1. Збільшений Розмір Адреси:

- IPv6 використовує 128 біт для адресації, що значно збільшує кількість унікальних IP-адрес, порівняно з IPv4.

2. Підтримка Розширених Функцій:

- IPv6 включає в себе покращені функції, такі як підтримка безпеки, автоматична конфігурація, покращений механізм маршрутизації тощо.

3. Більша Ефективність Маршрутизації:

- Зменшення таблиць маршрутизації та спрощення протоколів маршрутизації сприяє більш ефективній маршрутизації в мережах.

4. Автоматична Конфігурація:

- Механізми автоматичної конфігурації дозволяють пристроям отримувати IP-адреси без необхідності вручну призначати їх.

5. Підтримка Безпеки:

- Вбудована підтримка безпеки, така як IPsec, сприяє захисту даних під час передачі.

6. Підтримка Мультимедійних Додатків:

- Покращена підтримка для мультимедійних та інших передових додатків.

Процес Трансформації:

1. Двоступковий Перехід:

- Двоступковий підхід означає одночасне функціонування IPv4 і IPv6 в мережі протягом переходового періоду.

2. Тунелювання:

- Використання тунелювання дозволяє передавати пакети IPv6 через існуючу IPv4-мережу.

3. IPv6-компатібельність:

- Підтримка пристроїв і програмного забезпечення для обробки як IPv4, так і IPv6.

4. Мережеві Послуги Інтернет-постачальників (ISP):

- Інтернет-постачальники повинні підтримувати IPv6, щоб забезпечити доступність для клієнтів.

Однак, разом із перевагами IPv6, виникають і виклики. Одним з головних є потреба в адаптації обладнання та програмного забезпечення для підтримки нового протоколу. Це може становити значні витрати для компаній та організацій, оскільки вони повинні модернізувати свою мережеву інфраструктуру, щоб впровадити IPv6.

Крім того, важливо враховувати питання сумісності між IPv4 і IPv6, оскільки під час переходу можуть виникнути проблеми зі з'єднанням між різними версіями протоколів. Тому важливо провести детальне планування та тестування перед впровадженням IPv6 для уникнення можливих неполадок та забезпечення безперервності мережевого з'єднання.

Безпекові аспекти переходу на IPv6 є важливими для організацій. Деякі ключові безпекові аспекти, які слід враховувати при переході на IPv6, включають:

1. IPsec в IPv6:

- IPv6 включає в себе IPsec як обов'язковий елемент, що дозволяє забезпечити безпеку на рівні мережі. Організації повинні вивчити та налаштувати IPsec для забезпечення конфіденційності та цілісності даних.

2. Адресація та Фільтрація:

- IPv6 має іншу структуру адресації порівняно з IPv4, і політика фільтрації трафіку також може відрізнятися. Організації повинні налаштовувати файрволи та фільтри для ефективного контролю трафіку.

3. Розгляд Безпеки Протоколів:

- Організації повинні вивчити та розібратися в безпеці протоколів, що використовуються в IPv6, таких як NDP (Neighbor Discovery Protocol) та ICMPv6 (Internet Control Message Protocol version 6).

4. Мережевий Апарат:

- Мережевий апарат та обладнання повинні підтримувати IPv6. Це стосується як роутерів, так і інших мережевих пристроїв.

5. Шкідливі Атаки:

- Оскільки IPv6 набуває популярності, можливі шкідливі атаки, спрямовані на цей протокол. Організації повинні бути готові до виявлення та відповіді на атаки, специфічні для IPv6.

6. Управління Адресами:

- Управління адресами IPv6 включає в себе ефективне вживання та слідкування за життєвим циклом адрес. Це допомагає уникнути проблем, таких як адресне вичерпання.

7. Освіта та Тренування Персоналу:

- Організації повинні забезпечити належний рівень освіти та тренування персоналу з питань безпеки IPv6.

Один з головних викликів - обмежений пул IPv4-адрес, що призводить до ускладнень у розширенні та підтримці нових пристроїв. Перехід також вимагає паралельної підтримки обох протоколів, IPv4 та IPv6, що може створити труднощі в управлінні та забезпеченні безпеки. Різноманітні конфігурації обладнання та програмного забезпечення додають неоднорідність у процесі трансформації.

Заходи кіберзахисту є необхідною складовою цього процесу. Використання брандмауерів та фільтрації трафіку допомагає контролювати потік інформації, а шифрування трафіку забезпечує конфіденційність даних. Моніторинг та аудит безпеки дозволяють виявляти можливі загрози, а навчання та підготовка персоналу грають ключову роль у забезпеченні безпеки мережі. Впровадження принципів найменшого можливого доступу сприяє зменшенню ризиків та мінімізації атак.

Перехід на IPv6 необхідний для подолання обмежень, пов'язаних із вичерпанням IPv4-адрес. Однак це завдання також створює виклики для кібербезпеки, оскільки потребує комплексного підходу для збереження стійкості та захисту мереж під час переходу.

З технічної точки зору, важливо адаптувати обладнання та програмне забезпечення для підтримки IPv6, що може вимагати значних витрат. Разом із тим, планування та тестування є ключовими етапами для уникнення можливих проблем, таких як невідповідність між версіями протоколів та збереження неперервності з'єднань.

Організації повинні враховувати безпекові аспекти, враховуючи нові механізми захисту в IPv6. Перегляд політик безпеки та впровадження заходів, спрямованих на запобігання можливим загрозам, є необхідним етапом у забезпеченні кібербезпеки під час переходу.

Окрім технічних аспектів, важливо також враховувати організаційні питання, такі як навчання персоналу та визначення відповідальностей. Ефективна стратегія кіберзахисту під час переходу на IPv6 вимагає комплексного підходу, який об'єднує технічні і організаційні заходи для забезпечення стійкості та безпеки мережі.

1.3. Безпека MPLS в Телекомунікаційних Мережах

Многопротокольний комутаційний сервіс (MPLS) в телекомунікаційних мережах визначається своєю ефективністю у маршрутизації та управлінні трафіком. Однак, у контексті забезпечення безпеки мережі, важливо враховувати ряд аспектів. Зокрема, ізоляція міток грає критичну роль, дозволяючи зберігати відокремлені дані в межах різних міток, тим самим зменшуючи ризик змішування трафіку та небажаних втручань.

Важливим елементом додаткових заходів безпеки є керування доступом та аутентифікація, які призначені для обмеження несанкціонованого доступу до мережевих ресурсів. За допомогою строгих правил ідентифікації та авторизації

забезпечується лише авторизованим користувачам можливість отримання доступу до важливих систем та інформації.

Ще однією важливою складовою додаткових заходів є використання шифрування даних у MPLS-тунелях. Цей захід гарантує конфіденційність передаваних інформаційних потоків, зменшуючи ризик несанкціонованого доступу або перехоплення конфіденційної інформації. У телекомунікаційних мережах, де захист конфіденційності є важливим завданням, використання шифрування в тунелях MPLS стає пріоритетом.

Окрім цього, ефективна організація та конфігурація керування доступом сприяє створенню бар'єрів для потенційних загроз, забезпечуючи, що лише особи з необхідними правами отримують доступ до мережевих ресурсів. Забезпечення конфіденційності та обмеження доступу є критичними елементами загальної стратегії безпеки в телекомунікаційних мережах.

Однак, в сфері безпеки MPLS важливо враховувати й взаємодію з VPN технологіями. Забезпечення надійного функціонування та захист віртуальних приватних мереж від вторгнень та недозволених доступів є необхідністю. Також важливо регулярно моніторити та аудитувати безпеку мережі, виявляючи можливі загрози та вразливості в режимі реального часу, щоб невідкладно реагувати на потенційні ризики.

Комплексний підхід до забезпечення безпеки в MPLS телекомунікаційних мережах включає в себе ретельний розгляд усіх ключових аспектів, починаючи від керування доступом і аутентифікації до використання шифрування в MPLS-тунелях. Це важливо не лише для стійкості мережі, але й для забезпечення конфіденційності та доступності.

Систематичне впровадження оновлень і патчів є ще однією важливою складовою комплексного підходу. Цей етап дозволяє уникнути можливих вразливостей, оскільки виробники та постачальники послуг постійно вдосконалюють заходи безпеки, виправляючи виявлені недоліки.

Застосування зазначених заходів гарантує не лише стійкість та безпеку мережі, але й зберігає конфіденційність передаваної інформації та забезпечує

доступність для авторизованих користувачів. У контексті телекомунікаційного сектору це є критично важливим для забезпечення безперебійної та захищеної роботи мереж MPLS.

1.3.1 Запобігання шахрайству

Запобігання шахрайству передбачає формування та запровадження ефективного бухгалтерського, оперативного обліку контролю та виховання етичної культури, яка заохочує всіх відігравати свою роль у захисті державні ресурси [21]. Створення етичної культури є важливим кроком у запобіганні та виявлення шахрайства [21]. Політика запобігання шахрайству у сфері телекомунікацій – це документ, який окреслює захист, який слід запровадити, щоб гарантувати, що уряди, компанії/оператори, активи організації піддаються мінімальним ризикам [17]. Політика безпеки – це стратегія того, як установа чи компанія запровадить принципи та технології інформаційної безпеки [18]. Однією з проблем безпеки телекомунікаційної системи є вартість заміни всіх застаріле обладнання, яке було розроблено без відповідних функцій безпеки сучасні загрози безпеці [22]. Багаті економіки значною мірою змогли це зробити замінити частину цього обладнання на сучасне з розширеними функціями безпеки. Однак це не так для багатьох країн, що розвиваються. Окрім заміни застарілого обладнання, наявність централізованого регулювання органи влади, а саме (i) Європейська комісія (ЄК), яка координує свою діяльність з окремі національні регуляторні органи в країнах-членах, (ii) федеральний Комісія з комунікацій (FCC) Сполучених Штатів Америки, яка його координує діяльності з комісіями громадських комунальних послуг (PUC) для її окремих штатів [23], мають сприяв розробці та впровадженню ефективної та дієвої політики в сфері телекомунікацій. Це покращує належну та ретельну координацію між внутрішньою та міжрегуляторною діяльністю а також між операторами intra та inter [23]. Ця координація служить функцією стримувань і противаг, таким чином покращуючи належну координацію безпеки з метою мінімізації можливості вчинення шахрайства. Хоча такі існують конфлікт інтересів між окремими регуляторами країн-членів і континентальних блоки (ЕС і FCC) [23], маючи

централізований регуляторний орган, який координує з окремі національні регуляторні органи виявилися найефективнішим засобом підвищення безпеки в телекомунікаційній галузі [24], [25], [26], [27]. Незважаючи на існування Асамблеї регуляторів телекомунікацій Західної Африки (WATRA) [81] та Асоціація регуляторів телекомунікацій Південної Африки (TRASA) [82], Країни Африки на південь від Сахари ще не усвідомили подібних переваг, досягнутих європейськими країни-члени та Сполучені Штати. Таким чином, це перешкоджає ефективному внутрішньому регулюванню координація, що ускладнює управління безпекою на кордоні. Намагаючись вирішити проблеми телекомунікацій, Міжнародний Союз електрозв'язку (ITU) [28], Світовий банк [29], [30], Світова організація торгівлі (СОТ) [31], Асоціація контролю за шахрайством у зв’язку (CFCA) [32], Організація Об’єднаних Націй Економічна комісія для Африки (UNECA) [33], Європейська комісія (ЄК) [34], Асамблея регуляторів телекомунікацій Західної Африки (WATRA) [81] і Асоціація регуляторів телекомунікацій Південної Африки (TRASA)[82], є розробив і розробляє телекомунікаційну політику та закони, які будуть прийняті в її рамках державну політику управління телекомунікаційними операціями, а також пропонувати консультативні послуги окремим країнам з питань загальних телекомунікаційних операцій і безпеки питань. Окремі країни також розробляють політику та закони, щоб допомогти приборкати питання безпеки телекомунікаційних послуг і операцій [5]. Так само, як різні органи, установи, організації та уряди роблять напружені зусилля, спрямовані на забезпечення безпеки, пов'язаної з телекомунікаційними операціями та послуги, шахраї, пов'язані з телекомунікаційними операціями та послугами, є постійно розширюючи зони своїх цілей і просуваючись у режимі своїх операцій, щоб ухилятися від виявлення та затримання [15]. Загроза, яку представляють ці шахраї, означає, що уряди та оператори в усьому світі повинні це зробити завжди бути напоготові, щоб відповідати новим загрозам і викликам безпеки. Це приносить додаткові бюджетні витрати для урядів і операторів у всьому світі, і в цьому головна проблема викликає занепокоєння, оскільки ті, хто має невеликі фінансові ресурси та інфраструктуру, відстають. Це пропонує часткове пояснення того, чому існує велика невідповідність

у термінах безпека функціонування телекомунікаційної системи та послуг між просунутими, заможнішими економіки та країни, що розвиваються, менш заможні у всьому світі. Це робить недостатньо розвинутим а менш заможні економіки більш вразливі до телекомунікаційного шахрайства. У більшості розглянутої літератури виявляється, що більшість досліджень, проведених досі, зосереджені на рішення, які лікують симптоми, а не корінь проблем, пов’язаних з телекомунікаційний. Ця теза показує, що корінні джерела телекомунікаційного шахрайства походять з політику запобігання шахрайству в сфері телекомунікацій і те, як вона реалізується, а також пояснює, чому існує необхідність об'єднати політику запобігання шахрайству в телекомунікаційних зв'язках, впровадження виклики та шахрайство, пов’язане з телекомунікаціями, і подивіться на них разом, оскільки вони впливають одна на одну.

1.3.2. Урядова політика щодо зв’язку

Більшість урядів встановлюють стратегічні вимоги до телекомунікаційної політики, орієнтовані на досягнення універсальної доступності, а також на забезпечення доступних та високоякісних телекомунікаційних послуг. Ці вимоги реалізуються через створення відкритих, конкурентних та добре керованих ринків телекомунікацій, що сприяє ефективній конкуренції та розвитку інфраструктури.

Універсальна доступність та якісні телекомунікаційні послуги стають стратегічним завданням для економічного та соціального розвитку країни. Шляхом впровадження сучасних технологій та створення конкурентних умов, уряди сприяють вдосконаленню зв'язку та доступу громадян до інформації.

Добре керовані ринки та регулювання гарантують, що телекомунікаційні компанії діють відповідно до встановлених норм, забезпечуючи інноваційний розвиток та вдосконалення послуг. Це сприяє створенню конкурентоспроможного середовища та забезпечує високий стандарт обслуговування для споживачів.

Економічна та суспільна вигода від вдосконалення телекомунікаційної інфраструктури зростає, оскільки це сприяє розвитку бізнесу, підвищенню продуктивності та рівня інновацій в суспільстві.

1.3.3. Політика операторів

Оператори телекомунікацій формують свою політику, яка спрямована на технічну реалізацію телекомунікаційної стратегії, що визначена урядовими регуляторами. Одночасно, вони розробляють внутрішню політику, приділяючи особливу увагу захисту свого бізнесу та ресурсів, включаючи персонал як ключовий актив. Такий підхід дозволяє їм ефективно впроваджувати вимоги регуляторів та забезпечувати внутрішню безпеку.

У багатьох випадках виникають конфлікти інтересів між телекомунікаційними операторами і урядовими органами. Це може бути викликано різницею в пріоритетах та завданнях. Урядові регулятори можуть намагатися забезпечити універсальний доступ та якість послуг для громадян, тоді як оператори частіше ведуть свою політику, спрямовану на ефективність та конкурентоспроможність.

Незважаючи на конфлікти, оператори та урядові органи часто виробляють компроміси, спираючись на взаємну вигоду та дотримання законодавства. Такі узгодження дозволяють досягти балансу між ринковими інтересами та потребами суспільства в цілому, забезпечуючи сталий розвиток телекомунікаційного сектора.

1.3.4. Телекомунікаційне арбітражне шахрайство, слемінг і напихання

Телекомунікаційне арбітражне шахрайство – це використання різниці в ставках розрахунків між країни. Оператори телефонного зв’язку часто стягують різні тарифи на з’єднання залежно від типу дзвінок або постачальник послуг [32]. В дослідженні CFCA 2015, шахрайство з телекомунікаційним арбітражем склав 2,94 мільярда доларів США втрати доходу. Слемінг стосується випадків, коли телефонні оператори незаконно змінюють телефонні послуги клієнтів без їхнього дозволу [22], [50]. Оператори зв’язку часто шахрайським шляхом перемикають місцеві або міжнародний постачальник послуг клієнта сам собі без згоди клієнта та чітке повідомлення [22], [50]. Іноді вони можуть додатково стягувати плату з клієнта за високий дзвінок ставки за завершення з'єднання [22], [50]. Постачальники телефонних послуг зобов’язані за законом отримувати дозвіл клієнтів перед тим, як переключити їх на іншого постачальника [50]. Напихання стосується випадків, коли

телефонні оператори незаконно додають плату до телефонних рахунків клієнтів за послуги, які вони не санкціонували [22], [50]. Клієнтів часто обманюють, щоб прийняти ці витрати під час підписання рекламних матеріалів або за допомогою методів соціальної інженерії як маркетинг негативних опцій [22], [51]. Подібно до слемінгу, оператори телефонного зв'язку за законом зобов’язані отримати дозвіл клієнтів, перш ніж стягувати з них плату телефонний рахунок [22], [50]. Набивання та слемінг настільки поширені через те, що клієнти відсутність знань про ці шахрайства. Справа не тільки в тому, що клієнти не беруть необхідного запобіжні заходи, щоб переконатися, що їхні рахунки точні, але оскільки телефонні рахунки заплутані та важко зрозуміти [52].

1.3.5. Шахрайство з безкоштовними номерами та оптовий протокол ініціації сеансу (SIP)

У схемі шахрайства з безкоштовними номерами, шахрай вступає в угоду з оператором, що дозволяє використовувати мережу для здійснення великої кількості дзвінків на безкоштовний номер. Це призводить до збільшення рахунків власника безкоштовного номера, і оператор потім отримує частину прибутку з цієї схеми, ділячись з шахраєм [22]. Такий вид шахрайства може створити значні фінансові втрати для власників безкоштовних номерів, а також створює економічні стимули для співпраці злочинців із операторами.

Ще однією формою шахрайства є оптове використання транкінгового протоколу ініціювання сеансу (SIP), яке є відносно новою, але швидко зростаючою практикою [53]. У цьому виді шахрайства зловмисник заробляє гроші, продаючи оптові транкінгові послуги, використовуючи викрадені облікові дані для завершення дзвінків [53]. Це створює серйозні виклики для виявлення і протидії, оскільки шахраї можуть використовувати вивчені методи та облікові дані для уникнення виявлення.

Важко виявити дану форму шахрайства через її складні технічні аспекти та використання викрадених облікових даних. Оператори та власники

телекомунікаційних мереж повинні розвивати ефективні стратегії та заходи безпеки для виявлення та запобігання оптовому шахрайству SIP.

1.3.6. Шахрайство з Wangiri та роумінг

Японською мовою «wan» означає «один», а «giri» означає «повісити трубку» [22], [52]. Ця форма шахрайства, також відомий як «один дзвінок і перерва», націлений на мільйони користувачів мобільних телефонів шляхом випадкового відбору дзвінки з платних телефонних ліній, дозволяючи дзвінку пролунати один раз, а потім покласти трубку залишаючи на телефоні користувача повідомлення «пропущений дзвінок», шахраї сподіваються, що користувачі подзвонять назад. Коли вони це роблять, цей номер виявляється номером преміум-ставки, вони часто знаходять самі слухають рекламу, як-от підписки на преміум-лінії чату або Інтернет послуги. Шахрайство в роумінгу відбувається, коли абонент, який скористався послугами виїзної мережі відмовляється платити та посилається на необізнаність, недостатнє знання додаткових витрат, або стверджуючи, що послуга ніколи не запитувалася. Це шахрайство в своїй основній формі також це найпоширеніший [54]. Роумінг – це автоматичне підключення до гостьової мережі коли домашня мережа користувача недоступна [22], [32] [50], [51], [54]. Деталі виклику Запис (CDR) для цих витрат на роумінг не надходить у домашню мережу протягом кількох днів (іноді тижнями) пізніше, залишаючи велике вікно можливостей для шахрайських атак [22], [32], [50], [51], [54]. Опитування CFCA з 1 травня 2015 року по квітень 2016 року показало, що послуги роумінгу були найбільш вразливі до шахрайства. В опитуванні 130 операторів у всьому світі Гана була другою найвищий рівень шахрайства в роумінгу після Іспанії. Це поганий імідж для такої країни, що розвивається Гана. Сторінка 14 на малюнку 1 показано аналіз, зроблений у звіті про опитування CFCA [54].

1.3.7. Соціальна інженерія

Соціальна інженерія, це стара форма шахрайства. Цих шахраїв ще називають Впевнені хитруни. Розвиток інформаційних технологій зміцнив їх і складність. Це

найбільш ухильна форма шахрайства, оскільки вона дуже непередбачувана складний, оскільки приймає багато форм, зокрема дзвінки, мобільні текстові повідомлення, електронні листи, фізична взаємодія та обман. Основна проблема соціальної інженерії полягає в тому, що вона націлена на користувачів або людей, які є найслабшою ланкою будь-якої інфраструктури безпеки. Про це свідчать відомості шахрай із соціальної інженерії Кевін Мітнік, як він це висловлює; «Мені рідко доводилося вдаватися до технічного напад. Компанії можуть витрачати мільйони доларів на технологічний захист, і це так марно, якщо хтось може зателефонувати комусь по телефону та переконати їх у цьому робити щось на комп'ютері, що знижує захист комп'ютера або розкриває інформацію вони шукали»[50]. Це завдає безпрецедентних збитків економіці країн, що розвиваються, оскільки їм все ще бракує навички та знання для виявлення, контролю або навіть керування рівнем поширення та діями ці шахраї. Більшість людей абсолютно необізнані та неосвічені в цьому форми шахрайства. Незважаючи на те, що вони відчувають їх щодня, вони залишаються на їхню милість шахраї, оскільки уряди та установи або не мають необхідних навичок, робочої сили, або є такими переповнений. Це ще більше посилюється тим фактом, що більшість африканських країн подобається Гана не вважає інформаційну безпеку пріоритетом як у парламенті, так і у виконавчій владі рівнях. Отже, інституції знаходяться в набагато слабшому становищі, щоб впоратися з постійно прогресуючим соціальним інженерні шахраї. У Гані соціальна інженерія навіть набула релігійного вигляду [55], це називається «Сакава» (чорна магія) використовують для того, щоб заплутати, заманити та навіть закохати жертв у шахраїв щоб жертви надсилали гроші шахраям [92]. Шахраї вважають, що можуть використати це для вирівнювання контролювати свідомість своїх жертв [93], [94], [95]. Їх мішенню переважно є люди з західні країни, країни ЄС [92], [93], [94], [101] і деякі заможні жителі Гани [95]. Останнім часом ще більше занепокоєння викликає те, що ці шахраї («ХЛОПЦІ та ДІВЧАТА SAKAWA» або «GAME BOYS», як їх воліли називати), зробили новий поворот у сфері телекомунікацій індустрії (тепер вони займаються дзвінками та SMS-спамом), вони надсилають шахрайські текстові

повідомлення і здійснювати шахрайські дзвінки нічого не підозрюючим абонентам мобільної мережі. Шахраї часто користуються тим, що жертви запізнюються у розпізнаванні шахрайських прохань, і використовують загальні, добре відомі шаблони шахрайства, просто переробляючи та оновлюючи перевірені схеми успішні в минулому проти своїх жертв [20]. Шахраї пишуть зловмисні повідомлення на адресу нічого не підозрюючи мобільних телефонів жертв і спонукаючи їх надати їм свої особисті телефони облікові дані або навіть надсилати гроші на рахунки шахраїв. Це особливо часто зустрічається в країни, що розвиваються, такі як Гана. Найчастіше ці шахрайські повідомлення містять інформацію про те, що передплатники виграли а певна рекламна акція від мобільної мережі абонента, і що абонент повинен зателефонувати а певний номер мобільного телефону (номер шахрая), щоб дізнатися більше про те, як отримати гроші. Коли їм дзвонить нічого не підозрюючи абонент, вони обманюють його, щоб заплатити певну суму суму грошей на певний банківський рахунок або рахунок мобільних грошей (мобільний банкінг система, введена в телекомунікаційні системи в Гані) для використання для витрати на обробку, щоб переслати гроші нічого не підозрюючому абоненту. Одного разу гроші виплачуються, нічого не підозрюючий абонент більше ніколи не дізнається про шахраїв. Це Стратегія шахраїв використовує переваги справжньої реклами, зробленої різними телекомунікаційні компанії в Гані в рамках своїх методів винагороди лояльних клієнтів, просування нових продуктів і завоювати більше клієнтів. Інша часто використовувана стратегія полягає в тому, що шахрай телефонує нічого не підозрюючому мобільному абоненту, розповідає абонента, що він (шахрай) є співробітником певної компанії (переважно поштової, телекомунікаційна компанія або навіть авторитетний банк) і що вони мають у своєму розпорядженні певні предмети (переважно гроші, смартфони, айпади чи ноутбуки), призначені для нічого не підозрюючого абонента і що адреса (банківський рахунок, якщо це гроші), за якою вони повинні переслати пункти здаються неповними, тому вони хочуть, щоб передплатник дав їм право адресу для внесення змін. Це форма тесту для перевірки інтелекту абонента та рівень довірливості. Одного разу абонент без ґрунтовних роздумів дає їм свою адресу

через, вони знають, що дістали його/її. Спеціально для тих шахраїв, які видають себе за них співробітники поштових компаній відправлення, призначені для їхніх жертв, зазвичай відправляються з ЄС і західні країни. На наступному етапі вони повідомляють мобільному абоненту, що в щоб здійснити змінyes у своїх «Системах» він/вона повинен буде заплатити певну суму гроші на певний банківський рахунок або мобільний рахунок для використання як «комісія за обробку». Знову ж таки, як тільки вони отримують гроші, абонент мобільного зв'язку більше ніколи не чує про них. Всі контакти з шахраєм більше не працюють. Ця стратегія враховує довірливість і прагнення безкоштовних речей серед громадян Гани. За цією ж стратегією, між 2005 і 2010 роками шахрай просив нічого не підозрюючих жертв купити мобільний кредит і надіслати їм коди, які будуть використані як витрати на обробку їхніх товарів в Інтернеті, але має оскільки переглянув його до вищезазначеного, оскільки передплатникам стало відомо про їхні подвиги. «Найбільша проблема полягає в тому, що жертви «Sakawa» та інших кібершахраїв часто стикалися не знайдено оголошений центральний пункт у країні, щоб повідомити про випадки. Навіть коли ці про випадки було повідомлено Департаменту кримінальних розслідувань поліції Гани (CID), на затримання будь-якого підозрюваного знадобилося багато років через відсутність ноу-хау щодо відстеження ці злочинці використовують комп'ютерні навички розслідування. Гірше всього, коли таке кіберзлочинці були затримані та притягнуті до суду, не було достатніх правових підстав переслідувати цих злочинців, оскільки правова система не була сучасною, щоб засудити та покарати кібер злочинців, що призвело до погіршення іміджу Гани як місця, пов'язаного з кіберзлочинністю»[57] Романтичне шахрайство, ці шахраї все ще перебувають на соціальній інженерії, використовують законні сайти знайомств як а також створюють власні сайти знайомств, які потім використовують для полювання на невинних молодих жінок дівчата, чоловіки та молоді чоловіки, які в пошуках супутників життя стають жертвами ці шахраї, які користуються своїм відчаєм і вразливістю, щоб вимагати гроші з них [93], [94], [98], [99], [100], [101]. Ці шахраї, за допомогою висоти голосу зміни технології, вбудованої в більшість телефонів, можуть перемикати свій голос на будь-якого

чоловіка або жіночі голоси залежно від статі жертви, щоб маскуватися під протилежну стать здатні переконати своїх жертв [97], [100], [101]. Шахрайство через Skype — одна з найновіших форм шахрайства, спрямована на хлопців і чоловіків віком від 15 до 50 років років, які базуються на своїх посадах, які обіймають в установі чи суспільстві, релігійному чи культурному середовища мають міцніші сімейні стосунки та, як правило, не сприймають сексуальну аморальність ісламський світ і деякі інші географічні умови світу [93], [94], [95], [97], [98], [99], [100], [101]. Часто все починається з того, що шахрай використовує фотографію красивої молодої дівчини як свою фотографія профілю на онлайн-платформі соціальних мереж, із запитом на дружбу з нічого не підозрюючих хлопців і юнаків [93], [94], [95], [97], [98], [99], [100], [101]. Один раз жертви приймають дружбу, їх заманюють до відеочату з шахраєм через Skype. У Skype вони спочатку спілкуються перед відеочатом. У профілі шахрая в скайпі досі є фото молодої красивої дівчини фото шахрая. На початкових етапах чатів шахрай повідомляє жертвам вона відчуває мед (стан бажання займатися сексом або в сексуальному настрої) і бажає жертви був з нею (для жертви шахрай – красива дівчина, в яку випадково закохався його в онлайн-соцмережах), щоб привести душевний стан жертви в сексуальний настрій [93], [94], [95], [97], [98], [99], [100]. Потім шахрайка починає описувати, у що вона одягнена, наскільки вона готова до нього (жертви), незважаючи на те, що він далеко, вона (шахрай) потім слідує кажучи, що жертва повинна увімкнути свою веб-камеру, щоб вони могли бачити один одного [93], [94], [95], [97], [98], [99], [100], [101]. І під час цього процесу шахрай відтворює відео молодої дівчини, яка мастурбує нічого не підозрює жертва, спостерігаючи за її душевним станом і реакцією. Якщо нічого не підозрює випадково жертва мастурбує поруч, її записують у кінці шахрая [93], [94], [95], [96], [97], [98], [99], [100]. Потім шахрай використовує це, щоб попросити гроші (шантаж) від жертви та погрожуючи показати відео родині або привласнити влади країни, і залежно від наслідків опромінення, постраждалих змушені платити величезні суми грошей цим шахраям [93], [94], [95], [96], [97], [98], [99], [100]. Ця форма шахрайства ще не поширена в Гані, але зростає в інших країнах країни Африки. Смішинг або SMS-фішинг, а також голосовий фішинг або вішинг

(шахрайство з ідентифікаційною інформацією); Він діє схожий на звичайний електронний фішинг; його єдина мета — придбати нічого не підозрюючих абонентів особисту інформацію, таку як імена користувачів, паролі, дані рахунку кредитної картки та іншу конфіденційну інформацію, видаючи себе за законну компанію. Це робиться через телефон дзвінки або навіть текстові повідомлення [22]. Масове маркетингове шахрайство має широкий спектр і охоплює низку різних типів шахрайства (наприклад, це відбувається через Інтернет, телемаркетинг і поштою або на масових зібраннях) [20]. Шахраї часто намагаються обдурити кількох осіб, щоб максимізувати свої кримінальні доходи [20]. Зробити на основі цього жертви переконують передати гроші злочинцям заздалегідь 17 обіцяні товари, послуги чи вигоди, які з'являться за ними [20]. Скориставшись жертвами із запізненням у розпізнаванні шахрайських запитів, шахраї використовують загальне, добре відоме шахрайство шаблони, просто переробляючи та оновлюючи схеми, які виявилися успішними в минулому проти своїх жертв [20].

1.3.8. Ціноутворення, що вводить в оману, шахрайство з контролю за помилковими відповідями (FAS).

Ціноутворення Збиває з пантелику те, що більшість телекомунікаційних операторів використовують різноманітні та різні ціни планують ввести в оману абонентів щодо реальних ринкових цін на послуги [56]. Вони часто надають нові пропозиції зі спеціальними знижками [22], [50] і швидко змінюють ціни відразу передплатників зареєстровані [22]. Шахрайство з наглядом за помилковими відповідями (FAS), цей підхід до шахрайства дозволяє транзитним операторам шахрайським шляхом збільшувати свій дохід від кожного дзвінка, виконуючи такі дії:

 Помилкова відповідь або шахрайство з коротким зупиненням, у цьому випадку оператор перенаправляє дзвінок або зупиняє його на записане повідомлення та починає стягувати плату замість того, щоб передавати виклик на реальна мережа [22].

 Рання відповідь, при цьому оператор збільшує тривалість розмови шахрайським шляхом. Це можна зробити шляхом вибору дзвінка та відтворення музики або

фальшивий сигнал дзвінка, доки абонент не відповість [22], [58].

 Пізнє відключення, таким чином оператор навмисно затримує передачу

повідомлення про роз'єднання дзвінка стороні, що телефонує, щоб стягнути плату за довший дзвінок замість [22].

1.3.9. Шахрайство між з'єднаннями в обхід або сіра маршрутизація та поверхнева мережа (OTT)

Шахрайство Interconnect Bypass — це використання нелегітимних обмінів шлюзами для уникнення законних шлюзи та плата за міжнародне завершення [22]. Згідно з опитуванням 2015 року Communication Fraud Control Association (CFCA), шахрайство Simbox або шахрайство Bypass склав 5,97 мільярда доларів США, що є другим за величиною збитків від шахрайства Міжнародне шахрайство з розподілом доходів [32]. З доповіді ООН Економ Комісія для Африки щодо відстеження незаконних фінансових потоків в африканських країнах (UNECA 2015), Уряд Гани повідомив, що шахрайство з SIM-боксами коштувало 5,8 мільйонів доларів у вигляді вкрадених податків поодинці [33]. Виклик урядам і телекомунікаційній галузі ще більше посилюється поява нового варіанту цього шахрайства під назвою Over-The-Top (OTT) Bypass fraud також відоме як Over-The-Top (OTT) Hijack шахрайство. Програми OTT включають WhatsApp, Viber, IMO, Twitter, Skype тощо. Шахрайство в обхід OTT передбачає переадресацію звичайного телефонного дзвінка через IP на додаток голосового чату на смартфоні без згоди абонента та оператора або знання [58]. Це шахрайство відбувається, коли «постачальник послуг OTT співпрацює з транзитом оператора для перехоплення звичайних дзвінків (тобто дзвінків, що надходять із мобільного або стаціонарного телефону на мобільний телефон), щоб завершити їх через програму OTT» [58], [59]. У цій формі шахрайства служби OTT використовують IP-мережі для впровадження послуг і часто це роблять без залучення операторів, таким чином пропускаючи оператори [58]. Подібно до

шахрайства Simbox також приваблює високі міжнародні збори за завершення з'єднання, особливо в деяких країнах країни що розвиваються. В результаті вищесказаного шахраям вдається уникнути суворого правила, що накладаються на операторів різними урядами/країнами, навіть якщо вони надають аналогічні послуги [58], [62]. Послуги Over-The-Top створюють загрозу безпеці та конфіденційності передплатників як їх особистих дані часто передаються цим програмам OTT [58], [73]. Однак деякі країни робили спроби регулювати послуги Over-The-Top (OTT) [46], [59], [63]. Завдяки нижчій вартості, відеопослуги та перевагу абонентів спілкуватися в чаті на послуги OTT, це приваблює значну кількість абонентів абонентів операторів і це саме по собі коштує операторам значних втрат доходу, оскільки спостерігається зниження кількості звичайних дзвінків і SMS тексти [58], [60], [61]. Отже, поява шахрайства в обхід OTT погіршила становище компанії оператори можуть втрачати більше прибутку.

1.3.10. Міжнародне шахрайство з часткою доходу (IRSF)

Шахрайство з міжнародною часткою доходу відбувається, коли шахрайський оператор або третя сторона постачальник послуг оператора рекламує діапазон телефонних номерів як міжнародну преміальну ставку Числа (IPRN) у різних частинах світу, їхні жертви, чиї номери, на жаль трапляється, що серед ряду номерів, які рекламуються, часто є країни, що розвиваються, або малий супутниковий оператор із високою платою за завершення з'єднання [22]. Жертва отримує а величезний телефонний рахунок за несанкціоновані дзвінки, і шахрай збирає гроші з компанії, яка володіє номером преміум-ставки. Згідно з опитуванням CFCA 2015 року, шахрайство IRSF було найбільшою понесеною втратою, що становить сума доходу в 10,76 мільярдів доларів США [32]. Щорічне глобальне шахрайство 2015 року звіт про збитки Асоціації контролю за шахрайством у зв'язку (CFCA) вказує на а зниження збитків від шахрайства в сфері телекомунікацій. Опитування показало, що втрати від шахрайства зменшилися 18%, грошовий еквівалент $38,1 млрд з 2013 року [32]. У відсотках світових телекомунікаційних доходів втрати від шахрайства знизилися приблизно з 1,69% до 0,40%, зниження

порівняно з 2013 р. [32]. Основною причиною зниження називають ан посилення співпраці та координації між перевізниками у виявленні та зупинці шахрайська діяльність після опитування Асоціації контролю за шахрайством у зв'язку в 2013 році [32]. Висновок, зроблений за результатами опитування CFCA 2015 року, полягає в тому, що телекомунікаційне шахрайство все ще залишається дуже прибутковим. Незважаючи на зниження частки втрат від телекомунікаційного шахрайства в доходах у всьому світі є позитивним, фактична грошова вартість все ще дуже велика і мала дуже негативний результат вплив на телекомунікаційні компанії, підприємства, уряди та окремих осіб у всьому світі [32]

1.3.11. Телекомунікаційна політика

За словами Мерілі С. Ґріндла та Томаса Дж. В., чотири контекстуальні фактори впливають на розвиток політики в країнах, що розвиваються [2], [42]. До них належать:

(i) рівень технічного аналізу, використаний для вирішення проблеми,

(ii) політична стабільність і підтримка, пов'язана з політикою,

(iii) бюрократична мотивація та здатність до формулювання та реалізації політики

(iv) міжнародна допомога та підтримка.

Крім того, культура, рівень грамотності громадян і економічна потужність є одними з основних фактори, що впливають на розвиток політики в країнах, що розвиваються. Політика розроблена з н вклади населення країни можуть бути невдалими. І для широких верств населення щоб мати можливість зробити свій внесок, вони повинні бути просвітленими. Внесок громадян буде 19 фактором культури народу та вартості. Це часто призводить до компромісів і нехтування загальний внесок населення, отже, слабке формулювання політики**.**

1.3.12. Проблеми реалізації телекомунікаційної політики

«Етап імплементації політичного процесу — це робочий етап, на якому політика є фактично переведено в дію з надією вирішити якусь суспільну проблему»

[43]. Відповідно до Результати досліджень Майкла Л. Беста та Дханараджа Тхакура, проблеми впровадження політики в телекомунікаційній галузі в країнах, що розвиваються, є:

(i) слабке інституційне середовище,

(ii) внутрішньодержавні інституційні актори,

(iii) домінування елітних груп у прийнятті рішень [2] та

(iv) обмежене розуміння політичного процесу в країнах, що розвиваються, також є а заклопотаність. Багато з існуючих структур було розроблено з використанням даних із Сполучених Штатів Америки та меншою мірою Західної Європи [2]. За висновками Марта Канене Оньєаджува, деякі проблеми, що впливають на реалізацію телекомунікаційної політики та або правозастосування в Нігерії (країни, що розвиваються):

(i) слабкі інституційні структури, і, як наслідок, регулятори та мобільні служби

постачальники не тримають інтереси звичайних споживачів на рівнях, які відповідають політиці і закон,

(ii) немає спеціального втручання, щоб зробити базові мобільні послуги доступними та доступним для звичайних споживачів із низьким рівнем доходу

(iii) існує слабкість у забезпеченні дотримання правил регуляторними органами, і, як наслідок, є послідовна і навмисна експлуатація незахищених і нічого не підозрюючих абонентів провайдери телекомунікаційних послуг [14]. Переглянувши кілька літературних джерел щодо політики запобігання шахрайству в сфері телекомунікацій, проблеми впровадження та телекомунікаційне шахрайство, ми вирішили віднести їх до формальних виклики контролю як виклики регуляторів, виклики технічного контролю як оператори виклики та виклики неформального контролю як виклики передплатників, щоб зробити більш зрозумілим що було відкрито колегами-дослідниками в усьому світі

1.3.13. Проблеми регуляторів

Регулятори в усьому світі стикаються з різними проблемами, на які впливають такі фактори, як культура, географічні умови, рівень технології, економічна потужність, рівень грамотності громадян тощо Найпоширеніші проблеми перераховані нижче:

 Телекомунікаційна екосистема втілює в собі велику різноманітність правил і законів, і поняття законності значно відрізняються залежно від країни

комунікаційне середовище [22].

 Відсутність співпраці, правоохоронні органи мають труднощі з міжнародним правом правозастосування, яке ускладнює ідентифікацію шахраїв, навіть якщо шахрайство є виявлено [22], [44]. Незважаючи на наявність міжнародних організацій, бракує спільних промислових ініціатив для боротьби з шахрайством [22].

 Існує конфлікт інтересів щодо рівня відповідальності за регулювання

між централізованими блоками, Європейською Комісією (ЄК) та окремими особами

Національні регуляторні органи (НРО) для ЄС і Федерального зв'язку 20 Комісії та Комісії з комунальних послуг (PUC) окремих штатів Сполучені Штати Америки [23].

 «Під притягненням до відповідальності за правопорушення у сфері телекомунікацій виникають дві проблеми які мають міжнародний аспект: по-перше, визначення місця правопорушення сталося для того, щоб вирішити, право якої юрисдикції застосувати, і, по-друге, отримати докази та забезпечення того, що правопорушника можна знайти та притягнути до суду. Обидва ці питання породжують складні правові проблеми юрисдикції та екстрадиції. Навіть якщо можна вирішити, який закон застосовний, додаткові труднощі можуть виникнути під час застосування той закон. Екстериторіальні витрати на правоохоронні органи часто непомірно високі».[16]

 Більшість країн, що розвиваються, не мають законодавства про захист даних і, отже, не існує офіційного визначення крадіжки особистих даних [40]. Однак

у Гані парламент прийнято Закон про захист даних 2012 року, «ЗАКОН щодо встановлення захисту даних Комісії, для захисту конфіденційності особи та персональних даних шляхом регулювання обробку особистої інформації, щоб забезпечити процес отримання, зберігання, використання або розкривати особисту інформацію та пов'язані з цим питання» [45].

1.3.14. Загальні проблеми експлуатації телекомунікаційних мереж

Телекомунікаційна інфраструктура в усьому світі має спільний досвід виклики, для вирішення яких передові чи розвинені країни доклали величезних зусиль подолати деякі, але це не однаково для слаборозвинутих країн або країн, що розвиваються через різниця в рівнях технології, економічна сила та інші фактори.

Однак нижче наведено список деяких технічних проблем, які постають перед операторами зв'язку в усьому світі пивний досвід:

 Послуги Over-The-Top (OTT), які працюють поверх каналів передачі даних, переважно/загалом поза контролем операторів [22], [46], [47], [48].

 На відміну від IP-мереж, маршрутизація виклику дуже часто непрозора. Кожен оператор знає лише наступний стрибок маршрутів вгору та вниз за течією, а також вихідний і номер призначення [22].

 Через проблеми конфіденційності та конкуренції оператори зазвичай не бажають ділитися або публікувати свої умови ціноутворення, варіанти маршрутизації або висновки, пов'язані з шахрайством [15], [16], [22], [49].

 Оператори часто не мають однакового рівня стимулів для боротьби з шахрайством [22].

 CDR у роумінгу не одразу доступні домашньому оператору, тому

виявлення та припинення шахрайства, складне для домашнього оператора [22].

 Відсутність партнерських угод про належну перевірку робить трафік викликів вразливим до шахрайства, якщо одна сторона має шахрайські наміри (Процес перевірки якості та надійності транзитного оператора до угоди про партнерство називається належною обачністю [22]).

 Вартість модернізації застарілих систем. Застарілі системи, які лежать в основі

телефонна мережа не була розроблена з урахуванням безпеки. Оновлення цієї спадщини глобальна система неможлива в найближчому майбутньому через високу вартість [22]

1.4. Взаємодія Різних Типів Доступу: Контекст Безпеки

У сучасних інформаційних системах виникає необхідність взаємодії різних типів доступу для ефективного управління та забезпечення безпеки даних. З моменту появи різних методів доступу, таких як рівні дозволів, аутентифікація та авторизація, постало питання їхньої інтеграції та координації для оптимального функціонування систем. Контекст безпеки у таких системах набуває значущості, оскільки він стає ключовою архітектурною складовою для забезпечення взаємодії різних методів доступу та надання консистентного захисту в усій системі.

Контекст безпеки охоплює широкий спектр аспектів, таких як управління ідентифікацією користувачів, визначення рівнів доступу, аудит та моніторинг дій користувачів. Це дозволяє ефективно координувати взаємодію між різними методами контролю доступу та забезпечує комплексний захист в умовах динамічних вимог та загроз сучасного інформаційного середовища.

Інтеграція контексту безпеки допомагає уникнути розривів у захисті даних та сприяє створенню єдиної системи управління безпекою, яка може ефективно адаптуватися до змінних умов та нових викликів. Забезпечуючи консистентний рівень захисту на різних рівнях доступу, контекст безпеки стає необхідним елементом сучасних інформаційних систем, що працюють в умовах високих вимог до безпеки та конфіденційності.

Однією з важливих аспектів є ідентифікація та аутентифікація користувачів. В контексті взаємодії різних типів доступу, система повинна ефективно визначати особу користувача та перевіряти його легітимність. Використання багаторівневої ідентифікації, такої як біометричні дані, паролі та карткові системи, дозволяє

створити надійні механізми впізнавання, що реагують на різноманітні потреби та контексти доступу.

Управління авторизацією та привілеями є ще однією важливою складовою. Контроль доступу до різних ресурсів та функцій системи відповідає за те, щоб користувачі отримували лише той рівень доступу, який необхідний для виконання їх завдань. Здійснення прозорого та ефективного керування привілеями враховує конкретний контекст, забезпечуючи недоступність непотрібних або ризикових операцій для конкретного користувача чи групи.

Ще однією суттєвою частиною контексту безпеки є моніторинг та аудит безпеки. Здійснення систематичного спостереження за діяльністю користувачів та реагування на аномалії є важливою аспектом забезпечення безпеки в інформаційних системах. Моніторинг дозволяє вчасно виявляти та реагувати на незвичайні події, що може вказувати на можливі порушення або загрози безпеці. Аудит безпеки, у свою чергу, є механізмом реєстрації та аналізу важливих подій, що дозволяє детально вивчати дії користувачів та системи.

Ефективний моніторинг та аудит безпеки не лише попереджають випадкові чи зловмисні порушення, але й грають ключову роль у швидкому виявленні та усуненні потенційних проблем. Збір та аналіз відомостей про активність користувачів допомагає уточнити контекст безпеки та призначити відповідні заходи для подальшого удосконалення захисту.

Важливою складовою моніторингу та аудиту є визначення стандартів безпеки та встановлення метрик для оцінки ефективності заходів безпеки. Регулярний аналіз отриманих даних дозволяє визначати тенденції та прогали в системі безпеки, що є критичним для постійного вдосконалення заходів забезпечення безпеки інформаційних систем.

У цілому, моніторинг та аудит безпеки є важливою складовою контексту безпеки, що сприяє підтримці надійності та реагуванню на загрози у сучасних інформаційних системах.

Взагалі, створення високоефективної системи безпеки для взаємодії різних типів доступу вимагає глибокого розуміння контексту, в якому вони

використовуються. Ідентифікація, авторизація, управління привілеями та моніторинг узгоджуються для створення надійного та гнучкого середовища безпеки, яке може вирішувати різноманітні виклики в області доступу до інформації та ресурсів.

1.5. Хмарні та Віртуалізовані Сервіси: Вплив на Кібербезпеку

У сучасному цифровому ландшафті хмарні та віртуалізовані сервіси стали неодмінною складовою інформаційно-технологічних стратегій підприємств. Перехід до хмарних рішень і віртуалізації дозволяє підприємствам оптимізувати ресурси, забезпечувати більшу гнучкість та знижувати витрати на IT-інфраструктуру.

Однак ці інновації також приносять нові виклики в галузі кібербезпеки. Збільшена поверхня атаки, зумовлена розподіленою та віртуалізованою природою інфраструктури, вимагає вдосконалених підходів до захисту від кіберзагроз. Питання конфіденційності, цілісності та доступності даних стають актуальнішими в умовах хмарних та віртуалізованих середовищ.

Для ефективного керування кібербезпекою в хмарних та віртуалізованих середовищах, підприємства повинні розробляти та впроваджувати стратегії, що враховують специфіку цих технологій. Це включає в себе захист віртуалізованих мереж, виявлення та відповідь на загрози в хмарних середовищах, а також забезпечення безпеки даних при їх переміщенні між різними віртуальними об'єктами.

Ключовим аспектом успішної кібербезпеки в хмарних і віртуалізованих системах є поєднання технічних заходів та визначення чіткої стратегії управління ризиками. Забезпечення відповідності стандартам безпеки, регулярне тестування на проникнення та постійне моніторинг середовища допомагають підприємствам впроваджувати ефективні заходи з кіберзахисту в умовах хмарних та віртуалізованих технологій.

Перш за все, перехід до хмарних і віртуалізованих сервісів створює нові точки входу для потенційних загроз. Віддалені сервери, з якими взаємодіє хмарний сервіс,

та велика кількість віртуальних об'єктів можуть стати об'єктом інтересу для кіберзлочинців. Важливо мати комплексні стратегії захисту, щоб уникати несанкціонованого доступу до цих ресурсів.

Другий аспект - збільшення потенційних атак на дані в хмарних сховищах. Оскільки у великих об'ємів даних, збережених в хмарі, криються цінні інформаційні активи, кіберзлочинці зосереджують свою увагу на пошуку вразливостей. Заходи безпеки мають включати сильне шифрування, строгий контроль доступу та ефективне моніторингове виявлення загроз.

Третій важливий аспект - виклики при управлінні ідентифікацією та автентифікацією. З уведенням віртуалізованих та хмарних рішень, важливо розглядати системи, які забезпечують надійну ідентифікацію користувачів та забезпечують безпеку автентифікації на різних рівнях доступу.

Нарешті, у контексті хмарних та віртуалізованих середовищ важливо покладати основну увагу на прозорість та контроль. Завдяки великому обсягу даних та ресурсів, що обробляються в таких середовищах, ефективне керування вимагає ретельного моніторингу. Прозорість в контексті кібербезпеки означає доступність чіткої та зрозумілої інформації щодо всіх аспектів безпеки, що дозволяє операторам та адміністраторам швидко та ефективно реагувати на можливі загрози.

Контроль важливий для забезпечення безпеки даних та інфраструктури. Це включає в себе не лише виявлення потенційних аномалій, але й можливість активного втручання та захисту в разі виявлення загроз. Автоматизовані системи контролю та реагування дозволяють стежити за активністю в реальному часі та вживати заходів щодо забезпечення безпеки.

Організації, що використовують хмарні та віртуалізовані сервіси, повинні враховувати необхідність постійного оновлення та удосконалення систем моніторингу та контролю. Регулярні аудити та тестування на проникнення допомагають визначити можливі слабкі місця та вдосконалити процеси кібербезпеки.

Нарешті, успішне впровадження стратегій прозорості та контролю в хмарних та віртуалізованих середовищах передбачає не тільки технічні аспекти, але й

ретельне навчання персоналу та вдосконалення політик безпеки. Все це допомагає забезпечити стійкість та надійність кіберзахисту в умовах сучасних інформаційних технологій.

Усі ці виклики підкреслюють необхідність не просто адаптуватися до нових технологій, але й активно розвивати та вдосконалювати стратегії кібербезпеки, враховуючи специфіку хмарних та віртуалізованих сервісів. Лише такий підхід дозволить впевнено експлуатувати переваги цих інновацій, забезпечуючи одночасно високий рівень захисту від сучасних кіберзагроз.

1.6. Ядро Мультисервісної Архітектури: Ключові Складові та Безпека

Мультисервісна архітектура є інноваційним підходом до розвитку мережі, спрямованим на інтеграцію різноманітних сервісів та типів трафіку в єдину та добре організовану інфраструктуру. Основні компоненти цієї архітектури визначаються для забезпечення її функціональності та оптимальної ефективності.

На перший погляд, ключовим елементом мультисервісної архітектури є її здатність інтегрувати різні сервіси. Це означає, що в мережі можуть оптимально співіснувати різні види трафіку, такі як голосовий, відео, даних, забезпечуючи користувачам універсальний та багатофункціональний доступ.

Другим важливим аспектом є гнучкість архітектури. Мультисервісна модель дозволяє швидко адаптуватися до змінних вимог та обсягів трафіку, забезпечуючи ефективну роботу мережі в умовах зростаючих обсягів і різноманітності витоків даних.

Третій аспект полягає в забезпеченні якості обслуговування (QoS). Мультисервісна архітектура дозволяє ефективно керувати різними сервісами, приділяючи пріоритети відповідно до їхніх вимог до пропускної здатності та затримок. Це дозволяє забезпечити задовільну якість обслуговування для кожного типу трафіку.

Завершальний аспект архітектури полягає в її масштабованості. Мультисервісна модель розрахована на розширення та розвиток, щоб враховувати

зростаючі потреби мережі. Це дозволяє забезпечити стійкість та ефективність системи в умовах постійних змін у вимогах користувачів та технологічних інноваціях

Перш за все, централізована система управління є основною ключовою складовою. Це високорівневе ядро архітектури, що дозволяє централізовано керувати різними сервісами та ресурсами. Забезпечення гнучкості та швидкості реакції на зміни в мережі, це управління дозволяє оптимізувати використання ресурсів та гарантувати якість обслуговування для різних видів трафіку.

Друга ключова складова - використання технологій віртуалізації. Віртуалізація мережевих ресурсів дозволяє створювати віртуальні екземпляри мережевих складових, таких як комутатори та маршрутизатори. Це полегшує масштабування та розвиток мережі, забезпечуючи при цьому ефективне використання апаратних ресурсів.

Третя складова - підтримка різноманітного трафіку та сервісів. Ядро мультисервісної архітектури повинно бути готовим обробляти різні типи трафіку, включаючи голос, відео, дані та інші сервіси. Забезпечення якісної обробки та передачі кожного з цих видів трафіку відіграє ключову роль у забезпеченні задоволення потреб користувачів.

Щодо аспектів кібербезпеки, ядро мультисервісної архітектури повинно ретельно враховувати кілька ключових вимог. Зокрема, це включає в себе захист від несанкціонованого доступу до централізованих управлінських систем, шифрування данних для забезпечення конфіденційності та впровадження механізмів контролю доступу, щоб забезпечити безпеку віртуалізованих ресурсів. Також важливо надавати увагу моніторингу безпеки та виявленню інцидентів для оперативної реакції на потенційні загрози.

Мультисервісна архітектура, взагалі кажучи, характеризується своєю централізованістю, віртуалізацією та здатністю ефективно обробляти різноманітний трафік. Централізованість є ключовим аспектом, що дозволяє центральному елементу системи керувати та координувати роботу різноманітних сервісів, що

працюють в мережі. Це забезпечує єдність та злагодженість в управлінні різними аспектами мережі.

Віртуалізація в мультисервісній архітектурі грає важливу роль у створенні ефективної та гнучкої інфраструктури. Цей аспект дозволяє розділяти фізичні ресурси на віртуальні, що полегшує масштабування та адаптацію до змінних потреб мережі. Віртуалізація сприяє оптимізації використання ресурсів та забезпечує ефективне розгортання нових сервісів та можливостей.

Здатність ефективно обробляти різноманітний трафік стає ключовою функцією для мультисервісної архітектури. Система повинна вміло керувати різними видами трафіку, такими як голос, відео, даних, забезпечуючи оптимальні умови для кожного сервісу. Це важливо для забезпечення задовільної якості обслуговування та ефективного використання мережевих ресурсів.

В контексті мультисервісної архітектури, безпека стає необхідним елементом, який потребує постійного удосконалення та комплексного підходу. Забезпечення централізованого керування та віртуалізації мережі також вимагає ефективних засобів захисту від різних загроз та атак. Розвиток системи безпеки в мультисервісній архітектурі є ключовим елементом для забезпечення стійкості та безпеки мережі

1.7. Функціональні Модулі та Рівні Обслуговування: Заходи Кіберзахисту

У контексті мережевих систем, функціональні модулі та рівні обслуговування є критичними компонентами для забезпечення ефективного функціонування та кіберзахисту. Один із ключових аспектів цього підходу - індивідуалізація віртуальних з'єднань через конкретні логічні інтерфейси. Даний принцип дозволяє ефективно використовувати логічний інтерфейс для кількох віртуальних з'єднань, а отже, виникає потреба в розрізненні окремих віртуальних з'єднань, наприклад, за допомогою точок потоку Ethernet (EFP).

Створення індивідуальних віртуальних з'єднань на логічних інтерфейсах, відомих як точки потоку Ethernet (EFP), є ключовим етапом для забезпечення

безпеки та функціональності в мережевих системах. EFP дозволяє визначати параметри та атрибути на рівні інтерфейсу, що детально моделює проходження пакетів через систему.

На рівні EFP визначаються різні функції, які впливають на обробку даних на віртуальному з'єднанні. Це включає етапи інкапсуляції, де визначається спосіб упаковки даних для передачі, кондиціонування, яке визначає правила обробки та впорядкування пакетів, а також фільтрацію, що регулює, які пакети будуть передані чи відкинуті на основі певних умов.

Застосування функціональних та атрибутних параметрів на рівні EFP дозволяє точно керувати обробкою даних у віртуальних з'єднаннях, підвищуючи ефективність та забезпечуючи необхідний рівень безпеки.

Цей підхід також враховує різноманітні аспекти, такі як забезпечення якості обслуговування, яке визначає, як система повинна обробляти та пріоритетизувати пакети в залежності від їхніх характеристик та вимог мережі

Однією з ключових вимог у цьому контексті є обов'язкове використання IVC (Individual Virtual Connection). Це забезпечує унікальну ідентифікацію та ізоляцію віртуальних з'єднань, що є критичним для запобігання змішування та несанкціонованого доступу до даних. IVC також є необхідним для впровадження заходів кіберзахисту, таких як шифрування та контроль доступу.

Усі ці заходи на рівні функціональних модулів та рівнів обслуговування є важливою частиною кіберзахисту мережевих систем. Вони забезпечують не тільки ефективну обробку даних, але і гарантують високий рівень безпеки та захисту від різноманітних кіберзагроз.

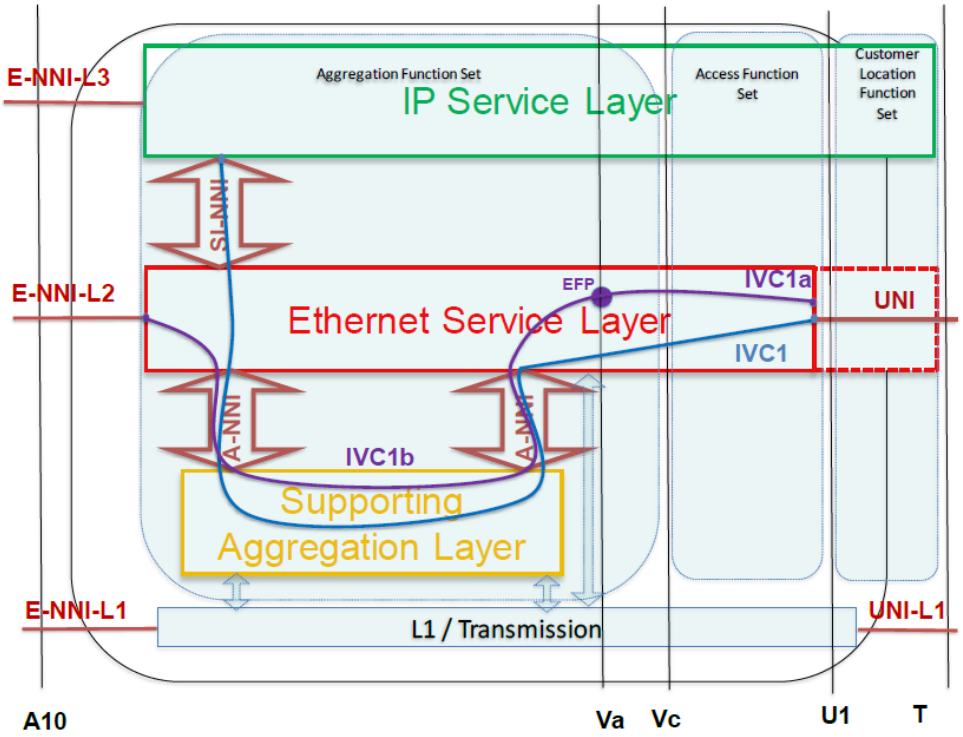

Рис. 1.1. Приклад IVC

1.8. Архітектурне Розподілення та Безпека Вузлів

Архітектурне розподілення в мережевих системах є стратегічним рішенням, що визначає організацію та взаємодію вузлів для досягнення ефективного функціонування. З разом із зростанням складності розподілених систем стає критично важливим приділяти особливу увагу безпеці вузлів. Безпека вузлів в архітектурному розподіленні охоплює кілька ключових аспектів, які впливають на стійкість та надійність мережі.

В першу чергу, слід приділяти увагу механізмам аутентифікації та авторизації вузлів в мережевих системах. Контроль доступу до вузлів, їхній ідентифікації та перевірці легітимності взаємодії відводиться ключова роль у забезпеченні безпеки мережі. Використання передових систем аутентифікації, таких як цифрові сертифікати та двофакторна аутентифікація, сприяє підвищенню рівня впізнавання та ефективному контролю за правами доступу до вузлів.

Далі, важливо розглядати різні аспекти системи аутентифікації. Цифрові сертифікати використовуються для підтвердження автентичності вузла, забезпечуючи довірену основу для встановлення з'єднання. Двофакторна

аутентифікація, у свою чергу, використовує два різні методи перевірки особи, часто комбінуючи щось, що відомо (наприклад, пароль) і щось, що володіє (наприклад, фізичний токен або мобільний пристрій). Ці підходи допомагають унеможливити несанкціонований доступ та підвищити рівень безпеки.

Додатково, слід враховувати роль авторизації у забезпеченні безпеки мережі. Це включає в себе визначення повноважень вузлів, контроль доступу до конкретних ресурсів та обмеження привілеїв користувачів. Ефективна система авторизації гарантує, що лише вповноважені суб'єкти мають доступ до необхідної інформації та ресурсів в системі.

Завершуючи, важливо вдосконалювати та підтримувати механізми аутентифікації та авторизації вузлів відповідно до сучасних вимог безпеки. Постійна оцінка та покращення цих систем є ключовим елементом впровадження ефективних стратегій кібербезпеки в мережевих середовищах.

Другий аспект - шифрування комунікацій між вузлами. Забезпечення конфіденційності даних під час їх передачі між розподіленими вузлами є невід'ємною частиною безпеки. Використання протоколів шифрування, таких як TLS (Transport Layer Security), дозволяє захищати інформацію від несанкціонованого доступу та перехоплення.

Третій аспект - моніторинг та виявлення аномалій в роботі вузлів. Системи безпеки повинні здати виявляти незвичайну або підозрілу активність в мережі. Застосування систем інтелектуального аналізу трафіку та регулярний моніторинг дозволяють ефективно реагувати на можливі загрози та інциденти.

Нарешті, важливо враховувати фізичну безпеку вузлів. Заходи, такі як обмеження фізичного доступу до обладнання та використання механізмів впізнавання та аудиту доступу, спрямовані на зменшення ризиків фізичних атак та внутрішніх загроз.

Узагальнюючи, архітектурне розподілення та безпека вузлів є взаємопов'язаними концепціями, спрямованими на створення надійних та стійких розподілених мережевих систем. Інтеграція цих аспектів узгодженого підходу дозволяє побудувати ефективну та захищену інфраструктуру

1.9. Напрямок розвитку технологій: вплив на кіберзахист

Технологічний розвиток створює як нові можливості, так і нові виклики для кібербезпеки. Зростання використання пристроїв IoT, впровадження штучного інтелекту та машинного навчання, а також розвиток квантових технологій мають значний вплив на кібербезпеку.

Інтернет речей (IoT) представляє собою глобальну мережу фізичних пристроїв, які з'єднані із Інтернетом для взаємодії та обміну даними. Ця універсальна система охоплює різні області, від побутових пристроїв до промислового обладнання, створюючи величезну інфраструктуру з'єднаного середовища. Принципова можливість пристроїв IoT збирати та обробляти дані в реальному часі робить їх ключовими акторами в сфері збільшення ефективності та автоматизації.

У контексті IoT важливо визначити роль збирання даних. Простеження та збір інформації від пристроїв, які можуть бути віддалено розташовані, в реальному часі надає можливість аналізу та прийняття швидких рішень. Це забезпечується високою ступенем автоматизації, що є однією з ключових переваг IoT в промислових, логістичних та багатьох інших секторах.

Ще однією характеристикою є спроможність взаємодії пристроїв IoT між собою та іншими системами. Це відкриває нові можливості для створення складних та високоефективних екосистем, де пристрої можуть взаємодіяти та вирішувати завдання разом, щоб досягти спільних цілей.

Нарешті, важливо визначити виклики та питання, пов'язані з безпекою та приватністю в області IoT. З великим обсягом збираємі та оброблюваними даними виникає необхідність строгого контролю за доступом та заходами забезпечення конфіденційності, оскільки це стає критичним для довіри та прийняття технологій IoT.

Пристрої IoT можна класифікувати за різними ознаками, такими як:

- Тип пристрою: датчики, виконавчі пристрої, розумні пристрої.

- Призначення: промислові пристрої, побутові пристрої, медичні пристрої.
- Місце розташування: пристрої, що знаходяться всередині будівель, пристрої, що знаходяться на відкритому повітрі.

Пристрої IoT взаємодіють між собою за допомогою стандартних протоколів, таких як:

- MQTT (Message Queuing Telemetry Transport) - протокол для передачі повідомлень між пристроями.
- CoAP (Constrained Application Protocol) - протокол для передачі повідомлень між пристроями з обмеженими ресурсами.
- HTTP (Hypertext Transfer Protocol) - протокол для передачі даних в Інтернеті.

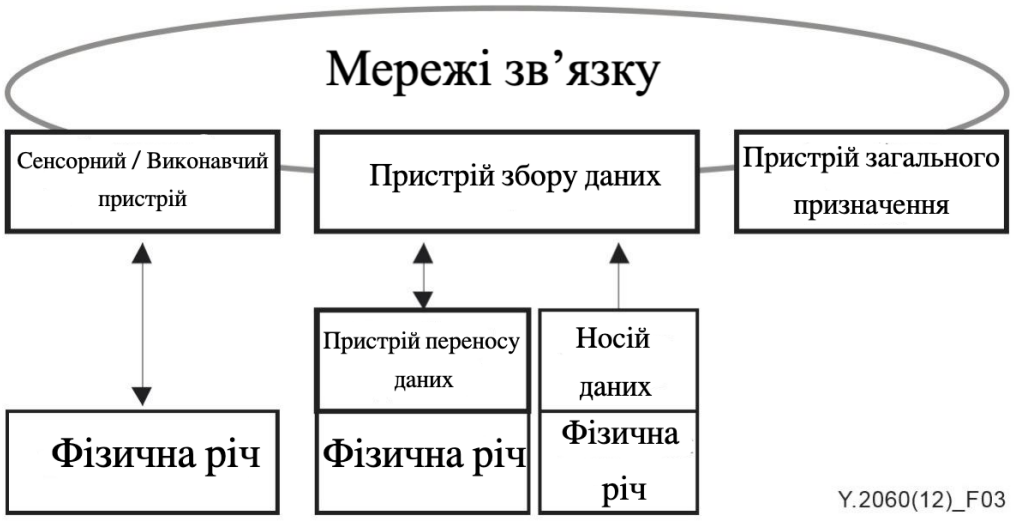

Рис. 1.2. Типи пристроїв IoT і їх взаємодія

Еталонна модель IoT - це концептуальна модель, яка використовується для опису архітектури IoT. Еталонна модель IoT може бути використана для розуміння того, як працюють пристрої IoT і як вони взаємодіють між собою.

Еталонна модель IoT за версією IWF (Internet of Things Forum) включає в себе такі компоненти:

- Датчики: пристрої, які збирають дані з реального світу.
- Контролери: пристрої, які обробляють дані, зібрані датчиками.
- Мережа: мережа, яка з'єднує пристрої IoT.
- Хмарні сервіси: сервіси, які надають пристроям IoT доступ до ресурсів, таких як зберігання даних, обчислювальні потужності та аналіз даних.

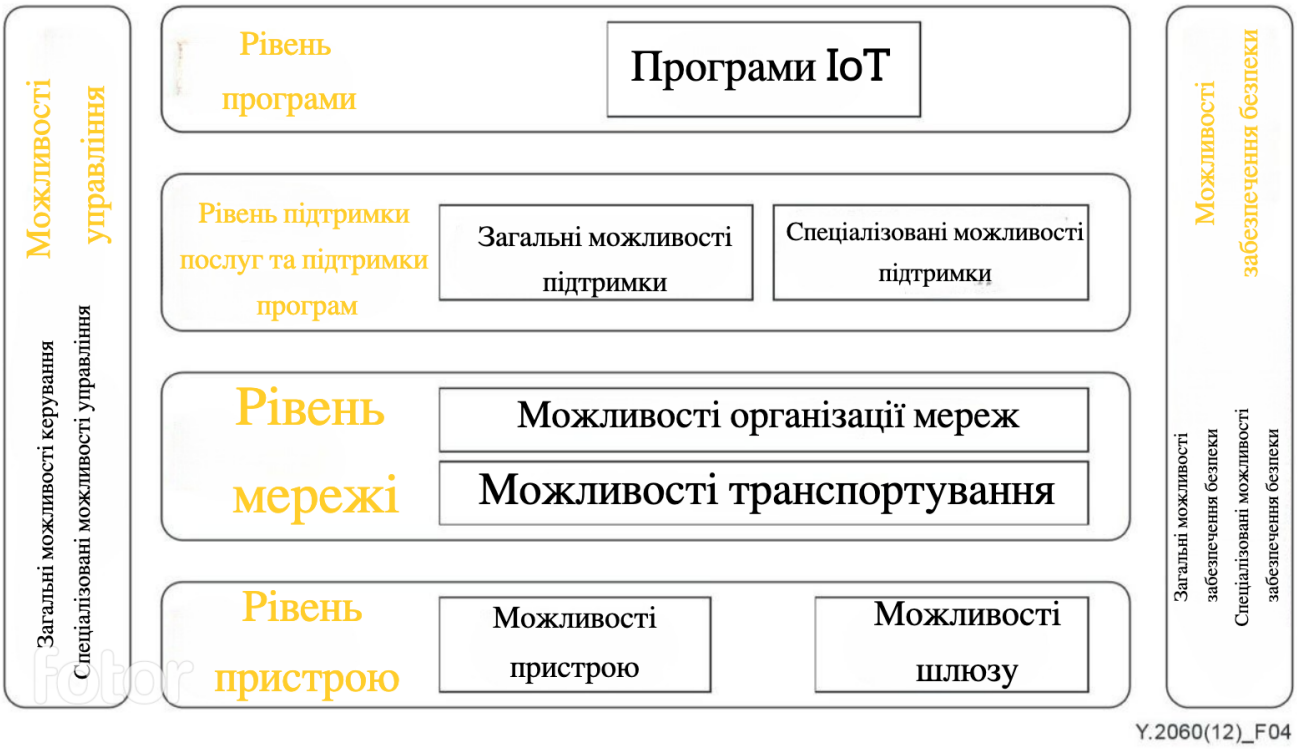

Рис. 1.3. Еталонна модель IoT

Датчики - це пристрої, які збирають дані з реального світу. Датчики можна класифікувати за різними ознаками, такими як:

- Тип даних: датчики, які збирають аналогові дані, датчики, які збирають цифрові дані.
- Призначення: датчики, які збирають дані про температуру, датчики, які збирають дані про рух.
- Місце розташування: датчики, які знаходяться всередині будівель, датчики, що знаходяться на відкритому повітрі.

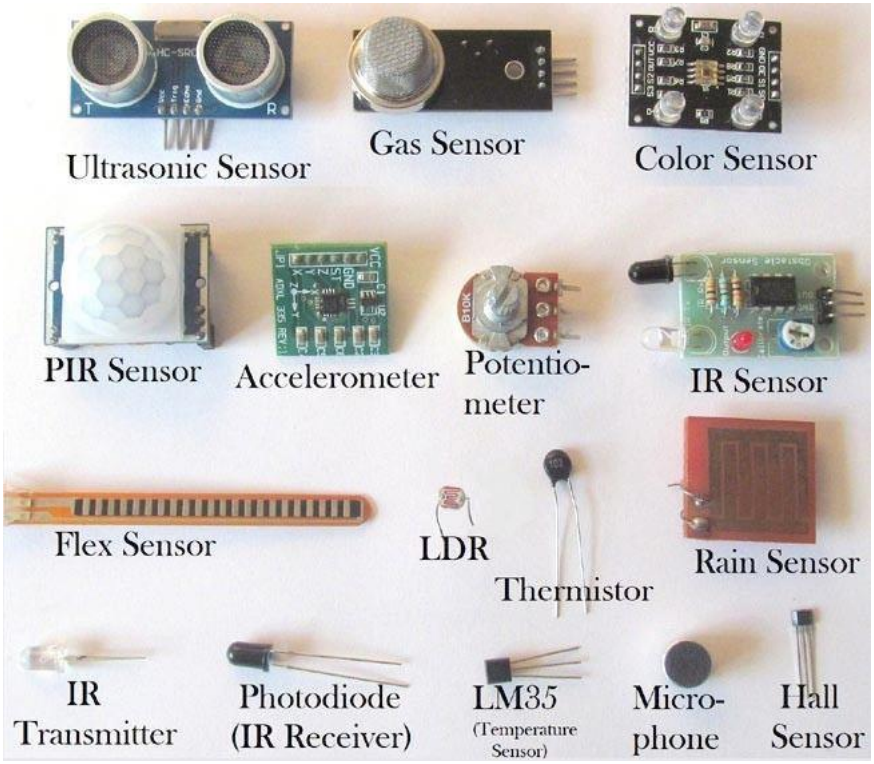

Рис. 1.4. Різні типи датчиків

SPINEX - це платформа для розробки та управління пристроями IoT. Платформа SPINEX включає в себе такі компоненти:

- Конструктор пристроїв: інструмент для створення пристроїв IoT.
- Платформа управління: інструмент для управління пристроями IoT.
- Платформа аналізу даних: інструмент для аналізу даних, зібраних пристроями IoT.

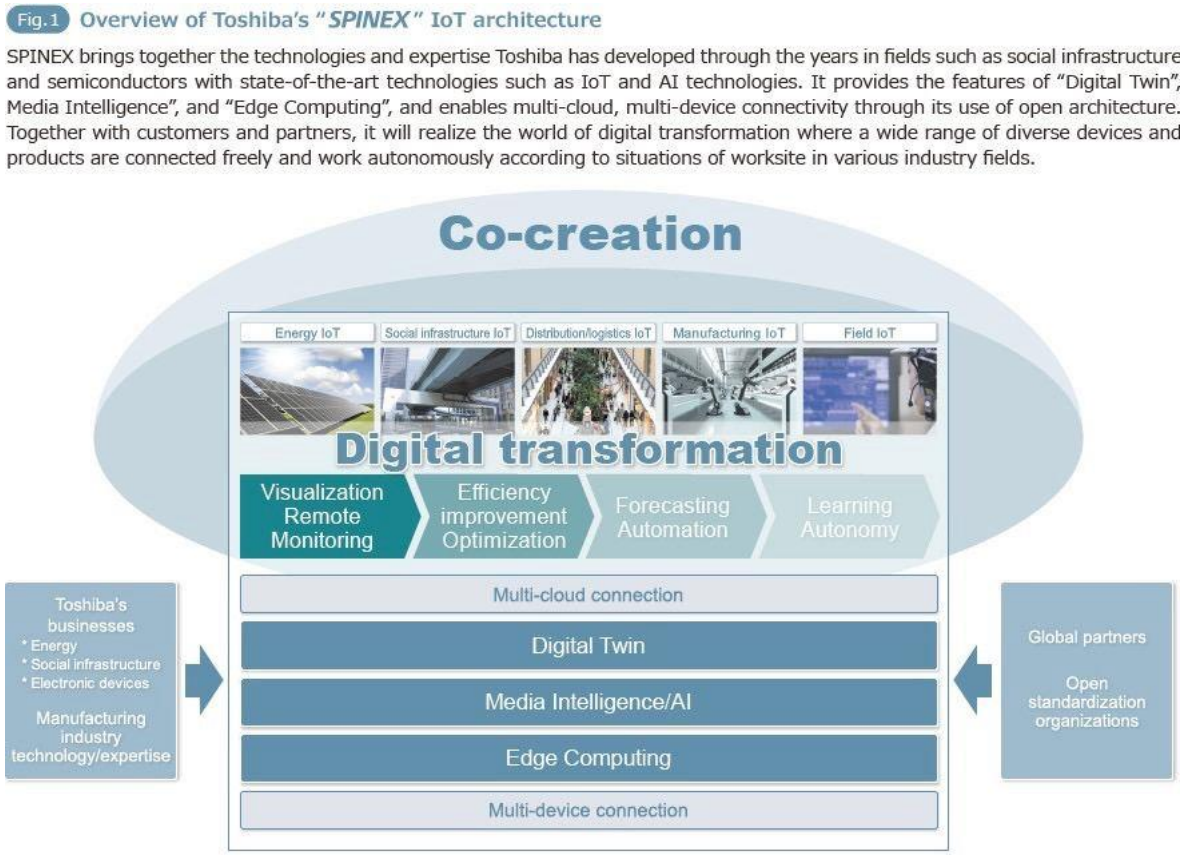

Рис. 1.5. Платформа SPINEX

За прогнозами IDC, обсяг ринку IoT у світі в 2026 році досягне 1,1 трлн. доларів. Це означає, що ринок IoT буде зростати в середньому на 18,7% щороку.

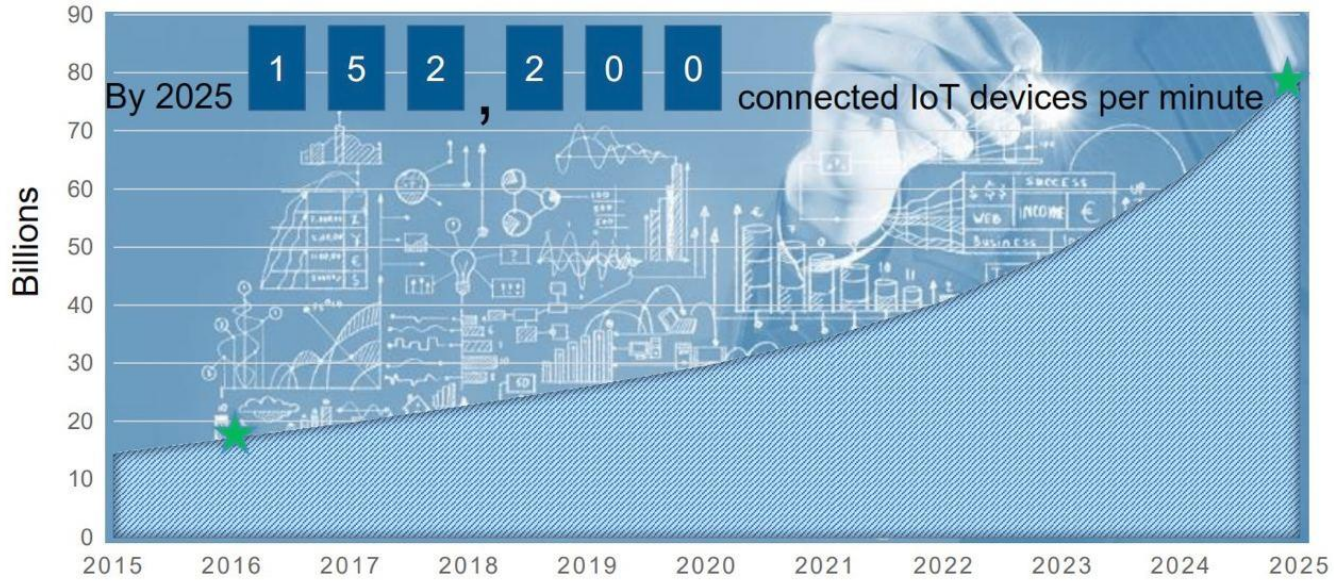

Рис. 1.6. Прогноз IDC про зростання кількості підключень IoT

За прогнозами IDC, кількість підключень IoT у світі в 2026 році досягне 41,6 млрд. Це означає, що кількість підключень IoT буде зростати в середньому на 22,3% щороку.

MIDAS (Multiscale Iterative Data Anomaly Solver) - це новий базовий рівень для виявлення аномалій на графіках.

MIDAS використовує багатомасштабний підхід для виявлення аномалій, які можуть бути приховані в даних на різних часових масштабах.

MIDAS працює в два етапи:

1. Визначення аномалій на локальному рівні: на цьому етапі MIDAS виявляє аномалії на кожному окремому часовому масштабі.
2. Визначення аномалій на глобальному рівні: на цьому етапі MIDAS об'єднує аномалії, виявлені на локальному рівні, в глобальні аномалії.

MIDAS має ряд переваг перед існуючими методами виявлення аномалій на графіках:

- Більша чутливість: MIDAS здатний виявляти аномалії, які можуть бути приховані в даних на різних часових масштабах.
- Більша точність: MIDAS менш схильний до помилкових спрацьовувань, ніж існуючі методи.
- Менька кількість помилок другого типу: MIDAS менш схильний до пропускання аномалій, ніж існуючі методи.

MIDAS може бути використаний для виявлення аномалій у даних з різних областей, таких як:

- Інтернет речей: MIDAS може бути використаний для виявлення аномалій у даних, зібраних пристроями IoT.
- Фінанси: MIDAS може бути використаний для виявлення аномалій у фінансових даних.
- Медицина: MIDAS може бути використаний для виявлення аномалій у медичних даних.

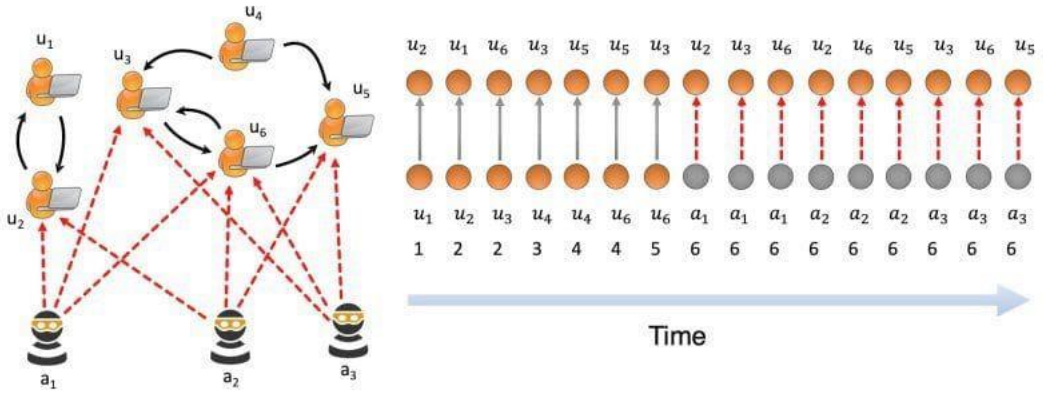

Рис. 1.7. Схема виявлення аномалій за допомогою MIDAS

Блокчейн - це розподілена реєстрова система, яка використовується для зберігання та передачі даних. Блокчейн складається з ланцюжка блоків, кожен з яких містить інформацію про операції, які були виконані в системі.

Блокчейн має ряд переваг перед традиційними системами зберігання даних:

- Централізованість: блокчейн є децентралізованою системою, яка не має центрального сервера. Це робить блокчейн більш стійким до збоїв та хакерських атак.
- Безпека: блокчейн використовує криптографію для забезпечення безпеки даних. Це робить блокчейн більш безпечним для зберігання конфіденційних даних.
- Прозорість: блокчейн є прозорою системою, яка дозволяє кожному учаснику системи переглядати інформацію, яка зберігається в системі. Це робить блокчейн більш прозорим для всіх учасників системи.

Блокчейн може бути використаний для різних цілей, таких як:

- Фінанси: блокчейн може бути використаний для створення децентралізованих фінансових систем, таких як криптовалюти.
- Торгівля: блокчейн може бути використаний для создания децентралізованих торговельних систем.
- Управління: блокчейн може бути використаний для створення децентралізованих систем управління.

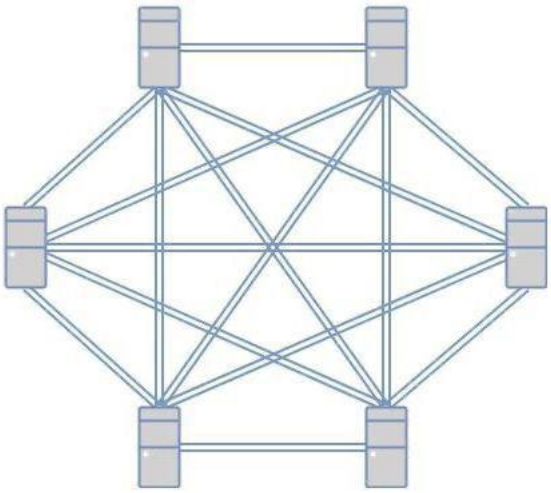

Рис. 1.8. Схема блокчейну

ВИСНОВКИ ДО РОЗДІЛУ 1

Вивчення основних принципів кібербезпеки телекомунікаційних мереж відкриває широкий спектр аспектів, що обумовлюють безпеку та надійність цифрового простору. Одним із ключових аспектів є визначення та розуміння основних концепцій кібербезпеки, включаючи трансформацію IPv4 на IPv6, забезпечення безпеки в MPLS телекомунікаційних мережах, взаємодію різних типів доступу та вплив хмарних та віртуалізованих сервісів на кібербезпеку.

Особлива увага приділяється ядру мультисервісної архітектури, його ключовим складовим та заходам забезпечення безпеки. Функціональні модулі та рівні обслуговування розглядаються як ефективні засоби кіберзахисту. Архітектурне розподілення та безпека вузлів розглядають в контексті надійності та витривалості мережі.

Окрема увага приділяється напрямкам розвитку технологій та їх впливу на кіберзахист. Зокрема, висвітлюється важливість заходів забезпечення кібербезпеки в умовах росту Інтернету речей, впровадження штучного інтелекту та машинного навчання, використання квантових технологій, а також застосування технологій блокчейну та розподілених реєстрів.

Усі ці аспекти формують комплексний підхід до кібербезпеки телекомунікаційних мереж, де ключовою складовою стає поєднання передових технологій та ефективних стратегій кіберзахисту. Отже, вивчення цих принципів відкриває шлях до створення надійних, стійких та сучасних телекомунікаційних мереж в умовах постійно зростаючих кіберзагроз.

РОЗДІЛ 2 АНАЛІЗ ОСНОВНИХ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1. Типи Кіберзагроз та їх вплив

Зараз ми спостерігаємо швидке та постійне змінювання ландшафту кіберзагроз. Ця динаміка визначається не лише появою нових видів загроз, але й постійною еволюцією тактик і методів атаки, що використовуються кіберзлочинцями. Відбувається це з метою уникнення виявлення та забезпечення успішних кібератак.

Один із основних факторів цього постійного розвитку кіберзагроз - це стрімка зміна технологічного середовища. Поява нових технологій, таких як штучний інтелект, блокчейн чи Інтернет речей, відкриває нові можливості для кіберзлочинців, які намагаються використовувати ці інновації для власної користі.

Постійна зміна тактик і методів атаки свідчить про необхідність постійного вдосконалення кібербезпекових стратегій. Компанії та організації повинні бути готові до адаптації та удосконалення своїх заходів безпеки, оскільки кіберзагрози надалі розвиватимуться та адаптуватимуться до змін у технологічному середовищі.

У цьому постійному змаганні за кібербезпекою, співпраця між галузевими експертами, державними установами та приватним сектором стає ключовою для обміну інформацією та створення спільних стратегій для протидії кіберзагрозам.

Кіберзлочинці, спеціалізовані в інформаційних технологіях, використовують різноманітні методи для отримання несанкціонованого доступу до комп'ютерів чи мережевих серверів з метою завдання шкоди. Один із способів цього надання доступу - це експлуатація вразливостей у програмному забезпеченні чи операційній системі, використовуючи шкідливі програми, такі як віруси, троянські коні чи черв'яки. Цей підхід дозволяє зловмисникам непомітно проникнути в систему та використовувати її ресурси без дозволу.

Ще одним способом, який кіберзлочинці можуть використовувати для отримання доступу, є соціальна інженерія. Цей метод передбачає обман користувачів чи персоналу організації для отримання конфіденційної інформації, такої як паролі або ключі доступу. Кіберзлочинці можуть використовувати переконливі методи, такі як відправлення фішингових листів, щоб введенням у оману отримати необхідні дані.

Вектор атаки, або шлях, яким кіберзлочинець отримує доступ, може також включати в себе використання наданого доступу зловмисникам іншими користувачами чи системами. Наприклад, якщо атака почалася від одного вузла, зловмисники можуть розповсюджувати свій доступ, використовуючи внутрішні мережеві механізми.

Захист від цих атак вимагає комплексного підходу, включаючи регулярне оновлення програмного забезпечення та використання ефективних засобів антивірусної та антималware захисту, а також навчання персоналу про принципи безпеки та впізнавання соціальної інженерії

Поширені способи отримати доступ до комп’ютера чи мережі:

Змінні носії, такі як флеш-накопичувачі

Атака методом грубої сили методом проб і помилок декодує зашифровані дані

Веб-атаки або атаки електронною поштою

Несанкціоноване використання системних привілеїв вашої організації

Втрата або крадіжка пристроїв, що містять конфіденційну інформацію

Відділ банків (DOB) заохочує всі фінансові установи та недепозитарні фінансові установи розробити детальну політику кібербезпеки для запобігання атакам.

Типи кіберзагроз, про які ваша установа повинна знати, включають:

Шкідливе програмне забезпечення

програми-вимагачі

Розподілені атаки на відмову в обслуговуванні (DDoS).

Спам і фішинг

Захоплення корпоративного рахунку (CATO)

Виведення готівки через банкомат

Шкідливе програмне забезпечення

Зловмисне програмне забезпечення також відоме як шкідливий код або зловмисне програмне забезпечення. Зловмисне програмне забезпечення – це програма, яка вставляється в систему для порушення конфіденційності, цілісності або доступності даних. Це робиться таємно та може вплинути на ваші дані, програми чи операційну систему. Зловмисне програмне забезпечення стало однією з найбільш значущих зовнішніх загроз для систем. Зловмисне програмне забезпечення може завдати значних збитків і збоїв і потребує великих зусиль у більшості організацій.

Шпигунське програмне забезпечення, шкідливе програмне забезпечення, призначене для порушення конфіденційності, також стало серйозною проблемою для організацій. Хоча зловмисне програмне забезпечення, що порушує конфіденційність, використовується протягом багатьох років, останнім часом воно стало набагато поширенішим. Шпигунське програмне забезпечення проникає в багато систем для відстеження особистої діяльності та фінансового шахрайства.

Організації також стикаються з подібними загрозами від кількох форм нешкідливого програмного забезпечення. Ці форми кіберзагроз часто пов’язані зі зловмисним програмним забезпеченням. Більш поширеною формою є фішинг. Фішинг передбачає обманним шляхом змусити людей розкрити конфіденційну або особисту інформацію.

Поради щодо запобігання зловмисному програмному забезпеченню від Посібника Національного інституту стандартів і технологій (NIST) із запобігання інцидентам зловмисного програмного забезпечення та обробки:

Вимагати сканування вкладених файлів електронної пошти та збереження на локальних дисках або знімних носіях.

Не дозволяйте певні типи файлів (наприклад, файли .exe) надсилати або отримувати електронною поштою.

Обмежте використання знімних носіїв, таких як компакт-диски або флеш-накопичувачі, у системах з високим ризиком.

Обмежте кількість користувачів із правами доступу або правами адміністратора.

Переконайтесь, що системи регулярно оновлюються за допомогою оновлень і виправлень операційної системи та програм.

програми-вимагачі

Програми-вимагачі запобігають або обмежують користувачам доступ до їхньої системи через зловмисне програмне забезпечення. Програмне забезпечення-вимагач просить вас заплатити викуп за допомогою методів онлайн-платежів, щоб відновити доступ до вашої системи або даних. Методи онлайн-платежів зазвичай включають віртуальні валюти, такі як біткойни. Програми-вимагачі є одним із найпоширеніших методів атак.

Програми-вимагачі проникають у комп'ютерні мережі та шифрують файли за допомогою шифрування з відкритим ключем. На відміну від інших шкідливих програм, цей ключ шифрування залишається на сервері кіберзлочинця. Кіберзлочинці вимагатимуть викуп за цей закритий ключ. Кіберзлочинці використовують шифрування як зброю, щоб тримати дані в заручниках.

Програми-вимагачі важко виявити, поки не стане надто пізно, і методи програм-вимагачів продовжують розвиватися. Через це ваша установа має зосередитися на профілактичних зусиллях. Профілактичні заходи включають навчання співробітників і жорсткий контроль безпеки інформації.

Департамент оборони бізнесу (DOB) настійно рекомендує підприємствам розробляти надійні плани безперервності бізнесу (ББ) для забезпечення стійкості та швидкого відновлення у випадку потенційних загроз. В умовах зростаючого ризику атак програм-вимагачів, такі плани є ключовим інструментом для забезпечення продовження діяльності підприємства під час кризових ситуацій. Правильно створений та регулярно вдосконалюваний план безперервності бізнесу дозволяє компаніям ефективно реагувати на інциденти та мінімізувати їхні наслідки.

Плани реагування на інциденти в рамках безперервності бізнесу визначають послідовність дій та процедури, які необхідно виконати для швидкого та ефективного відновлення роботи підприємства після інциденту, зокрема, атаки

програм-вимагачів. Ці плани враховують вплив інцидентів на інфраструктуру, персонал та клієнтів, а також визначають ролі та відповідальності відповідних членів команди управління кризовими ситуаціями.

Важливим елементом планів безперервності бізнесу є проведення регулярних тренувань та вправ, щоб переконатися в їхній ефективності та готовності персоналу до дії у кризових ситуаціях. Добре підготовлений персонал може допомогти у вчасному та правильному впровадженні планів реагування на інциденти та уникненні серйозних наслідків для підприємства.

Взагалі, розробка та ефективне використання планів безперервності бізнесу є критичними компонентами управління ризиками та забезпеченням стабільності діяльності компанії навіть у непередбачуваних обставинах.Розподілені атаки на відмову в обслуговуванні (DDoS).

DDoS-атаки роблять онлайн-сервіс недоступним, перевантажуючи його надмірним трафіком із багатьох місць і джерел. Час відповіді веб-сайту сповільнюється, запобігаючи доступу під час DDoS-атаки. Кіберзлочинці створюють великі мережі заражених комп’ютерів, які називаються ботнетами, розміщуючи зловмисне програмне забезпечення. DDoS-атака може не бути основним кіберзлочином. Атаки часто відволікають увагу, тоді як здійснюються інші види шахрайства та кібервторгнення.

Федеральна рада з перевірки фінансових установ (FFIEC) недавно висловила серйозну турботу стосовно зростаючої загрози атак на збій обслуговування через переповнення каналів (DDoS) у фінансовому секторі. Ця загальна заява відзначає важливість вживання заходів для захисту фінансових установ від таких атак, які можуть призвести до великих ризиків для функціонування фінансових послуг і піддачі великому тиску фінансові організації.

У заяві FFIEC наголошує на важливості розробки та впровадження ефективних стратегій зменшення ризиків DDoS-атак. Це включає в себе усвідомлення власного рівня загрози, застосування технічних заходів безпеки, а також вивчення та впровадження найкращих практик відповідно до рекомендацій

FFIEC. Забезпечення високого рівня готовності та реагування на DDoS-атаки є невід'ємною частиною управління кібербезпекою в фінансовому секторі.

Додаткові ресурси, які FFIEC обіцяє, включають надання підтримки та вказівок для фінансових установ щодо підготовки та реагування на DDoS-атаки. Це може включати в себе доступ до інформаційних матеріалів, вебінарів або консультацій, спрямованих на покращення здатностей фінансових установ боротьби з цим типом кіберзагроз.

В цілому, FFIEC вчинила крок у напрямку підвищення свідомості та захисту фінансових установ від DDoS-атак, визначаючи їх як серйозну загрозу і надаючи додаткові ресурси для підтримки управління цим ризиком.

Спам і фішинг

Спам включає в себе небажані, небажані або небажані повідомлення та електронні листи. Фішинг — це форма соціальної інженерії, включаючи спроби отримати конфіденційну інформацію. Здається, що спроби фішингу походять від надійної особи чи компанії.

Кіберзлочинці видають себе за офіційного представника, надсилаючи вам електронний лист або повідомлення з попередженням, пов'язаним із інформацією вашого облікового запису. У повідомленні часто буде запропоновано відповісти за посиланням на підроблений веб-сайт або електронну адресу, де ви надасте конфіденційну інформацію. Формат повідомлення, як правило, виглядатиме легітимним із використанням відповідних логотипів і назв. Будь-яка інформація, введена за фейковим посиланням, переходить до кіберзлочинця.

Федеральне бюро розслідувань (ФБР) розробило набір порад, спрямованих на запобігання фішинговим атакам, визнаючи цей вид кіберзагрози як один із найпоширеніших і найсерйозніших. У своїх рекомендаціях ФБР акцентує на важливості збереження особистої та фінансової інформації в безпеці від атак, які спрямовані на вибухове підіймання даних та паролів.

ФБР підкреслює важливість освіти користувачів стосовно виявлення фішингових атак. Вони рекомендують уникати кліків на підозрілі посилання, особливо тих, що надійшли у непроханій електронній пошті чи повідомленнях.

Додатково, наголошується на важливості перевірки достовірності веб-сайтів та уникання введення особистої інформації на сумнівних ресурсах.

Однією з ключових порад є ретельна перевірка електронної адреси відправника перед відкриттям листа чи файлу. ФБР вказує, що зловмисники часто вдаються до підробки адрес відомих і довірених компаній, тому ретельне перевіряння є критичним кроком для запобігання атак.

Також, ФБР рекомендує регулярно оновлювати програми та операційні системи, оскільки це допомагає у закриванні потенційних вразливостей, які можуть бути використані зловмисниками для атак.

Узагальнюючи, ФБР акцентує на освіті, обачності та ретельності при взаємодії з електронними повідомленнями для зменшення ризиків фішингових атак.

Захоплення корпоративного рахунку (CATO)

CATO — це крадіжка суб'єкта господарювання, коли кіберзлодії видають себе за компанію та надсилають неавторизовані транзакції банківського переказу та ACH. Несанкціоновані кошти надсилаються на рахунки, контрольовані кіберзлочинцем.

Багато підприємств уразливі до атаки CATO. Легкими мішенями стають установи зі слабким комп'ютерним захистом і мінімальним контролем систем онлайн-банкінгу. Ця форма кіберзлочинності може призвести до великих збитків. Кіберзлочинці використовують зловмисне програмне забезпечення для зараження комп'ютера через електронну пошту, веб-сайти або зловмисне програмне забезпечення, замасковане під програмне забезпечення.

Конференція наглядових органів державних банків (CSBS) розробила документ із найкращої практики для Комплексного Аналізу та Тестування Оперативної готовності (CATO). Цей документ становить ключовий ресурс для управління ризиками та підвищення стійкості фінансових установ перед можливими кризовими ситуаціями.

CSBS визначає стратегічні та тактичні аспекти CATO, вказуючи на необхідність розробки ретельного плану дій, який охоплює всі сфери банківської діяльності. В документі розглядаються найкращі практики щодо оцінки ризиків,

розробки сценаріїв для тестування, взаємодії з іншими установами та органами нагляду.

Основною метою CATO є забезпечення готовності банків до різних кризових ситуацій, таких як кібератаки, природні лиха чи економічні збої. Документ CSBS визначає рекомендації для впровадження стратегій реагування та відновлення після подій, а також встановлює стандарти ефективного та прозорого взаємодії між банками та регулюючими органами.

Виведення готівки через банкомат

ATM Cash Out – це різновид шахрайства з використанням банкоматів на великі долари. Кеш-аут передбачає одночасне зняття великої кількості готівки в кількох банкоматах у багатьох регіонах. Це також може включати великі зняття в одному банкоматі.

Cash Out зазвичай стосується малих і середніх фінансових установ. Атака передбачає зміну налаштувань веб-панелі керування банкоматом. Кіберзлочинці змінюють функцію видачі банкомату на «Необмежені операції». Налаштування «Необмежені операції» дозволяє знімати кошти понад баланс рахунку клієнта або понад ліміт готівки в банкоматі. Викрадені дані банкомату або дебетової картки часто використовуються для зняття коштів. У результаті ваша фінансова установа може зазнати великих збитків.

DOB рекомендує переглянути ваш контроль над мережами інформаційних технологій, системами авторизації емітентів карток, системами, які керують параметрами банкоматів, а також процесами виявлення шахрайства та реагування на них, щоб запобігти атакам ATM Cash Out.

FFIEC виступила зі спільною заявою щодо кібератак на банкомати та системи авторизації карток фінансових установ.

2.2 Засоби та Методи Атак

Кібератаки стають все більш складними та розповсюдженими, використовуючи різноманітні засоби та методи для неправомірного доступу,

знищення чи крадіжки інформації. Розглянемо деякі з найбільш типових засобів та методів кібератак, а також способи захисту від них.

1. Малвара (Malware), яка включає віруси, черв'яки, троянські програми та інші форми шкідливого програмного забезпечення, є серйозною загрозою для інформаційної безпеки. Ці засоби використовують різні методи для проникнення в систему та завдання шкоди, такі як введення шкідливого коду для отримання контролю над системою, викрадення або пошкодження даних.

Методи атак включають в себе розсилання заражених файлів через електронну пошту, використання вразливостей у програмах або операційних системах для несанкціонованого доступу, а також імітацію легітимних додатків для обману користувачів.

Захист від малвари вимагає комплексного підходу, який включає регулярне оновлення антивірусного програмного забезпечення для виявлення та вилучення нових загроз, фільтрацію електронної пошти для блокування заражених вкладень та обмеження прав користувачів для уникнення несанкціонованого доступу.

2. Фішинг є методом соціально-інженерної атаки, який використовує різні засоби та методи для маніпулювання користувачами з метою видачі конфіденційної інформації, такої як паролі чи банківські реквізити.

Цей вид атаки може включати в себе надсилання спам-повідомлень, створення фіктивних веб-сайтів або електронних листів, що імітують легітимні джерела, а також використання соціальних мереж для отримання доступу до конфіденційної інформації.

Захист від фішингу включає в себе освіту користувачів, щоб вони були уважні до підозрілих повідомлень та веб-сайтів, перевірку достовірності веб-сайтів перед введенням конфіденційної інформації, а також використання антиспам-фільтрів для виявлення та блокування фішингових повідомлень.

3. DDoS-атаки (атаки з відмовою в обслуговуванні) – це метод, при якому використовуються засоби, такі як зомбі-комп'ютери та ботнети, для переповнення мережевих ресурсів і відмови в обслуговуванні легітимних користувачів.

Ці атаки спрямовані на те, щоб перевантажити цільовий вузол, мережу чи службу, роблячи їх недоступними для користувачів. Для захисту від DDoS-атак використовуються спеціалізовані системи, які виявляють та фільтрують надмірний трафік, а також можливе резервування мережевих ресурсів для забезпечення неперервності обслуговування навіть під час атак.

4. Зломування паролів – це процес, при якому використовуються засоби, такі як брутфорс, словники та атаки на паролі, для спроб вгадати або зламати паролі і отримання неправомірного доступу до облікових записів.

Цей метод атаки найчастіше використовується для отримання несанкціонованого доступу до особистої інформації, електронної пошти чи інших захищених ресурсів. Захист від зломування паролів включає в себе використання складних та унікальних паролів, які важко вгадати, а також впровадження двофакторної аутентифікації для додаткового шару безпеки.

5. Стеганографія – це метод, при якому інформація приховується в мультимедійних файлах, таких як зображення, аудіофайли або відеофайли, з метою непомітного передавання даних.

Зловмисники можуть вбудовувати приховані повідомлення в файл, не порушуючи зовнішнього вигляду або якості мультимедійного контенту. Захист від стеганографії включає в себе регулярну перевірку мультимедійних файлів на наявність прихованої інформації та використання антивірусного програмного забезпечення для виявлення потенційних загроз.

6. Zero-Day вразливості виникають при використанні неопублікованих слабкостей у програмному забезпеченні, і зловмисники використовують ці вразливості до того, як розробник випустить відповідний патч чи оновлення.

Один з основних методів захисту від Zero-Day вразливостей - це регулярне оновлення програмного забезпечення. Забезпечення своєчасних патчів та оновлень важливо для усунення вразливостей, які можуть бути використані зловмисниками. Крім того, моніторинг нових вразливостей і швидке реагування на їхнє виявлення також є важливими елементами стратегії захисту.

7. Соціальний Інжиніринг є методом атаки, при якому зловмисники використовують маніпулювання інформацією та психологічний тиск для отримання чутливої інформації від людей шляхом обману чи впливу на їхню поведінку.

Один із засобів захисту від соціального інжинірингу - це навчання персоналу. Регулярні тренінги та освіта щодо методів атак та ознак соціального інжинірингу можуть підвищити обізнаність персоналу та допомогти їм впізнавати потенційні загрози.

Важливим елементом захисту є також встановлення строгих правил обробки інформації. Обмеження доступу до чутливих даних та використання політик безпеки допомагає уникнути ситуацій, коли зловмисники можуть використовувати соціальний інжиніринг для незаконного доступу до інформації.

2.3. Сценарії Атак та їх Поширення

Кібератаки можуть приймати різноманітні форми та використовувати різні сценарії для досягнення своїх цілей. Нижче наведено кілька типових сценаріїв атак та їх можливе поширення:

1. Фішингові Кампанії:

Сценарій: Атакуючі відправляють спам-повідомлення, що містять фішингові посилання або вкладення, на велику кількість адрес електронної пошти. Користувачі, отримавши такі повідомлення, можуть бути перенаправлені на підроблені веб-сайти, де їм може бути запропоновано ввести конфіденційну інформацію.

Поширення: Якщо один користувач стає жертвою, атака може розповсюдитися через адресну книгу його контактів або шляхом використання його облікового запису для подальшого відправлення фішингових повідомлень.

2. Використання Малвари:

Сценарій: Атакуючі вбирають малвару в легітимне виглядати програмне забезпечення, що може призвести до її встановлення на цільові системи. Малвара

може використовуватися для збору даних, встановлення додаткових загроз або навіть викрадення контролю над системою.

Поширення: Малвара може використовувати мережеві вразливості для самостійного поширення або включати в себе механізми соціальної інженерії для отримання доступу до інших систем.

3. DDoS-Атаки:

Сценарій: Атакуючі масовано генерують запити до цільового сервера чи мережі, завдаючи їм перевантаження. Це може призвести до відмови в обслуговуванні для легітимних користувачів.

Поширення: Атака може бути розповсюджена через ботнет, де багато комп'ютерів або пристроїв використовуються для одночасного генерування трафіку.

4. Використання Zero-Day Вразливостей:

Сценарій: Атакуючі використовують невідомі вразливості в програмному забезпеченні до того, як вони стають відомими розробникам. Це може дати їм можливість невиявленого доступу до систем.

Поширення: Атака може бути розширена на інші системи, які також мають ту саму вразливість, або використана для розвідки та підготовки до подальших атак.

5. Атаки на Системи Сніфінгу та Інтерсептації:

Сценарій: Зловмисники використовують засоби для перехоплення та аналізу трафіку мережі для здобуття конфіденційної інформації, такої як паролі чи дані кредитних карток.

Поширення: Отримана інформація може бути використана для подальших атак або продана на чорному ринку.

Захист від таких сценаріїв атак включає в себе використання заходів безпеки, вдосконалення політики доступу та постійне моніторинг і виявлення інцидентів для своєчасного реагування на потенційні загрози

2.3.1. Огляд та архітектура платформи Alcatel 5020 Softswitch

SolarWinds:

Сценарій: У грудні 2020 року сталася одна з найбільших кібератак, коли зловмисники внедрили шкідливий код у програмне забезпечення SolarWinds, яке використовувалося тисячами організацій та урядових структур. Це надзвичайно вдосконалена атака, яка тривала місяці та дозволила зловмисникам отримати доступ до чутливої інформації.

Поширення: Шкідливий код вплинув на тисячі організацій, оскільки вони використовували заражений софт. Зловмисники отримали можливість шпигувати за користувачами, здобувати конфіденційну інформацію та навіть створювати імітацію юридичних осіб.

2. WannaCry:

Сценарій: У 2017 році вірус-вимагач WannaCry атакував комп'ютери під управлінням операційних систем Windows, використовуючи вразливість, яку розробники не виправили. Вірус заблоковував доступ до файлів та вимагав викуп у криптовалюті за їх розблокування.

Поширення: WannaCry поширювався через мережеві вразливості, використовуючи засоби автоматичного поширення в мережі. Імпакт атаки відчували компанії та організації у всьому світі.

3. Phishing атаки на електронну пошту:

Сценарій: Фішингові атаки на електронну пошту залишаються одними з найпоширеніших. Атакуючі відправляють користувачам листи, що імітують легітимні повідомлення від банків, компаній чи інших організацій з метою викликати реакцію, яка може призвести до розголошення конфіденційної інформації.

Поширення: Якщо один користувач стає жертвою фішингової атаки, атакуючі можуть використати його облікові дані для подальшого розсилання фішингових повідомлень його контактам, розширюючи таким чином атаку.

4. Ransomware атаки на галузь охорони здоров'я:

Сценарій: У 2021 році стало відомо про рекордну кількість атак на галузь охорони здоров'я, де вірус-вимагачі блокували доступ до медичних систем і вимагали викуп.

Поширення: Зловмисники використовували спеціалізовані методи для атак на медичні заклади, де вони блокували доступ до медичної інформації та доводили, що це може загрожувати пацієнтам.

Висновок:

Аналіз реальних сценаріїв кібератак вказує на те, що загрози щоразу стають більш вдосконаленими та небезпечними. Захист від таких атак вимагає комплексних заходів, включаючи понадмежевий моніторинг, оновлення програмного забезпечення та ефективну освіту користувачів

2.4. Вплив Кіберзагроз на Інфраструктуру

1. Вплив на Енергетичну Інфраструктуру:

Кіберзагрози мають потенціал серйозно впливати на енергетичні системи. Наприклад, атаки на енергетичні об'єкти можуть призвести до відключення електроенергії для великих територій, що може мати негативний економічний та соціальний вплив.

2. Загрози для Транспортної Інфраструктури:

Кіберзагрози стають серйозним обліком для транспортних систем, таких як системи управління рухом транспорту та системи автоматизації. Атаки можуть спричинити хаос у роботі транспортної інфраструктури, включаючи перешкоди в роботі автоматичних систем та безпеку пасажирів.

3. Кіберзагрози для Фінансової Інфраструктури:

Фінансова інфраструктура є особливо привабливою для кіберзлочинців. Атаки можуть впливати на банківські системи, електронні платіжні системи та інші фінансові послуги. Розголошення фінансової інформації може призвести до великих втрат та порушень конфіденційності.

4. Віддалені Атаки на Критичну Інфраструктуру:

Критична інфраструктура, така як системи водопостачання та обробки відходів, може бути предметом віддалених кібератак. Порушення в роботі цих систем може викликати серйозні екологічні проблеми та загрожувати здоров'ю громадян.

5. Загрози для Телекомунікаційної Інфраструктури:

Телекомунікаційна інфраструктура є ключовою для забезпечення зв'язку та обміну інформацією. Кібератаки на телекомунікаційні системи можуть спричинити відключення мережі, перешкоджаючи комунікації та доступу до інтернету.

Наслідки та Висновок:

Вплив кіберзагроз на інфраструктуру є широким та загрозливим. Враховуючи зростання кількості підключених пристроїв та автоматизованих систем, необхідно надавати пріоритет безпеці та захисту інфраструктури від кібератак. Ефективна кібербезпека вимагає постійного моніторингу, вдосконалення заходів захисту та готовності до виявлення та реагування на кіберзагрози.

2.4.1. Оцінка можливого впливу кіберзагроз на телекомунікаційну інфраструктуру

1. Відмова мережі та послуг: Кіберзагрози можуть призвести до відмови в роботі мережі та послуг телекомунікацій. Наприклад, DDoS-атаки можуть переповнити мережеві ресурси, призводячи до відмови у наданні послуг і відсутності зв'язку для користувачів.

2. Крадіжка та розголошення конфіденційної інформації: Атаки на телекомунікаційні системи можуть спрямовуватися на крадіжку конфіденційної інформації, такої як особисті дані користувачів або комерційні таємниці компаній. Це може мати серйозні наслідки для приватності та безпеки.

3. Втручання в роботу мережі: Кіберзагрози можуть викликати втручання в роботу мережевої інфраструктури. Наприклад, атаки на рівень маршрутизації можуть призвести до перенаправлення трафіку та порушення нормального функціонування.

4. Вплив на якість обслуговування (QoS): Атаки на телекомунікаційну інфраструктуру можуть впливати на якість обслуговування, знижуючи швидкість передачі даних та спричиняючи перерви в з'єднанні. Це може викликати невдоволення користувачів та втрату довіри.

5. Вплив на безпеку та інтегрітет даних: Кіберзагрози можуть ставити під загрозу безпеку та інтегрітет передаваних даних. Шкідливі програми, такі як віруси або шифровальники, можуть викликати виток чи пошкодження інформації, що передається через мережу.

Висновок: Забезпечення безпеки та надійності телекомунікаційної інфраструктури в умовах постійної загрози кібератак є надзвичайно важливим завданням. Ефективні заходи кібербезпеки повинні включати моніторинг, виявлення та відповідь на інциденти, а також вдосконалення захисних механізмів для забезпечення стійкості мережі та забезпечення надійності обслуговування користувачів.

2.5. Оцінка Ризиків та Пріоритизація

Оцінка ризиків у телекомунікаційній сфері передбачає проведення комплексного аналізу для ідентифікації потенційних загроз та вразливостей. Цей процес включає в себе аналіз можливих атак, виявлення слабких місць у мережі, а також оцінку інших факторів, які можуть призвести до виникнення проблем в системі телекомунікацій.

Ризики в телекомунікаціях можна класифікувати за різними параметрами. Перш за все, важливо оцінити ймовірність виникнення загрози, що дозволяє передбачити ймовірність виникнення негативних подій. Далі, важливо визначити потенційний вплив цих загроз на систему телекомунікацій, оцінивши можливі наслідки виникнення ризикованих ситуацій. Крім того, важливим етапом є визначення рівня уразливості системи, що може вплинути на те, наскільки швидко та ефективно система може відновитися після атаки чи інциденту.

Цей комплексний підхід дозволяє структурувати ризики та визначити їх серйозність, надаючи можливість зосередитися на найбільш критичних аспектах безпеки телекомунікацій.

Після ідентифікації ризиків, важливо визначити їх пріоритетність. Пріоритизація ґрунтується на двох ключових чинниках - ймовірності виникнення

загрози та потенційному впливі. Це допомагає визначити, які ризики потребують найбільш уваги та ресурсів для запобігання.

Після пріоритизації ризиків розробляються стратегії для їх мінімізації та управління. Цей етап включає в себе прийняття конкретних заходів для запобігання та обмеження можливих загроз. Одним із засобів є впровадження захисних заходів, таких як використання вогнеметів, інтрузійних систем, антивірусного програмного забезпечення та інших засобів, що допомагають виявляти та блокувати потенційні атаки.

Резервне копіювання даних є ще однією важливою стратегією. Регулярне створення резервних копій дозволяє відновлювати дані у випадку їх втрати чи пошкодження в результаті кібератак або інших інцидентів. Також важливим елементом стратегії є тренування персоналу з питань кібербезпеки, щоб забезпечити свідомість та готовність працівників до можливих сценаріїв атак.

Цей комплекс заходів створює надійну систему захисту, що сприяє зменшенню ризиків та забезпеченню стійкості та надійності телекомунікаційної мережі.

2.5.1 Методи оцінки ризиків та їх застосування в контексті кібербезпеки

Оцінка ризиків у сфері кібербезпеки - це систематичний процес, який включає в себе ідентифікацію, аналіз та оцінку потенційних загроз і вразливостей. Декілька методів використовуються для визначення ризиків та їх можливого впливу.

Одним із основних методів є **кваліативний аналіз**, що базується на експертному оцінюванні. В цьому випадку, фахівці в області кібербезпеки визначають ймовірність виникнення загроз та їх потенційний вплив, використовуючи свій досвід та знання.

Інший підхід - **кількісний аналіз**, який використовує конкретні числові значення для оцінки ризиків. Це може включати в себе визначення фінансових втрат, ймовірності атаки, та інших кількісних параметрів.

Додатково, використовується метод **SWOT-аналізу** (аналіз сильних і слабких сторін, можливостей та загроз). Цей підхід дозволяє визначити внутрішні та зовнішні фактори, що можуть впливати на ризики кібербезпеки.

Крім того, існують різні методи оцінки ризиків у телекомунікаційній сфері, такі як аналіз дерева вирішень, який дозволяє враховувати різноманітні сценарії та їх ймовірності. Цей метод дозволяє систематично вивчати можливі наслідки виникнення ризиків і визначати оптимальні шляхи дій для мінімізації чи уникнення їх.

Застосування цих методів важливо для створення не лише об'єктивного уявлення про потенційні загрози, але й для розробки конкретних стратегій їх запобігання та мінімізації. Це стає ключовим елементом комплексного підходу до кібербезпеки в телекомунікаціях.

Комплексний підхід до оцінки ризиків дозволяє ефективно враховувати різноманітні аспекти безпеки та визначати пріоритети для впровадження заходів забезпечення безпеки та стійкості кіберінфраструктури. Такий підхід сприяє розробці імовірних та ефективних стратегій кіберзахисту, що є критичним для забезпечення надійності та безпеки телекомунікаційних систем.

ВИСНОВКИ ДО РОЗДІЛУ 2

У світлі наших розділених вивчень, стає очевидним, що динамічний розвиток технологій надає кіберзагрозам новий рівень складності та різноманітності. Класифікація різних типів кіберзагроз сприяє глибшому розумінню їхнього впливу на телекомунікаційні мережі, враховуючи як технічні аспекти, так і соціально-економічні фактори.

У практиці, засоби та методи кібератак охоплюють широкий спектр від традиційних до новаторських. Врахування реальних сценаріїв атак і їхнього поширення є ключовим в комплексному розумінні динаміки кіберзагроз. Сучасні тенденції використання штучного інтелекту, квантових технологій та блокчейну додають нові аспекти до стратегій кіберзахисту.

Важливість оцінки можливого впливу кіберзагроз на телекомунікаційну інфраструктуру стає настільки ж невід'ємною, скільки й реалізація ефективних методів пріоритизації ризиків. Розвиток цих методів важливий для забезпечення гнучкості та адаптивності стратегій кіберзахисту в умовах постійної зміни технологічного ландшафту.

Таким чином, ми приходимо до висновку, що сучасні умови вимагають комплексного підходу до кібербезпеки, що включає в себе не лише технічні заходи, а й соціальні, правові та етичні аспекти. Лише інтегрований підхід забезпечить ефективний захист телекомунікаційних мереж в умовах непередбачуваного кіберзлочинства та швидкозмінюваних технологій.

РОЗДІЛ 3 РОЗРОБКА СТРАТЕГІЙ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ВІД КІБЕРАТАК

3.1. Мережеве шифрування та стратегії захисту

В області мережевої безпеки важливо приймати фізичні та програмні запобіжні заходи. Це включає захист базової мережевої інфраструктури від несанкціонованого доступу, уникнення неправильного використання, модифікації чи руйнування даних, а також забезпечення конфіденційності інформації, щоб створити безпечне середовище для комп'ютерів, користувачів та додатків.

Ефективна боротьба з вразливостями починається саме з мережі. Управління вразливістю мережі охоплює всі складові середовища, такі як підключені пристрої, операційні системи, апаратне і програмне забезпечення, а також небезпечні пристрої, як от маршрутизатори Wi-Fi та Інтернет речей.

Неправильна конфігурація брандмауера або надмірний контроль доступу можуть стати точкою входу для зловмисників у систему. Регулярне встановлення патчів і виправлень є ключовим для забезпечення безпеки даних та запобігання можливим витокам інформації.

Інформаційно-комунікаційні технології (ІКТ) мають значний вплив на безпеку даних і мереж. Правильна конфігурація, постійне вдосконалення та регулярне оновлення захисту є необхідними для ефективного захисту мережі від потенційних загроз.

Тема соціального забезпечення, економічного зростання та національної безпеки в сучасному світі тісно пов'язана з використанням інформаційно-комунікаційних технологій (ІКТ). ІКТ охоплюють широкий спектр технологій, таких як комп'ютери, мобільні пристрої та мережі. У цьому контексті важливо враховувати також загрози, які ставлять перед собою мережі зловмисників, кіберзлочинців та інші агенти.

Протидія шкідливій кібер-активності визначається міжнародними пріоритетами та ключовими напрямками досліджень. Ефективне впровадження та вдосконалення заходів безпеки є важливим завданням, оскільки це допомагає забезпечити інформаційну та національну безпеку.

Виявлення вразливостей в інформаційних і телекомунікаційних мережах є одним із ключових завдань. Використання інструментів та методів для сканування та моніторингу мережі дозволяє ефективно виявляти і усувати інформаційні вразливості. Одним із ефективних засобів є мережеві сканери, які допомагають проводити ретельний аналіз мережі та виявляти слабкі місця.

Загалом, впровадження передових методів інформаційно-комунікаційної безпеки є важливою складовою стратегії для забезпечення стабільності та безпеки сучасних суспільств.

Існує ряд утиліт, які можуть бути використані для виявлення уразливостей в мережах, будь то в домашньому оточенні або в корпоративному середовищі. Важливо розглянути ефективність цих інструментів та методів у попередженні небажаних загроз та захисті даних.

Для досягнення ефективності безпеки в інформаційно-комунікаційних мережах необхідно розвивати і вдосконалювати існуючі методи та створювати власні рішення для виявлення уразливостей. Врахування особливостей конкретного середовища, в якому використовуються ці інструменти, може забезпечити більш точне та адаптоване до умов застосування виявлення уразливостей.

Ряд статей [1-2] визначає основні проблеми та виклики, пов'язані з інформаційно-комунікаційною безпекою, і надає ключові моменти, які можуть бути використані для розуміння динаміки цього сектору. Інші джерела [3-9, 18, 19] досліджують різні методи протидії загрозам в інформаційно-комунікаційних мережах.

Мета статті полягає в вивченні поточного стану інформаційної безпеки в інформаційно-комунікаційних мережах і визначенні ключових тенденцій та викликів, які стоять перед цією галуззю.

3.2. Аналіз сучасного стану безпеки в інформаційних та комунікаційних мережах та вивчення методів протидії актуальним загрозам

"Аналіз сучасного стану безпеки в інформаційних та комунікаційних мережах та вивчення методів протидії актуальним загрозам" є ключовим етапом дослідження, спрямованого на оцінку рівня вразливості та вивчення заходів для забезпечення безпеки в цих мережах.

Початковий етап аналізу передбачає вивчення сучасного стану безпеки в інформаційних і комунікаційних мережах. Це включає в себе огляд існуючих технологій, протоколів і архітектур, які використовуються в цих мережах, а також ідентифікацію потенційних загроз і вразливостей.

Другий аспект полягає в оцінці ефективності поточних методів безпеки та їх здатності протистояти актуальним загрозам. Аналіз існуючих заходів безпеки, таких як брандмауери, антивіруси, системи виявлення вторгнень, дозволяє визначити їхню дієздатність та визначити прогалини.

Третій етап включає вивчення актуальних загроз, що може включати в себе кібератаки, витоки даних, атаки на конфіденційність та доступність мережевої інфраструктури. Аналіз типів і характеристик цих загроз допомагає розробити стратегії їхнього ефективного запобігання та виявлення.

Четвертий аспект дослідження передбачає розробку та вивчення нових методів протидії, орієнтованих на зменшення ризиків та посилення безпеки в інформаційних та комунікаційних мережах.

У п'ятому етапі формулюються рекомендації та стратегії для вдосконалення систем безпеки в інформаційних і комунікаційних мережах на основі результатів аналізу та вивчення методів протидії актуальним загрозам.

3.2.1. Особливості поточного стану безпеки в інформаційних і комунікаційних мережах

1. Недостатня автентифікація та авторизація: Якщо системи не вимагають достатнього рівня автентифікації (перевірки ідентичності) та авторизації (надання прав доступу), це може створювати ризики несанкціонованого доступу.

2. Відсутність адекватного шифрування даних: Якщо дані передаються або зберігаються без використання ефективних методів шифрування, це може призвести до їхнього неправомірного доступу та витоку.

3. Вразливості програмного забезпечення: Застосунки та операційні системи можуть містити вразливості, які можна використовувати для атак. Важливо регулярно встановлювати оновлення та патчі для забезпечення безпеки.

4. Недостатній моніторинг мережі: Відсутність ефективних систем моніторингу може ускладнити виявлення незвичайної або підозрілої активності в мережі.

5. Соціальний інжиніринг та фішинг: Люди можуть бути слабким ланцюгом у системах безпеки. Зловмисники можуть використовувати соціальний інжиніринг (психологічні методи) або фішинг (шахрайські спроби вибудувати чутливі дані) для обхідництва технічних заходів захисту.

6. Відсутність аудиту та аналізу подій: Без системи аудиту та аналізу подій може бути важко визначити, які дії виконуються в мережі та хто має до них доступ.

7. Використання слабких паролів: Якщо користувачі використовують слабкі паролі або використовують один пароль для кількох облікових записів, це може стати легкою мішенню для атак.

8. Неадекватне керування правами доступу: Надмірні права доступу або невірно налаштовані правила можуть призвести до неправомірного використання ресурсів.

Він сіє хаос. Існує безліч потенційних проблем, але розглядаються деякі з найбільш поширених проблем мережевої безпеки, і основними методами є

Вам буде запропоновано їх вирішити.

Проблема №1. Невідомі джерела в мережі.

Є багато компаній, які не мають повного списку всіх своїх IT-активів

Вони підключені до власної мережі. Це велика проблема. Якщо ви не знаєте всіх активів

Він знаходиться у вашій мережі і як ви можете бути впевнені, що ваша мережа безпечна.

Найпростіший спосіб вирішити цю проблему-перевірити всі пристрої в мережі.、

Визначте всі платформи, на яких вони працюють. Роблячи це, ви можете дізнатися наступне

Всі різні точки доступу в мережі та необхідні точки доступу

Більшість оновлень безпеки.

Проблема №2. Зловживання правами облікового запису Користувача.

Згідно з даними, наданими Harvard Business Review, у 2016 році "це було 60% усіх атак."

Це було зроблено інсайдером " [1].Чи було це викликано чесною помилкою

(Випадкова відправка або втрата інформації на неправильну адресу електронної пошти

Працюючий пристрій), навмисний витік та зловживання привілеями

або крадіжка особистих даних в результаті фішингової кампанії; або

Інші атаки соціальної інженерії, які ставлять під загрозу дані облікового запису Користувача,

Контакти у вашій компанії представляють одну з найбільших проблем безпеки, з якими ви стикаєтесь

Я ніколи його не зустрічав.Тому що ці загрози надходять від довірених користувачів、

Системи також найважче виявити та зупинити.

Однак існують способи мінімізувати ризик у разі внутрішньої атаки. Наприклад, якщо

Ваша компанія використовує політику найменших привілеїв (

POLP) Політика щодо доступу користувачів, ви можете обмежити можливі збитки

Це викликано неправильним використанням облікового запису Користувача. В ПОЛПЕ

Крім того, кожен користувач має обмежений доступ до різних систем і баз даних в мережі жовтня

Тільки те, що їм потрібно для виконання своєї роботи.

Проблема №3. Це немодифікована вразливість.

Багато компаній стурбовані зловживанням нульовим днем. Ці експлойти

Невідомі проблеми безпеки для додатків та систем, які ще не використовуються

Однак уразливість нульового дня не є проблемою, і проблема не вирішена

Відповідно до відомих вразливостей. Як описано в онлайн-статті неурядової організації [2], " 2015 рік

Було виявлено близько 6300 унікальних вразливостей. За даними Symantec, лише 54 з них

Він класифікується як нульовий день."

Це пов'язано з тим, що якщо ви використовуєте експлойт нульового дня, це тому, що

Можна виявити - це буде відома проблема

Постачальник програмного забезпечення може приступити до роботи. найчастіше використовуються експлойти、

Це з більшою ймовірністю буде виявлено та виправлено. Це також вимагає великих зусиль

Самостійно виявляйте абсолютно невідомі уразливості в системі.Ось чому зловмисники часто хочуть використовувати відомі подвиги.

Насправді, як описано в статті ОГС: "звіт Verizon про порушення даних за 2016 рік

Ми показали, що більшість усіх виявлених подвигів були пов'язані із застарілими вразливими місцями безпеки

У 2007 році наступним роком став 2011 рік."[2] іншими словами, вразливості, які існують для більшості

У 2016 році за більшість порушень було призначено 10 років. Найпростіший спосіб

Рішення цієї проблеми-дотримуватися чіткого розкладу оновлень для системи безпеки

. Крім того, поступово змінюйте програми та операційну систему в мережі жовтня наступним чином:

Ви можете спростити цей процес, зробивши його таким же. Наприклад, для кожної системи

Він заснований на Windows або Mac (Mac, Windows, Linux і т.д. Це не комбінація.).), після

Просто дотримуйтесь розкладу жовтневих виправлень безпеки для Mac OS або Windows

Операційна система і повідомлення.

Проблема номер 4.Глибока відсутність захисту.

Нарешті, незважаючи на всі ваші зусилля, настане наступальний день

Ви зможете зламати безпеку своєї мережі. Але наскільки це шкідливо AMI

Зловмисник може викликати залежність від структури мережі.

Проблема в тому, що деякі компанії мають відкриту мережу

Як тільки зловмисник входить в довірену систему, він отримує необмежену структуру

Доступ до всіх систем в мережі.

Якщо мережа складається з сильної сегментації, то всі її окремі частини

Якщо він ізольований, можна уповільнити його достатньо, щоб запобігти нападу

Підключайтеся до критично важливих систем, поки ваша служба безпеки працює над виявленням,

Знайдіть помилки та виправте їх.

Все гаразд, ні. 5. Погане управління IT-безпекою.

Ще одна поширена проблема для багатьох компаній,

У них найкращі рішення для кібербезпеки, у них може не вистачити людей

Правильно керуйте цими рішеннями.

Коли це станеться, важливі попередження про кібербезпеку можуть бути пропущені,

І успішну атаку неможливо вчасно усунути, щоб мінімізувати шкоду.

3.2.2 Вивчення методів протидії сучасним загрозам інформаційно-комунікаційних мереж

Вивчення методів протидії сучасним загрозам інформаційно-комунікаційних мереж. Як протистояти безпеці безпосередньо пов'язано з наступним

Параметри та параметри, що зберігаються як помилки мережі та вразливості

Це призводить до створення мережі зв'язку. Проаналізувавши вплив цих параметрів, ми можемо вибрати

Ось кілька важливих способів протидії мережевій безпеці.

Вибір і застосування цих методів реакції в мережевому середовищі залежить від

У команді мережевих адміністраторів. Це залежить від їх базових знань та обізнаності

Мережа, стандартна мережева архітектура, параметри формату трафіку

Інформація про роботу програми (знання мережевих протоколів OSI і TCP / IP і опис правил роботи програми

мережева безпека), продуктивність мережевого обладнання, загрози безпеці, доступні

Мережеві недоліки. Приблизна або застаріла інформація може виникнути через

Мережеві помилки та вразливості.

Беручи до уваги наведену вище інформацію, багато дослідницьких установ

Ми призначили для вас деякі з найбільш важливих основних методів протидії безпеці

Мережева інфраструктура стандартного рівня [8].

Політика безпеки. Надійна політика безпеки відіграє важливу роль у мережі.

Якщо політика була розроблена після аналізу поведінки мережі та її компонентів, вона буде виглядати так

Це призводить до створення значно безпечної та безперебійної мережі.

Дозволи на ресурси. Підтвердження системи або мережевого ресурсу

Важлива роль у протидії безпеці. Після ретельного вивчення мережі ми можемо призначити

Дозволи відповідного рівня для доступу до системних ресурсів. Захист від вірусів

Політики додатків або списки контролю доступу для маршрутизаторів або брандмауерів

Визначте дозволи для правильного доступу до мережевих ресурсів.

Визначте шкідливу поведінку. Наявність системи виявлення вторгнень зіграє свою роль

Важлива роль у протидії безпеці. Досліджуйте та аналізуйте файли журналів на предмет шкідливої активності

Ви можете зареєструвати систему в мережі. Це забезпечує простий підхід до безпеки для багатьох людей

Інші шкідливі цілі

Це зменшує ймовірність нападу на мережу. Ознаки зловмисних атак говорять нам

Будь-яке уявлення про те, який захист потрібна системі від цієї атаки. Ми можемо це зробити

Для переналаштування або переналаштування параметрів системи безпеки:

Потужна перешкода для атаки.

Виправте реальну проблему. Вирішіть основні проблеми системи або мережі, ми можемо зареєструвати систему або мережу. ці основні, але важливі питання в основному AMI

Приховані точки, присутні в будь-якій звичайній мережі або системі, наприклад

Наприклад, неправильні оновлення системних додатків, застарілі програми та віруси

Оновлення виправлень (не вчасно) можуть створювати недоліки безпеки для всіх мереж.

Що стосується інструментів заходів безпеки, до них відносяться: 1).

Метод захисту від шифрування, тобто безпечний протокол IPSec і SSL; 2) Система

Виявлення вторгнень (IDS), яке може виявляти несанкціонований доступ

Або вторгнення в систему чи мережу. Це рішення для забезпечення безпеки з пасивною позицією.

Система або Мережа проти цих вторгнень. Властивість ідентифікатори в мережевому розгортанні

Контролюйте трафік або мережеву активність, не впливаючи на трафік [10,11].3) вторгнення

Превентивна система (IPS), яка служить захистом від будь-яких вторгнень, які відбуваються

У мережі або локальній системі. Працює на основі виведення

Ідентифікатори файлів системного журналу. Таким чином, ми можемо сказати, що система IPS є розширенням системи IDS;

4) затоплення брандмауера. Брандмауер-це бар'єр, який виконує ізоляцію між 2 дек.

Різні мережі або системи. Визначте, який тип трафіку може проходити

Мережа і в якому напрямку. Брандмауер надає наступні жовтневі додаткові рівні

Захист, що забезпечує можливість додавання набагато більш суворих і складних протоколів

Між різними сегментами мережі або регіонами. Декомунізація мережі. Брандмауер може містити лише 1 систему

Або складається з декількох систем. Про його роль у мережевій безпеці、

Захистіть одну мережу від іншої.

Брандмауер в мережі-це створення бар'єру між 2 сет декомунізацією. -до

Для цього у вас повинно бути принаймні два мережеві інтерфейси.

Інші призначені для захисту, а інші - для загальнодоступних мереж [13]. Брандмауер

Захистіть свою внутрішню мережу від зовнішніх мереж.5) Сурикота-професіонал

Програмне забезпечення для аналізу мережі та виявлення загроз з відкритим кодом

Він використовується і застосовується в більшості приватних і державних установ

Великими постачальниками для захисту своїх активів.

Як бачите, кожен з розглянутих методів протидії сучасним загрозам включає в себе:

Плюси і мінуси. Про те, що ці методи можуть забезпечити надійний захист

Що стосується мереж, то єдина відмінність полягає в тому, наскільки ефективно кожен з них може це зробити

І які зусилля для цього потрібні. на основі досліджень,

Було виявлено використання двох найбільш ефективних методів: брандмауера і сурикати. Бувши

Для брандмауерів він заснований на використанні обох алгоритмів шифрування

І напишіть правила, які є ефективними рішеннями для захисту мережі. Коли ми розмовляємо

Що стосується сурикати, то тут також використовується відповідна комбінація з 2 методів, а саме. посвідчення особи та посвідчення особи.

Також IP-адреси, які допомагають підвищити безпеку та безперебійну роботу мережі.

3.3. Експериментальне вивчення поточного стану безпеки в інформаційних і комунікаційних мережах та дослідження методів протидії сучасним загрозам інформаційно-телекомунікаційних мереж

Ми проаналізували загрози та вразливості з урахуванням основних проблем

інформаційні та комунікаційні мережі та методи розслідування цих загроз

Крім того, напій два методи для більш сильної захисту і талант, була визначена переміщення

Зберігайте наші дані від зловмисників і зберігайте конфіденційність、

Безпечне функціонування інформації у великих організаціях, державних мережах

Установи та критично важливі об'єкти інфраструктури.

Брандмауери-найпоширеніша технологія захисту внутрішніх ресурсів. О...

Основна мета-відстежувати вхідний і вихідний мережевий трафік, аналізуючи його наступним чином:

Пакети даних і, відповідно, вирішіть, чи слід їх пропускати

У заздалегідь визначеному наборі правил

Мережеве шифрування захищає дані, що проходять через мережу зв'язку. Стандарт Secure Sockets Layer (SSL) (технологія, що лежить в основі символу блокування браузера, більш точно звана Transport layer security [TLS]) [14] вказує, що багато компаній, які цінують мережеву безпеку для інтернет-комунікацій, зацікавлені не тільки в інтернет-трафіку, але і у внутрішніх мережах. корпоративні магістральні мережі і т. д. Він також використовує шифрування мережевого рівня для захисту вашої мережі та віртуальних приватних мереж (VPN).Однак, як і у

випадку з іншими методами безпеки низького рівня, шифрування даних на мережевому рівні є досить грубим інструментом. Мережа майже повністю не бачить значення, надіслані через неї, і відсутність цього контексту часто налаштовується таким чином, щоб захищати все або нічого. І навіть при використанні підходу "захисти все" потенційні зловмисники можуть отримати цінну інформацію з моделі мережевого трафіку.Шифрування даних у міру їх проходження по мережі є лише частиною комплексної стратегії шифрування мережевих даних. Організації також повинні враховувати ризики у своїх джерелах та кінцевих пунктах призначення, перш ніж передавати інформацію. Тому виникають питання, пов'язані з вибором методів шифрування в інформаційно-комунікаційних мережах.Розглядаючи функціональність брандмауера в попередньому параграфі, ми виявили, що захист мережі базується на налаштуванні конфігурації обладнання та створенні відповідних правил (дозволів та заборон). Таким чином, цей метод в інформаційно-комунікаційних мережах (ІТМ) служить ефективним інструментом для виявлення вразливостей і встановлення належної мережевої безпеки.Ми аналізуємо ці функції в брандмауерах і пропонуємо використовувати потокове шифрування на основі регістрів зсуву з лінійним зворотним зв'язком (rdlz) з урахуванням структурних особливостей захищених мереж.Цей метод полягає у створенні алгоритму потокового шифрування, який перетворює відкритий текст у байтах у код, який неможливо прочитати без відповідного ключа.Потокові шифри є лінійними, тому той самий ключ шифрує та розшифровує повідомлення. Всі методи шифрування спрямовані на кодування, щоб приховати дані ззовні. Однак, на відміну від своїх аналогів, потокові шифри не групують повідомлення і не розшифровують його блоками, а використовують всі містяться в повідомленні PyCharmCommunity Edition2021.2.2 для включення потокового шифрування на основі регістрів з лінійним зворотним зв'язком (RZLZZ) в брандмауері. Як подати заявку на наступні операції в algo, якщо бути точним: 1. Генерація псевдовипадкової послідовності RDLZ.2. Використовуйте тест FIPS-140-1.3 для перевірки отриманої псевдовипадкової послідовності. Перевірте право доступу до маршрутизатора.4. Виявлення вразливостей мережевої безпеки 5. Правильне закриття програми.

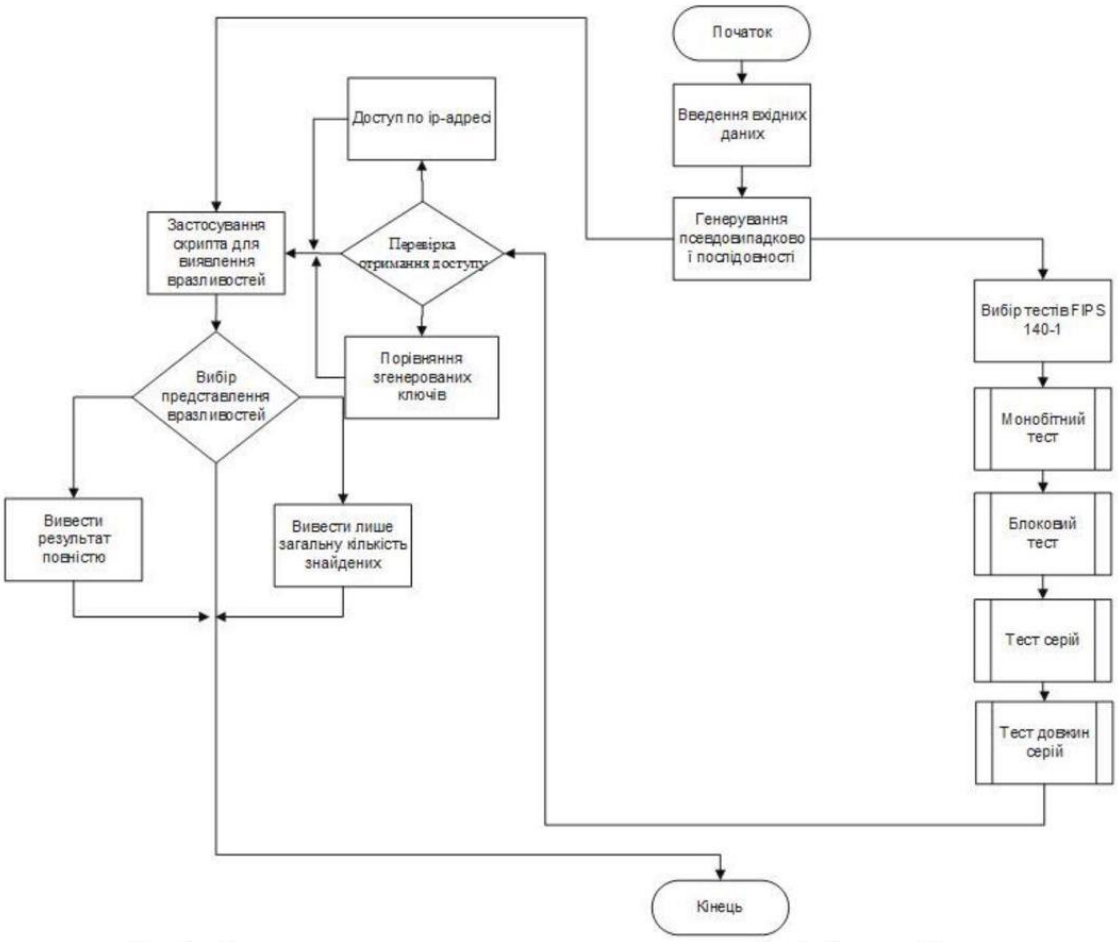

Рис. 1.9. Блок-схема першого виявлення вразливостей в інформаційно-телекомунікаційних системах

В цьому випадку це покриє один з недоліків брандмауера, а саме, таким чином можна буде приховати локальну мережу від інтернету.1 усі дані, що надсилаються до та з локальної мережі, будуть приховані, і якщо під час передачі будуть виявлені певні вразливості, вони будуть швидко ідентифіковані та оброблені. На малюнку 2 показана схема використання потокового шифрування в інформаційно-комунікаційній мережі. Вся інформація, що надходить з локальної мережі і пройшла перевірку правил в брандмауері, зашифровується у вигляді двійкового коду. Також за допомогою тесту FIPS140-1 перевіряється доступ до проміжного обладнання, перевіряються уразливості при спробі доступу в Інтернет і, відповідно, ті ж перевірки проводяться при отриманні даних безпосередньо в ДЕКУ. Тобто не всі

дані, які залишають локальну мережу по каналу зв'язку і надходять в локальну мережу з інших джерел, Інтернету, уразливі.

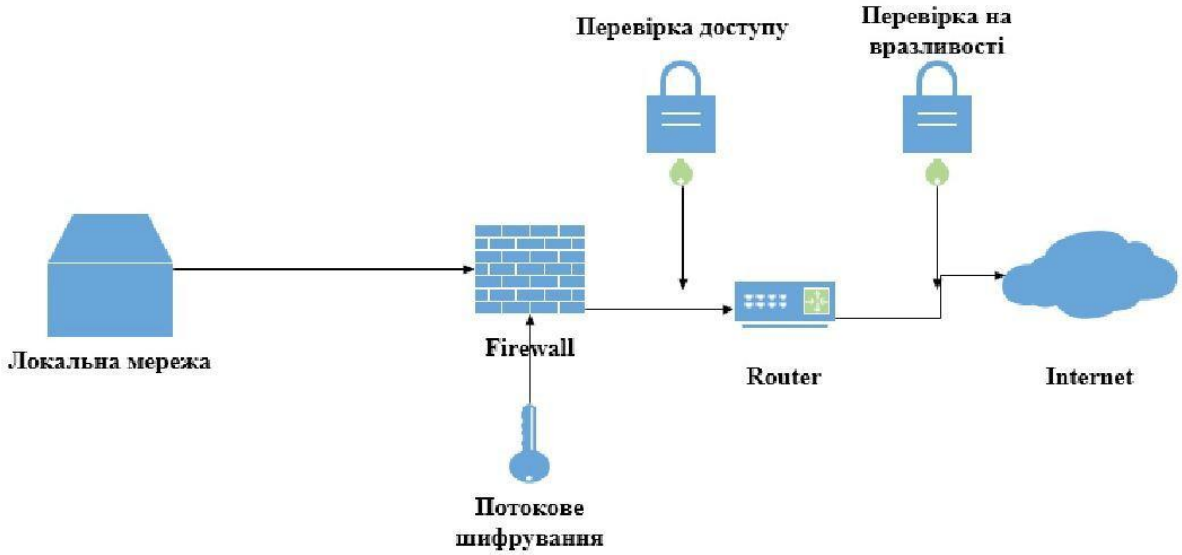

Рис. 2. Застосування потокового шифрування в ІТМ

В якості другого методу виявлення вразливостей в інформаційно-комунікаційних мережах було обрано використання системи передачі виявлення мережевих вторгнень, а саме Suricata (рис. 2.1)

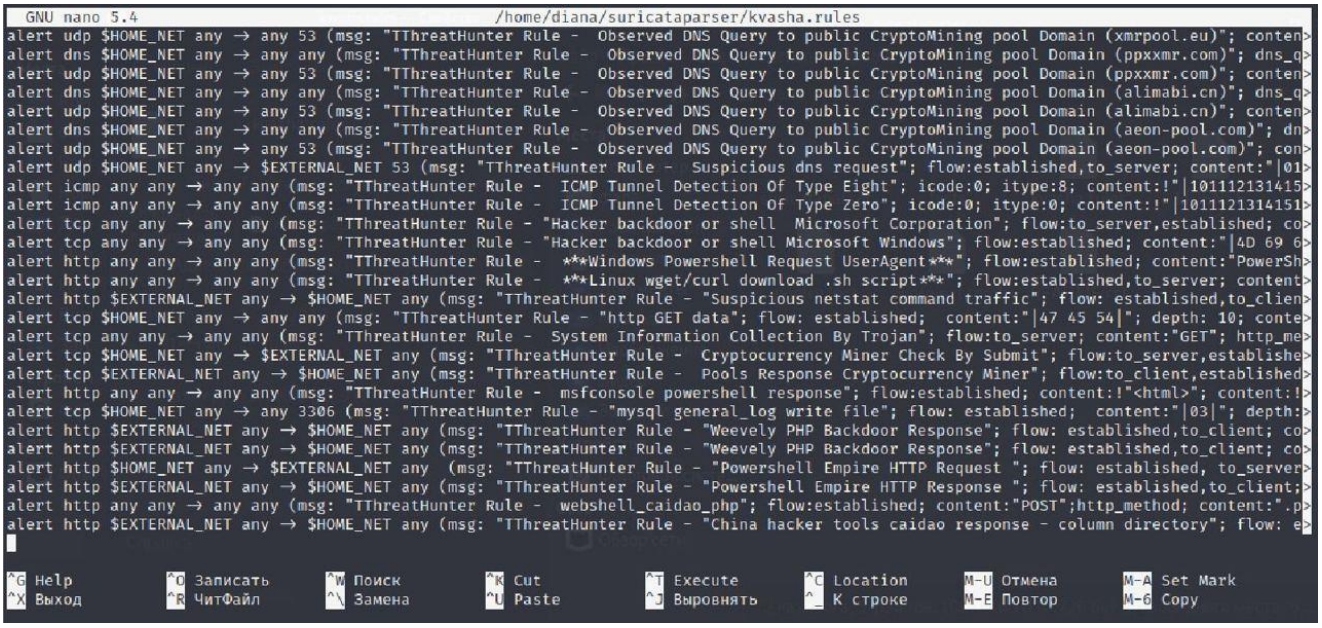

Рис. 2.1. Вивід створених правил на виявлення вразливостей

Suricata-це безкоштовний механізм виявлення мережевих загроз з відкритим вихідним кодом, який забезпечує виявлення вторгнень, запобігання вторгнень і моніторинг мережевої безпеки. Проект Suricata орієнтований на громаду, орієнтований на безпеку, зручність та ефективність, належить та підтримується Фондом відкритої інформаційної безпеки (OISF). Suricata відрізняється від інших подібних механізмів виявлення мережевих загроз, таких як Snort1, тим, що забезпечує оптимальну продуктивність багатопоточності [16]. Крім того, мова правил Suricata полегшує узгодження протоколів прикладного рівня жовтня без необхідності глибшого розуміння структур пакетів та протоколів.Підписи та правила є важливим аспектом Suricata, оскільки саме їх Ids використовує для виявлення підозрілої активності в мережі. Адміністратори можуть використовувати існуючі набори правил, такі як ті, що надаються oisf, але можуть створювати власні підписи або змінювати існуючі підписи [17].Таким чином, після розслідування можна сказати, що встановлення та дотримання правил за допомогою Suricata сприяє швидкому та ефективному отриманню інформації, включаючи якомога детальнішу інформацію про зловмисника та про те, що відбувається в мережі зв'язку.На основі цих тестів, Відстежувалися результати роботи такої кількості вразливостей, виявлених в інформаційних і комунікаційних мережах, а також швидкість і кількість виявлених вразливостей протягом відповідного періоду часу для впровадження розроблених методів і після їх впровадження. Звідси ми можемо побачити може бути.4, застосовуючи розроблений метод, ми маємо найкращі докази як швидкості, так і кількості виявлених вразливостей

Рис. 2.2. Залежність швидкодії від кількості виявлених загроз в ІТМ довпровадження методів виявлення вразливостей

З графіка це можна спостерігати до застосування методу (рис. 1.9.).дек. дек. (як показано на малюнку 2.1), час пошуку вразливостей значно збільшився, а загальна кількість вразливостей, виявлених за відповідний період, зменшилася, але час пошуку повинен був збільшитися, оскільки вони збільшилися.На графіку з'являється "зменшення", що вказує на те, що ці методи виявлення вразливостей потрібно вдосконалити, щоб час був постійним, і ви витрачали менше часу на Пошук вразливостей.Тому, коли ми застосували власний метод на практиці, результати моніторингу показали, що ситуація дещо покращилася (рис. 2.3.)). Звичайно, є деякі "провали", але вони не такі значні, як до впровадження методу. При цьому можна трохи скоротити час пошуку вразливостей, але при цьому збільшити кількість виявлених вразливостей за допомогою правильно розроблених дек-рішень, які є основою кожного із запропонованих методів.Це дуже ефективно, коли ми говоримо про великі організації.Грунтуючись на результатах, показаних на графіку (рис.4, рис.5) складено загальний графік залежності швидкості і кількості виявлених загроз в інформаційно-телекомунікаційних мережах до і після

впровадження методу (рис. 1).6) Він показав загальний час, витрачений на виявлення вразливостей, і загальна кількість вразливостей, виявлених за цей час

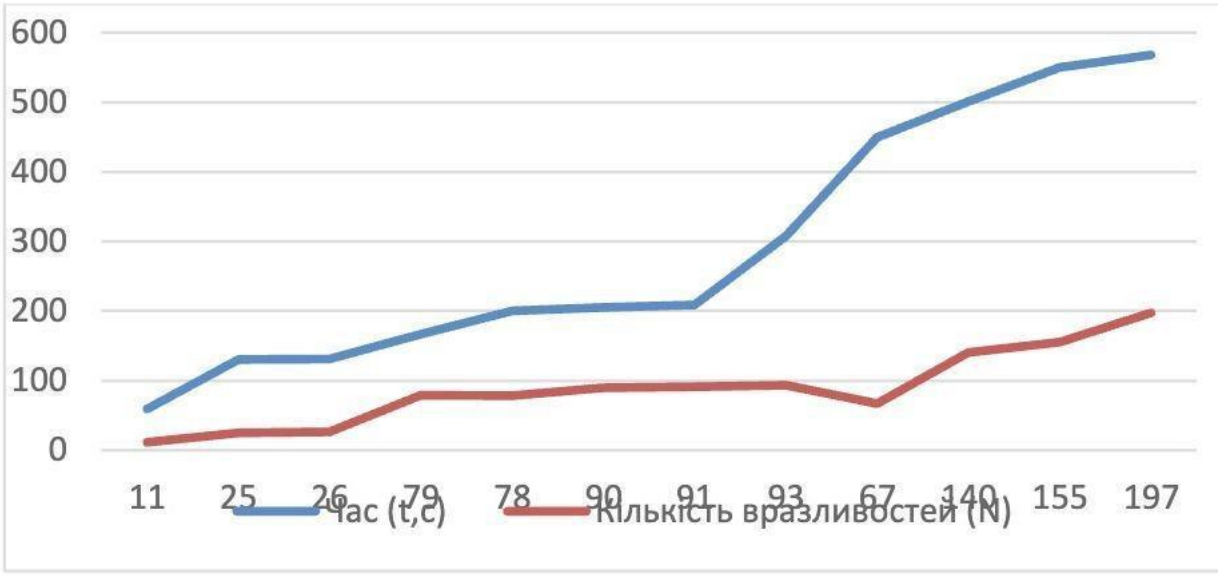

Рис. 2.3. Залежність швидкодії від кількості виявлених загроз в ІТМ післявпровадження методів виявлення вразливостейРис

Рис. 2.4. Діаграма швидкодії та кількості виявлених загроз до та післявпровадження методів виявлення вразливостей

Як бачите, на цій діаграмі чітко показано, що швидкість до використання методу становила 4244 секунди (1 година). 18 хвилин), і було виявлено 685 вразливостей мережі. Після впровадження розробленого методу було витрачено 3478 секунд (58 хвилин) і виявлено 1054 загрози. Таким чином, продуктивність після впровадження методів знижується на 766 секунд (13 хвилин), кількість виявлених вразливостей збільшується на 369, і ці методи можуть використовуватися в інформаційних і комунікаційних мережах.

ВИСНОВКИ ДО РОЗДІЛУ 3

Дана робота вказує на важливість впровадження програмного забезпечення для виявлення вразливостей, використання шифрування в брандмауері та правильне налаштування правил Suricata. Ці заходи спрямовані на забезпечення ефективного захисту мережі від потенційних атак та небезпек.

Врахування фізичної безпеки також наголошується як важливий компонент загальної стратегії кібербезпеки. Забезпечення надійного захисту для різних користувачів, включаючи як великі компанії, так і звичайних домашніх користувачів, вважається ключовим завданням.

Загальний висновок полягає в тому, що у вас є сучасні та ефективні засоби для забезпечення безпеки вашої телекомунікаційної мережі. Використання цих методів може сприяти створенню стійких та безпечних мереж в умовах сучасного цифрового середовища.

Виокремлені методи і підходи до забезпечення кібербезпеки в телекомунікаційних мережах. Реалізація програмного забезпечення для виявлення вразливостей, використання шифрування в брандмауері та налаштування правил Suricata є сучасними та ефективними стратегіями для захисту мережі від потенційних загроз.

Зазначена важливість фізичної безпеки вказує на те, що для повноцінного захисту мережі необхідно приділяти увагу не лише програмним аспектам, але й фізичним аспектам інфраструктури та обладнання. Інтеграція цих підходів в

комплексну стратегію допомагає забезпечити високий рівень безпеки в умовах сучасного інтернет-середовища

Реалізація програмного забезпечення для виявлення вразливостей, використання шифрування в брандмауері та налаштування правил Suricata є ефективними методами захисту мережі від потенційних атак і небезпек.

При цьому важливим аспектом є також врахування фізичної безпеки. Фізична безпека є ключовим компонентом комплексного підходу до кібербезпеки, оскільки вона враховує заходи для захисту фізичних ресурсів, інфраструктури та обладнання від незаконного доступу, крадіжок та інших фізичних загроз.

Інтеграція цих методів та підходів дозволяє створити комплексну систему захисту, що сприяє підвищенню рівня безпеки телекомунікаційних мереж.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ

При роботі з елементами телекомунікаційних мереж, у тому числі з центрами обслуговування клієнтів, для яких у даній статті розроблено алгоритм управління трафіком, необхідно звертати увагу на умови та засоби охорони праці, а також на їх належне дотримання всіх норм, встановлених чинним законодавством України.

4.1. Вивчення методів підтримки та аналіз умов праці інженерів для оцінки якості обслуговування.

4.1.1 Організація робочого місця інженера для вивчення методів підтримки та оцінки якості обслуговування.

Інженери активно займаються розробкою та моделюванням нових алгоритмів для підвищення якості обслуговування в мережах мобільного зв'язку. Ця робота включає в себе використання спеціалізованого програмного забезпечення та враховує вимоги до ефективності та надійності у сфері мобільних комунікацій.

Зокрема, інженери зосереджуються на розробці нових алгоритмів, які спрямовані на покращення якості обслуговування в мобільних мережах. Це може включати в себе оптимізацію ресурсів, підвищення швидкодії передачі даних та забезпечення стабільності мережі.

Зорове напруження, яке характеризується як робота з помірним ступенем нервового напруження, виконується у вільному темпі. Це може свідчити про те, що інженери працюють в умовах, коли їм дозволяється присвячувати достатньо часу на ретельний аналіз та вдосконалення алгоритмів без підвищеного тиску часових обмежень.

Такий підхід дозволяє забезпечити якісне розвиток алгоритмів для мобільних мереж, зберігаючи важливий баланс між ефективністю та стабільністю.

Робоче місце інженера, Залізобетон 3. поверх 9. На його поверсі знаходиться лабораторія телекомунікаційної компанії. Довжина приміщення - 7 м, ширина - 4,5

м, висота - 3,2 м.Загальна площа приміщення = 31,5 м2, Загальна площа = 100,8 м3. У лабораторії є 4 робочі станції, кожна з яких оснащена комп'ютером, VDT і телефоном. Крім того, в кімнаті є МФУ (принтер, сканер, копіювальний апарат), яким користується весь персонал лабораторії. Є система вентиляції.

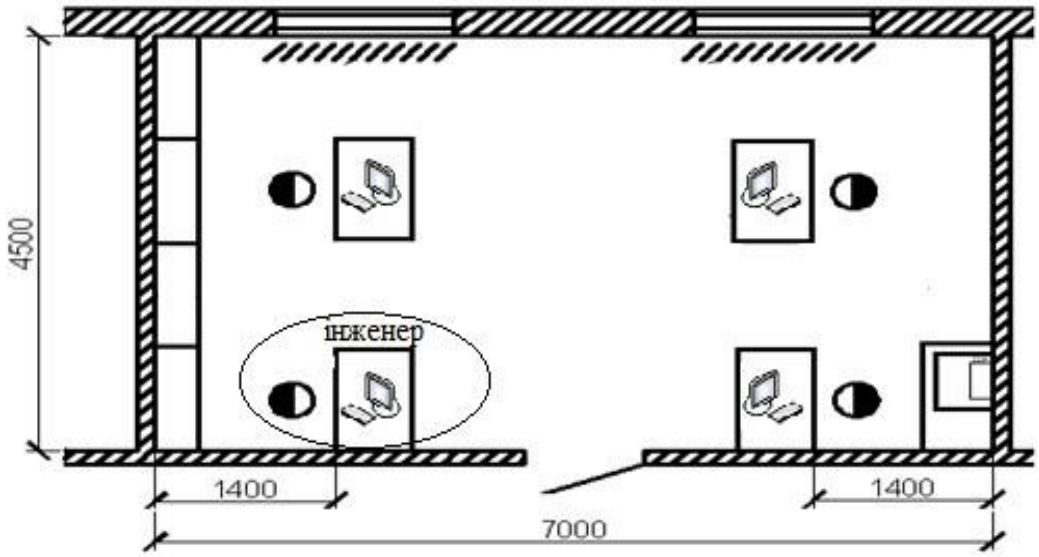

Рис. 2.5. Схема лабораторного приміщення, де працює інженер

Робоча площа на одного інженера складає:

$$S_{\text{роб.}} = \frac{S_{\text{заг.}}}{N} = \frac{31{,}5}{4} \approx 7{,}9 \text{ м}^2,$$

а робочий об’єм:

$$V_{\text{роб.}} = \frac{V_{\text{заг.}}}{N} = \frac{100{,}8}{4} = 25{,}2 \text{ м}^3,$$

де N – кількість робітників у відділку,

$S_{\text{роб.}}$, $V_{\text{роб.}}$ – площа та об’єм у приміщенні на одного працівника,

$S_{\text{заг.}}$, $V_{\text{заг.}}$ – загальні площа та об’єм приміщення

На підставі вказаних критеріїв згідно з НПАОП 0.00-1.31-98, робоче місце кожного працівника повинно відповідати наступним параметрам:

1. Мінімальна площа: Згідно зі стандартом, мінімальна площа кожного робочого місця повинна становити 6 м². Це означає, що для кожного працівника має бути виділено простір не менше 6 квадратних метрів.

2. Мінімальний обсяг: Стандарт визначає, що мінімальний обсяг приміщення для кожного робочого місця повинен бути не менше 20 м³. Це означає, що не лише площа, але і об'єм простору, в якому працює працівник, має відповідати вказаним вимогам.

Якщо робоче місце відповідає цим вимогам, то воно відповідає критеріям NPAOP 0.00-4.15-98. Переконайтеся, що розрахунки площі та об'єму відповідають встановленим стандартам, і вам буде забезпечено відповідне робоче середовище для працівників.

4.1.2. Список шкідливих і небезпечних факторів виробництва

Під час своєї роботи інженери можуть піддаватися впливу таких небезпечних і шкідливих виробничих факторів:

1) відсутність природного світла;

2) перевищення рівня шуму на робочому місці

3) Підвищення рівня електромагнітного випромінювання;

4) підвищення рівня статичної електрики;

5) підвищення або зниження температури повітря в робочій зоні.

4.2. Аналіз шкідливих та небезпечних виробничих чинників, що діють на робочому місці інженера з дослідження методів підтримки та оцінки якості обслуговування

Аналіз шкідливих та небезпечних виробничих чинників на робочому місці інженера з дослідження методів підтримки та оцінки якості обслуговування включає в себе оцінку ризиків, визначення можливих шляхів підвищення якості обслуговування та забезпечення безпеки працівника. Ось деякі аспекти, які можна розглядати в аналізі:

1. Шкідливі хімічні речовини: Інженер може мати стосунок до різних хімічних речовин у процесі досліджень. Аналіз потенційних небезпек може включати в

себе ідентифікацію хімічних речовин, їх властивостей та впливу на здоров'я працівника.

2. Фізичні фактори: До фізичних факторів можуть входити підвищена робоча температура, шум, вібрації тощо. Важливо визначити, чи вони перевищують норми безпеки та як вони можуть впливати на здоров'я та продуктивність працівника.
3. Ергономіка робочого місця: Оцінка, чи робоче місце відповідає ергономічним вимогам, може включати в себе аналіз розташування обладнання, меблів та інших елементів.
4. Психосоціальні фактори: Сюди можна віднести вплив стресу, робочого темпу, взаємодії з колегами тощо. Оцінка психосоціальних аспектів може допомогти забезпечити комфортні умови праці.
5. Оцінка методів підтримки та якості обслуговування: Проведення аналізу ефективності інструментів та систем підтримки для інженера, а також оцінка якості обслуговування, допоможе виявити можливість поліпшення робочого процесу.

Після проведення аналізу можна розробити план заходів з покращення умов праці, зменшення ризиків та забезпечення безпеки та ефективності праці інженера.

4.2.1. Відсутність або нестача природного освітлення

Нормалізований параметр природного освітлення (КПО) визначається за допомогою коефіцієнта природного освітлення та вказує, як ефективно приміщення отримує світло від природного джерела. Ви вказали, що КПО дорівнює 1,5%, що може свідчити про те, що лише невелика частина природного світла потрапляє в приміщення.

Вікна на робочому місці інженера важливі для забезпечення природного освітлення. Вказано, що вікна є на робочій поверхні і нормалізовано в 2,5 рази, що може означати збільшення площі вікон.

Фактор природного освітлення за даними DBN V вказує на середню точність роботи інженера. Використання бічного освітлення може впливати на сприйняття освітлення в робочому приміщенні.

Фактичне значення КПО становить 1,2%, що може свідчити про те, що забезпечення достатнього природного світла може бути важливим аспектом для комфортної і продуктивної роботи.

4.2.2. Розрахунок природного освітлення робочого приміщення інженера

Обчислимо дійсне значення коефіцієнта

Вивчіть природне освітлення (КПО) в офісній зоні, де працюють інженери, і порівняйте його зі стандартом.

Кімнати з розмірами π = 7 м, π = 4,5 м, π = 3,2 м2 кімнати

Металопластикові вікна з подвійним склінням 1,4 х 1,5 м визначають загальну площу вікна: вік. = 2 × 1,4 × 1,5 = 4,2 м2. Площа підлоги не більше 1/2. = 31,5 м2.

Це норма нормалізованого значення КПО (КПО) для аналітичних лабораторій і проектних приміщень. = 1.5%.

Умовна робоча поверхня знаходиться на висоті 0,8 м від підлоги, висота віконної рами-1 м, а висота вікна-1,5 м, отже, висота від висоти робочої поверхні до верхнього краю вікна 1 + 1,5 − 0,8 = 1.7 розрахункова точка а умовної робочої поверхні знаходиться на відстані 0,5 м від найдальшої від вікна стіни, тобто відстань від точки А до зовнішньої стіни приміщення дорівнює: $b = B - 2 = 4,5 - 0,5 = 4$ м.

Світлові характеристики вікон: λ = 15.

Відносини визначаються:.

Визначимо площу стіни стіни, стелі, перекриття, підлоги, підлоги і відповідний коефіцієнт відображення. Бічні стіни мають площу 2 × 4,5 м × 3,2 м = 28,8 м2, протилежна стіна вікна, включаючи двері: 7 м × 3,2 м = 22,4 м2, за якою слідує Загальна площа стіни: товщина стіни = 28,8 + 22,4 = 51,2 м2.

Кам'яна меморіальна стеля = основа = 31,5 м2.

Для побілених стель висота стелі = 0,7; для стін, пофарбованих світлою лакованою фарбою, товщина стін = 0,6; для підлог товщина підлоги = 0,25. Середній коефіцієнт відбиття сірого стелі, стін і підлоги:

Вибирається значення фактора ≤1.

Коефіцієнт світлопропускання склопакета, виготовленого з листового віконного скла: ≤1 = 0,8; коефіцієнт 2 = 0,85 для подвійної металевої відкидної рами; регульовані внутрішні жалюзі 3 = 3 = 1 потім можна відрегулювати загальний коефіцієнт світлопропускання вікна.:

підсумки заг... = $\tau 1 \times \tau 2 \times \tau 3 = 0,8 \times 0,85 \times 1 = 0,68$

Коефіцієнти Kbud.Враховуючи затінення вікон через будівлю з іншого боку, це пов'язано з Kbud. = 1.1.

Розрахуйте площу вікна, необхідну для забезпечення бічного природного освітлення, з урахуванням реальних умов і особливостей приміщення:

Розрахуйте фактичний коефіцієнт природного освітлення з урахуванням реальних умов і характеристик приміщення

Фактичне значення КПО менше нормованого значення, що говорить про недостатнє природному освітленні в цьому приміщенні, тому додатково слід використовувати штучне освітлення. жовтень.

4.2.3. Підвищення рівня шуму на робочому місці

У номері є 4 робочих місця, в кожному з яких є комп'ютер з жорстким диском в системному блоці, 3 вентилятора в системі охолодження ПК і телефон. Крім того, поблизу працюють периферійні пристрої. Таким чином, в приміщенні присутній шум механічного та аеродинамічного Походження, широкосмуговий з апериодическим посиленням під час роботи принтера. Приблизний еквівалентний рівень звукового тиску робочого джерела шуму інженера на робочому місці:

1) Принтер-55 дБ;

2) Сканер-50 дБА;

3) Вентилятор-45 дБА; 4) жорсткий диск -45 дБА; 5) Телефон–70 дБА.

Відповідно до hs3.3.6.037-99[40], еквівалентний допустимий рівень шуму інженера на робочому місці становить 50 дБА.

Давайте розрахуємо середній рівень шуму на робочому місці під час роботи всього зазначеного обладнання. Рівні шуму від декількох неузгоджених джерел, що працюють одночасно, розраховуються за принципом підсумовування енергії рівнів інтенсивності окремих джерел:

(4.1)

де θ, 2. це рівень звукового тиску джерела шуму;

√ - Кількість джерел шуму.

Коли значення рівня звукового тиску для кожного типу обладнання підставляється в рівняння (4.1) , воно виглядає наступним чином:

$$\triangle = 10(105{,}5 + 105 + 104{,}5 + 104{,}5 + 107) = 70{,}2 \text{ бД}$$

Якщо на одному рівні є більше одного джерела шуму

Інтенсивність загального рівня шуму визначається за формулою = = ++10LG LG.

В даному випадку таких джерел 5, тому існує загальний рівень шуму:

$$\sqrt{} = 70{,}2 + 10\lg 4 = 76{,}2 \text{ дБ}$$

Отримані результати перевищують допустимий рівень, тому необхідно вжити особливих заходів для зниження рівня шуму в приміщенні

4.2.4. Захист від виробничого шуму та вібрацій

Однією з альтернатив для зниження шуму є ізоляція обладнання з високим рівнем шуму, такого як багатофункціональні пристрої (МФУ). Розміщення їх в окремому приміщенні або утеплення внутрішніх стін спеціальними звукопоглинальними матеріалами може ефективно знизити рівень звукового впливу.

Так, ізоляція обладнання з високим рівнем шуму, наприклад, багатофункціональних пристроїв (МФУ), може бути ефективним способом зниження рівня шуму в приміщенні. Розміщення такого обладнання в окремому приміщенні або утеплення внутрішніх стін з використанням спеціальних звукопоглинальних матеріалів може значно зменшити звуковий вплив на робоче

середовище. Це сприяє створенню сприятливих умов для праці та комфортного відпочинку.

Загальний підхід до управління шумом повинен включати різноманітні методи, такі як акустичне облицювання, правильне розташування обладнання, використання звукопоглинальних та ізоляційних матеріалів. Це допомагає створити тихе та комфортне робоче середовище для працівників.

Так, врахування звукопоглинальних властивостей корпусу обладнання є важливим кроком при плануванні ізоляції від шуму. Важливо, щоб корпус не тільки зменшував шум, але й не перешкоджав обслуговуванню обладнання і відповідав естетичним вимогам приміщення.

Вибір матеріалів для ізоляції та конструкції корпусу повинен бути здійснений з урахуванням конкретних умов приміщення, його розміру, форми і розташування джерел шуму. Також слід враховувати можливість регулювання ізоляційних властивостей, наприклад, за допомогою додаткових звукопоглинальних матеріалів чи систем акустичного контролю.

Загальний підхід до ізоляції включає різні аспекти, і обрані рішення повинні бути оптимальними для забезпечення ефективного зниження рівня шуму в робочому середовищі.

4.2.5. Захист від електромагнітних полів і випромінювань

Інженери, які вивчають методи підтримки і оцінюють якість обслуговування, щодня працюють на ПК зі спеціальним програмним забезпеченням, оточених 3 ПК, які створюють електромагнітне поле і випромінюють електромагнітне випромінювання. Підвищений рівень ЕМВ шкідливий для здоров'я людини. В основному уражаються нервова і серцево-судинна системи, виникають головні болі і стомлюваність, знижується точність виконання робочих вправ, порушується сон. Електромагнітне випромінювання викликає зміни артеріального тиску, гіпотонію або гіпертонію.

Для захисту працівників лабораторії виділяють наступні методи:

1) використання обладнання, його emv буде мінімальним;

2) Кількість обладнання, що постачає комп'ютер, потрібно як мінімум;

3) огляд робочого місця;

4) якщо можливо, виконайте дистанційне керування випромінюючим комп'ютером

4.3. Пожежна безпека

Вимоги до протипожежних, протипожежних та вибухозахищених систем є важливою складовою безпеки будівель та приміщень. Основні вимоги можна сформулювати наступним чином:

1. Відповідність законодавству: Системи повинні відповідати вимогам місцевого протипожежного законодавства та нормативних документів, таких як НАПБ.
2. Захист від електропожеж: Системи повинні максимально захищати від електропожеж, що можуть виникнути через несправність електрообладнання, коротке замикання чи інші причини.
3. Детектори пожежі: Наявність автоматичних детекторів пожежі для вчасного виявлення можливих загорянь та сповіщення про них.
4. Евакуаційні шляхи та засоби евакуації: Забезпечення безпечних і чітко позначених шляхів евакуації та наявності необхідних засобів евакуації.
5. Пожежогасіння: Встановлення систем гасіння пожежі, таких як протипожежні водяні системи або автоматичні пожежогасники, для швидкого і ефективного виявлення та гасіння пожеж.
6. Ізоляція вибухонебезпечних зон: Використання спеціальних заходів для захисту від вибуху в умовах, де існує вибухонебезпека.
7. Навчання персоналу: Навчання працівників правилам пожежної безпеки та ефективного ведення евакуації в разі пожежі.

Всі ці вимоги спрямовані на максимальний захист людей, майна та навколишнього середовища в разі пожежі чи вибуху.

НАПБ В. згідно з 01.053-2000, приміщення, в якому працює інженер, відноситься до категорії D через ризик загоряння. У приміщенні, де знаходиться

обладнання, знаходяться негорючі рідини і матеріали в холодному стані, провідники електричного кабелю до обладнання, меблі.

Портативний порошковий вогнегасник ВП-5 є засобом пожежогасіння, який може використовуватися для гасіння пожеж різних класів. Основні характеристики вогнегасника і його використання визначаються його конструкцією та видами пожеж, які він може гасити:

1. Клас А: Вогнегасник призначений для гасіння пожежі матеріалів, таких як дерево, папір, тканини та інші тверді речовини.
2. Клас В: Використовується для гасіння пожежі, пов'язаної з рідкими горючими речовинами, такими як бензин, нафта тощо.
3. Клас С: Застосовується для гасіння пожежі газів, наприклад, при витоку газу.
4. Клас Е: Вогнегасник призначений для гасіння пожеж електроустаткування.

ВП-5 є порошковим вогнегасником, і порошок використовується як ефективний засіб гасіння пожежі. Важливо дотримуватися інструкцій щодо використання цього вогнегасника та враховувати його обмеження. Щодо виявлення пожежі, 1-точковий детектор диму може бути корисним, але, як ви зазначили, він реагує тільки на дим і може бути неефективним у випадках, коли пожежа супроводжується іншими видами викидів або не супроводжується димом, наприклад, при пожежі газу чи рідини.

Робоче місце інженера 3. Оскільки він знаходиться на підлозі, потрібно не менше 2 зливних отворів коли він не підходить для евакуації у разі пожежі

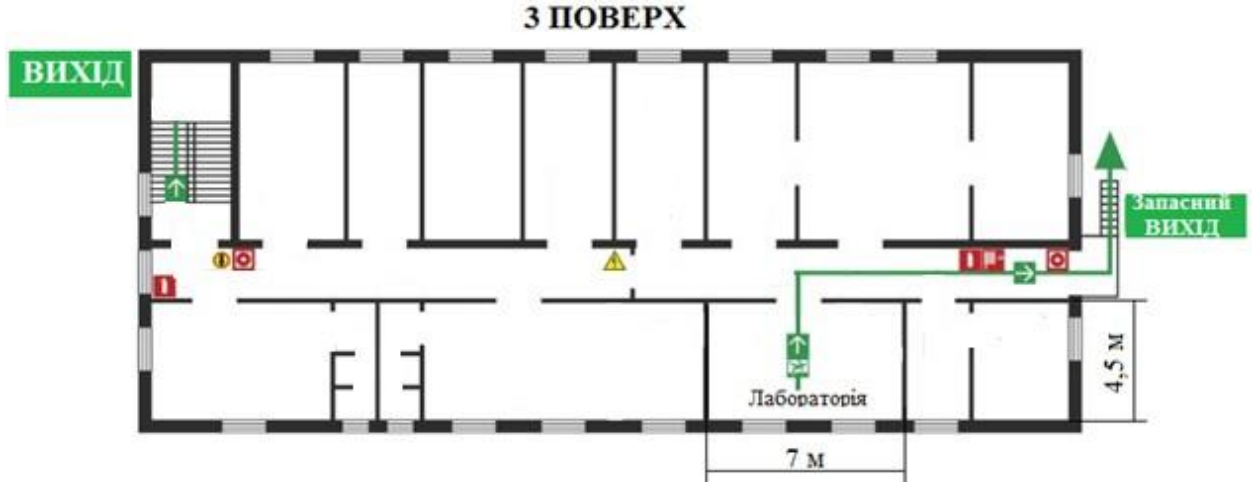

Рис. 2.6. План евакуації з лабораторного приміщення

4.4. Інструкція з охорони праці

Загальні положення

правильна інструкція та навчання з питань охорони праці, промислової гігієни, пожежної безпеки, надання першої допомоги та правил поведінки в надзвичайних ситуаціях є важливими аспектами для працевлаштованих осіб. Дотримання цих правил може значно покращити безпеку та забезпечити добробут працівників.

Основні елементи навчання та інструкції для працівників включають:

1. Охорона праці: Включає в себе інструкції щодо безпеки на робочому місці, користування захисним спорядженням, управління ризиками та використання безпечних методів праці.

2. Промислова гігієна: Охоплює питання збереження здоров'я на робочому місці, контроль шкідливих виробничих факторів, особистої гігієни та правильного використання обладнання.

3. Пожежна безпека: Включає навчання працівників ефективно користуватися засобами пожежогасіння, розуміти евакуаційні шляхи та діяти в надзвичайних ситуаціях.

4. Перша допомога: Проходження курсів першої допомоги для надання допомоги постраждалим в разі нещасних випадків чи невилучної хвороби.

5. Правила поведінки в надзвичайних ситуаціях: Вивчення та регулярна практика дій в разі виникнення надзвичайних ситуацій, таких як пожежі, землетруси, повені тощо.

Ці знання допомагають працівникам уникати та врегульовувати можливі загрози для їхнього здоров'я і безпеки на робочому місці

Після первинного інструктажу на робочому місці працівники повинні пройти стажування під керівництвом досвідчених та кваліфікованих працівників протягом 2-15 змін.

Право працівника відмовитися від виконання роботи в разі наявності небезпечної ситуації для його життя або здоров'я є важливим аспектом охорони

праці. Це право, яке може використовуватися в обставинах, коли виконання роботи може становити серйозну загрозу безпеці працівника.

Право працівника відмовитися від роботи в разі наявності небезпечної ситуації для його життя або здоров'я визнане багатьма законодавчими актами та нормативами у різних країнах. Проте це право має обмеження і повинно бути обгрунтованим і пов'язаним із реальною небезпекою.

Зазвичай працівник повинен:

1. Повідомити про небезпеку: Проінформувати негайно свого непосереднього керівника або відповідного представника про існуючу небезпеку.

2. Чекати на дозвіл: Перед призупиненням роботи працівник повинен отримати дозвіл від уповноваженого представника або відділу охорони праці.

3. Обговорення з керівництвом**:** Якщо після повідомлення про небезпеку ситуація не виправляється, працівник може звернутися до вищого керівництва або органів, відповідальних за охорону праці.

Це право визначено для забезпечення безпеки працівників та вказує на важливість співробітництва між роботодавцем і працівником у забезпеченні безпечних умов праці.

Це право сприяє підтримці безпеки та здоров'я працівників, а також підтримує принцип взаємодії між роботодавцем і працівником у забезпеченні безпечних умов праці.

Вимоги безпеки перед початком роботи:

1. Огляньте робоче місце. Розмістіть робоче місце, переконавшись, що на робочому місці немає сторонніх предметів або всіх пристроїв, і підключіть ПК до системного блоку за допомогою кабельного роз'єму відповідно до схеми підключення.

2. Контроль:

- Простота обслуговування роз'ємів шнура живлення і Блоку приладів;

- Відсутність обривів і пошкоджень ізоляції подає дроти;

- Відсутність відкритих живих доріжок на пристроях ПК;

3. Підготуйте робоче місце для роботи з таким пристроєм, як"екран".:

- Оптимально відрегулюйте сидіння робочого крісла (крісла) на зручну висоту; кут нахилу спинки деки крісла повинен варіюватися в межах 90-11 градусів. До площини листа;

- Розташуйте крісло і екран так, щоб кут огляду на екрані становив 15 градусів, а відстань до екрану - 400-800 мм.;

- Вживайте запобіжних заходів, щоб при нормальному освітленні на робочому місці світло не потрапляло безпосередньо на екран монітора.

4.Протріть клавіатуру (щоб знизити рівень статичної електрики), зовнішню поверхню екрану злегка вологою тканиною (зробленої з бязі або марлі).

Вимоги безпеки при експлуатації

1.Перш ніж підключати шнур живлення до розетки 220 В, переконайтеся, що всі мережеві комутатори на всіх пристроях ПК знаходяться в "заземленому" положенні (нуль).

2.Після підключення пристрою ПК до джерела живлення Відрегулюйте яскравість і фокусування зображення VDT за допомогою кнопки регулювання відповідно до характеристик вашого прицілу.

3. Не залишайте робоче місце, не попереджаючи свого начальника.

4.Do Не залишайте робочий комп'ютер і його пристрої без нагляду.

5. Підключайте і від'єднуйте кабельний роз'єм ПК-пристрої тільки при відключеному напрузі живлення.

6. Напруга живлення приладу і окремих блоків ПК, але тільки після ретельної перевірки надійності заземлюючого провідника, справності кабелів і роз'ємів електромережі.

7. Якщо ви вимкнете vdt (Відеотермінал), і при його включенні на екрані не відображається ніякої інформації (екран порожній) або в центрі екрану загоряється яскрава біла смуга, Відеотермінал буде вимкнений.、

8.Якщо на пристрої ПК виявлено запах гару, негайно вимкніть обладнання, вимкніть живлення 2. Необхідно не включати його один раз і звернутися до фахівця з обслуговування ПК.

9. Операторам ПК жовтень повинен бути наданий 10 додаткових регульованих перерв по 2 або 3 хвилини відповідно.Згідно dsan pin3.3. 2 007 1998 року, оператори комп'ютерів отримують декомунізацію на 15 хвилин кожні 2 години.

10. Кількість оброблених символів (або символів VDT) не повинна перевищувати 4 мільйонів за 3 години роботи.

11. Щоб нойропсихиатрически усунути або зменшити зорове і м'язове напруження, а також запобігти перевтомі, необхідно виконувати комплекс вправ після регулярних перерв, хвилин фізкультури і закінчення робочого дня.

Вимоги безпеки в кінці роботи

1. Встановіть усі тумблери (перемикачі) робочого пристрою та перемикачі (Перемикачі) електричної панелі в положення "виключити".

2. Від'єднайте вилку від електричної розетки.

3. Виключити вентиляцію.

4. Виконуйте вологе прибирання на робочому місці. Протріть екран VDT від пилу не менше 1 разу, щоб провести пальцем. Збір пилу з обладнання повинен проводитися при відключеному живленні.

5. Повідомляйте про всі несправності, виявлені під час роботи, і про заходи, вжиті для їх усунення, заносячи відповідні записи в робочий журнал.

6.Вимийте руки водою з милом.

ВИСНОВКИ ДО РОЗДІЛУ 4

Результати аналізу умов праці інженерів вказують на кілька важливих проблем, що вимагають уваги та можливих заходів для поліпшення.

1. Природне освітлення: Фактичний коефіцієнт природного освітлення (КПО) становить 1,2%, що менше від нормативного значення 1,5%. Це може впливати на ефективність та зручність виконання візуальних завдань. Рекомендується розглянути можливості додаткового освітлення або оптимізації розміщення робочих місць.

2. Рівень шуму: Загальний рівень шуму в приміщенні становить 76,2 дБА, що перевищує допустимий рівень в 50 дБА. Це може призводити до проблем з концентрацією та загрози здоров'ю працівників. Рекомендується вживати заходів щодо зменшення шумового впливу, таких як використання звукоізоляційних матеріалів чи застосування засобів індивідуального захисту.

3. Вібрація: Якщо вибрація є проблемою, то слід розглянути застосування антивібраційних технік та обладнання, яке може зменшити вплив вібрації на працівників.

4. Безпека та охорона праці: Доцільно переглянути та оновити заходи безпеки та охорони праці, забезпечити дотримання стандартів та нормативів.

Ці заходи допоможуть покращити умови праці інженерів, забезпечити їхню безпеку та збільшити продуктивність.

РОЗДІЛ 5 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

5.1. Аналіз впливу на довкілля при роботі аналізатора потоків Е1 цифрових систем електрозв'язку.

Аналізатор потоків Е1 включає кілька ключових компонентів, які можуть впливати на електромагнітну обстановку та навколишнє середовище на робочому місці. Декілька аспектів, які варто врахувати:

1. Генератор тестових сигналів: Залежно від характеристик генерованих сигналів, можуть виникати електромагнітні перешкоди. Додаткові заходи можуть бути прийняті для мінімізації впливу.

2. Процесор: Висока продуктивність процесора може викликати підвищення рівня тепловиділення та споживання електроенергії. Необхідно розглянути ефективність та тепловий режим.

3. Пристрої управління та відображення: Клавіатура, дисплей і інші пристрої можуть викликати комутаційний шум та впливати на якість електромагнітної обстановки.

4. Мережні фільтри та джерела безперебійного живлення: Вони можуть впливати на якість струму та враховувати вплив на електромагнітну сумісність.

5. Електроустаткування: Загалом, всі елементи, що живляться електроенергією, можуть впливати на електромагнітну обстановку.

Щоб зменшити негативний вплив, рекомендується використовувати екрановані кабелі, електромагнітні фільтри, дотримуватися електромагнітних стандартів і розташовувати обладнання так, щоб мінімізувати ефект взаємодії між компонентами.

Рис. 2.7. Зовнішній вигляд аналізатора потоків

Основними факторами негативного впливу приладу на навколишнє середовище є:

1. Перевірте генератор сигналів і електромагнітну корекцію процесора.
2. Ергономічні Налаштування дисплея:

а) зменшення контрастності зображення в умовах сильного зовнішнього освітлення;

б) дзеркальні відблиски з передньої поверхні екрану;

в) наявність мерехтливого зображення на екрані;

3. Характеристики випромінювання екрану:

а) контролюйте електромагнітне поле в грудні в діапазоні від 5 Гц до 1000 МГц;

б) статичне навантаження екрану;

c) ультрафіолетове випромінювання в грудні 200-400 нм;

d) інфрачервоне випромінювання в грудні 1050 нм - 1 мм

Давайте докладніше опишемо деякі з перерахованих вище факторів негативного впливу роботи з комп'ютером.

Коли екран рухається, на екрані накопичується статична електрика, створюючи електростатичне поле. У різних дослідженнях дека електростатичного поля при

різних умовах вимірювання коливається від 8 до 75 кВ/м, але в той же час люди, що працюють з монітором, отримують електростатичний потенціал. Значний внесок в загальне електростатичне поле вноситься за рахунок з'єднання клавіатури, поверхні, навантаженої тертям, і кабелю. Експерименти показали, що навіть після включення клавіатури електростатичне поле швидко збільшувалося з 2 до 12 кВ / м. На окремих робочих місцях в області рук була зареєстрована напруженість статичного електричного поля більше 20 кВ / м.

Звукове забруднення в приміщенні з вимірювальними приладами може бути викликане різними джерелами, які ви вказали. Низький рівень шуму є важливим аспектом комфортної та безпечної робочої обстановки. Ось кілька можливих заходів для зменшення рівня шуму в такому приміщенні:

1. Акустична обробка приміщення: Використання акустичних панелей або інших матеріалів, що поглинають звук, може допомогти знизити відбиття звуку та загальний рівень шуму.

2. Ізоляція пристроїв: Застосування ізоляційних матеріалів на пристроях, які виробляють шум (наприклад, вентилятори, трансформатори), може значно зменшити їхній вплив на оточуюче середовище.

3. Оптимізація робочих процесів: Розгляньте можливість розміщення обладнання так, щоб зменшити взаємодію між джерелами шуму.

4. Використання тихших обладнань: Придбання та використання обладнання з меншим рівнем шуму або застосування тихших аналогів може бути ефективним рішенням.

5. Регулювання вентиляційних систем: Вентиляційні системи можуть бути джерелом шуму. Оптимізуйте їх роботу та розгляньте можливість використання менш шумних вентиляторів.

6. Використання вакуумних систем: Якщо можливо, використовуйте вакуумні системи для кондиціонування повітря, оскільки вони можуть бути менш шумними, ніж традиційні системи кондиціювання повітря.

Важливо провести детальний аналіз джерел шуму та впровадити комплексний план заходів для забезпечення оптимального рівня звуку в

5.2. Вплив на здоров'я користувача електромагнітних полів приладу

Наукові дослідження в галузі впливу роботи з комп'ютером на здоров'я людини дійсно проводилися. Однак важливо враховувати, що більшість досліджень не надає однозначних доказів щодо серйозного негативного впливу роботи з комп'ютером на всі аспекти здоров'я. Наразі вважається, що вплив комп'ютерної роботи на здоров'я залежить від кількох факторів, таких як тривалість робочого дня за комп'ютером, організація робочого місця, паузи на відпочинок, правильне користування обладнанням та ін.

Основні аспекти, на які зазвичай звертають увагу в дослідженнях, включають:

1. Очі: Довготривалий перегляд екрану комп'ютера може спричинити такі проблеми, як напруга очей, сухість та подразнення.
2. М'язи та Спина: Довгий період сидіння за комп'ютером може викликати проблеми із м'язами спини та шиї.
3. Стрес: Робота за комп'ютером може бути пов'язана із стресом, особливо при тривалій роботі, тиском відстроченої відповіді (наприклад, чекання на відповідь на електронний лист) та ін.
4. Сон: Довгі години перед комп'ютером перед сном можуть впливати на якість сну.

Щоб зменшити можливий негативний вплив, рекомендується вживати такі заходи як регулярні перерви, вправи для очей та тіла, налагодження ергономіки робочого місця та інші превентивні заходи.

Будь ласка, звертайте увагу на оновлення та рекомендації організацій з охорони здоров'я для актуальної інформації та порад.

З фізичної точки зору тканини людини є парамагнітними матеріалами: це означає, що вони можуть відчувати магнітне поле і можуть відчувати магнітне поле. Медичні дослідження показали, що вплив на такі ділянки викликає зміни метаболізму на клітинному рівні. Змінні електромагнітні поля викликають іонні коливання в організмі людини, що дає певний результат.

За загальними даними, дисфункція ЦНС виникає в середньому у людей, які працюють біля монітора по 1-2-6 годин на добу, в порівнянні з контрольною групою - в 4,6 рази частіше, захворювання серцево-судинної системи - в 2 рази частіше, захворювання верхніх дихальних шляхів - в 1,9 рази частіше, захворювання ЦНС. опорно - руховий апарат-в 3,1 рази частіше листопада. При більш тривалому часу роботи за комп'ютером співвідношення здорових і хворих користувачів значно збільшується.

За даними Бюро статистики декомунізації США, кількість випадків користувачів зросла у 8 разів між 1982 і 1990 роками. Крім того, було виявлено, що часте вплив електромагнітного випромінювання монітора призводить до аномальних результатів вагітності.

Дослідження функціонального стану користувачів комп'ютерів, проведене Центром електромагнітної безпеки в 1996 році, показало, що значні зміни гормонального статусу і специфічні зміни біологічних струмів головного мозку відбуваються в організмі користувача під впливом електромагнітного випромінювання монітора. навіть для короткострокових операцій (45 хвилин).

біологічні реакції людини на електромагнітне випромінювання можуть залежати від різних факторів, включаючи:

1. Інтенсивність і частота випромінювання: Високі рівні інтенсивності та високі частоти можуть викликати різні ефекти порівняно з низькими рівнями та низькими частотами.

2. Час опромінення: Тривалість впливу також може бути фактором. Тривале опромінення може мати інші наслідки, ніж короткочасне.

3. Модуляція сигналу: Зміна характеристик сигналу, така як амплітудна або частотна модуляція, також може впливати на його взаємодію з біологічними системами.

4. Частотний спектр і частота **впливу:** Різні частоти можуть взаємодіяти з різними аспектами тканин та органів людського тіла.

Важливо зауважити, що багато досліджень проводяться для вивчення безпеки електромагнітного випромінювання в реальних умовах використання електронних

пристроїв. Наразі немає загальновизнаного наукового підтвердження серйозних шкідливих ефектів від низькочастотного випромінювання, якого використовується в електроніці повсякденного використання.

5.3. Захист користувача від негативних впливів електромагнітного поля

Дисплеї приладів створюють сильне електростатичне поле не зовсім безпечне для людського організму. Правда, на відстані 50-60 см від екрана його вплив значно зменшується. Застосування ж спеціальних фільтрів, що прикривають екран, узагалі дозволяє звести його до нуля. Варто звернути увагу ще і на те, що при роботі монітора електризується не тільки його екран, але і повітря в приміщенні. Причому він здобуває позитивний заряд. Позитивно наелектризована молекула кисню не сприймається організмом як кисень, що викликає в користувача кисневе голодування.

Як технічні стандарти безпеки моніторів широко відомі шведські TCO-92, 95, 99 і MPR-II. Вони обмежують параметри випромінювання монітора, споживання електроенергії, візуальні параметри і т.д. Деякі основні параметри, визначені стандартом MPR-приведені в таблиці 1.

По-перше, дослідження показали, що встановлення фільтрів на екран може зменшити електричну складову електромагнітного поля в безпосередній близькості від екрану.Через перерозподіл площі це може призвести до збільшення електронно-променевої трубки вздовж її осі на відстані 1,0-1,5 м і більше від екрану.

По-друге, рівень електромагнітних полів багато в чому залежить від типу і якості електропроводки. Наприклад, у багатьох кімнатах, де знаходиться пристрій, немає загального заземлення, що означає, що штекер ПК повинен бути заземлений на 3. його контакт "підвішений" в повітрі, а також рівень електромагнітного поля, електроприлади, люмінесцентні лампи, Джгути проводів і т.д. він з'явиться. він часто випромінює низькочастотні електричні поля, які бентежать робоче місце.

Таблиця 1.

Вимоги до електромагнітного поля дисплея

Найменування параметра	MPRII
Напруженість електромагнітного поля у 50см навколо дисплея по електричній складовій, В/м, не більше в діапазоні частот: • 5Гц – 2кГц 2кГц – 400кГц	 25 2.5
Щільність магнітного потоку у 50 см навколо дисплея, нТл, не більше в діапазоні частот: • Гц – 2кГц 2кГц – 400кГц	 250 25
Поверхневий електростатичний потенціал, В, не більше	500

5.4. Рекомендації щодо роботи з приладом

* Неприйнятна відстань монітора від користувача становить 0,3 м, критична відстань - 0,5 м, а оптимальна відстань - більше 1 метра.

* Не залишайте пристрій увімкненим протягом тривалого часу, якщо він не використовується. Також рекомендується використовувати "сплячий режим"для відображення.

* Через високий рівень електромагнітного випромінювання від тестового генератора сигналів для роботи необхідно використовувати екранований кабель.

** Оскільки на дисплеї також присутній електромагнітне випромінювання, пристрій повинен бути розміщений так, щоб воно не поширювалося на сусіднє робоче місце.

* По можливості варто скоротити час роботи на пристрої і якомога частіше переривати роботу.

* Пристрій повинен бути заземлений. Якщо є захисний екран, він також повинен бути заземлений.Для цієї мети спеціально передбачена дріт з металевими засувками на кінці.

ВИСНОВКИ ДО РОЗДІЛУ 5

Справжня ступінь небезпеки від електромагнітного випромінювання телекомунікаційних вимірювальних приладів визначається великою кількістю факторів, включаючи інтенсивність випромінювання, частоту, відстань від джерела, тривалість впливу та інші параметри.

Більшість досліджень та стандартів у галузі безпеки електромагнітного випромінювання приходять до висновку, що при відповідності стандартам та правилам безпеки сучасні технології та телекомунікаційні пристрої, такі як мобільні телефони, не представляють значущої небезпеки для здоров'я при звичайному користуванні.

Організації, такі як Всесвітня організація охорони здоров'я (ВООЗ) та інші, встановлюють міжнародні стандарти та рекомендації щодо допустимого рівня електромагнітного випромінювання. Пристрої повинні відповідати цим стандартам для того, щоб бути визнаними безпечними для використання.

Якщо у вас є конкретні питання або концерни стосовно конкретних пристроїв чи ситуацій, рекомендую звертатися до офіційних джерел інформації, таких як організації з охорони здоров'я та експерти з безпеки, для отримання точної інформації та порад

В Україні Безпека рівнів іонізуючого випромінювання комп'ютерних моніторів регулюється стандартами nrbu-97. Стандарт обмежує потужність дози рентгенівського випромінювання на відстані 5 см від поверхні екрану монітора до 100 мікрон на годину і встановлює граничну величину річної еквівалентної дози опромінення кришталика ока, рівну 15 мЗв. Але на практиці це значення становить менше 0,7 мЗв і приблизно дорівнює. Цей результат вказує на радіаційну безпеку

дисплея, оскільки річна еквівалентна доза, що накопичується кришталиком ока, в 97 разів перевищує значення, Допустиме критеріями NRBU-20.

Надзвичайно важливо враховувати можливість впливу електромагнітного поля пристроїв на здоров'я користувачів, і заходи для забезпечення їхньої безпеки є важливою частиною процесу розробки та використання таких технологій. Ваш підхід до охарактеризування аналізатора потоку E1 як джерела забруднення та опису впливу електромагнітного поля є розумним.

Щоб ефективно захистити користувачів від негативного впливу, можна розглядати такі заходи:

1. Електромагнітна сумісність (EMC): Впевніться, що пристрої відповідають вимогам стандартів щодо електромагнітної сумісності.
2. Зони безпеки: Встановлюйте зони, де рівень електромагнітного випромінювання є безпечним для протягом тривалого часу. Забезпечте, щоб користувачі могли уникати тривалого перебування в зоні високого впливу.
3. Захисні пристрої: Розгляньте можливість використання захисних пристроїв, таких як екрани та фільтри, щоб зменшити вплив електромагнітного поля на користувачів.
4. Інформаційна кампанія: Проводьте навчальні кампанії для користувачів щодо правил безпеки використання технологій та можливих ризиків.
5. Дослідження та моніторинг: Проводьте дослідження впливу електромагнітного поля на здоров'я, і моніторьте нові розробки в цій області.

Ці заходи можуть сприяти забезпеченню безпечного використання технологій у відповідності з вимогами безпеки та здоров'я

ВИСНОВОК

В даному дипломному проекті була розглянута актуальна проблема заміни аналогового обладнання на сучасну мультисервісну систему на базі обладнання Alcatel-Lucent шляхом перемикання абонентів з аналогових АТС на медіа-шлюзи типу Alcatel 7510 Media Gateway.

Медіа-шлюз Alcatel 7510 Media Gateway, як одна з ключових складових мережевих рішень Alcatel наступного покоління (NGN), Alcatel 7510 Media Gateway забезпечує безперебійну взаємодію голосових з'єднань між комутованою телефонною мережею (PSTN) та IP-мережами. Для вирішення поставленого завдання був проведений аналіз структури існуючої міської телефонної мережі з виявленням особливості міжстанційних зв'язків проектованих медіа шлюзів зі станціями мережі.

Було дано обгрунтування доцільность перемикання абонентів аналогових АТС на Alcatel 7510 Media Gateway. При цьому були враховані такі позитивні якості, властиві цифровим АТС даного типу:

1) хороша сполучність з різними типами існуючих станцій;

2) висока надійність і ремонтопридатність;

3) апаратні засоби легко нарощуються при необхідності збільшення числа абонентів;

4) наявність добре відпрацьованого програмного забезпечення, легкоадаптуючого до будь-якої конфігурації апаратних засобів, і що поставляється в комплекті зі станцією;

5) для абонентів є можливість введення цілого комплексу додаткових послуг;

6) позитивний досвід експлуатації АТС даного типу в реальній мережі, що підтверджує заявлені виробником високі технічні характеристики обладнання.

Так само були розглянуті технічні характеристики обладнання Alcatel-Lucent, структура апаратних засобів і програмного забезпечення, описані основні блоки і

структурні одиниці. Отримані в результаті розрахунку навантаження, створювані користувачами пакетної мережі були покладені в основу розрахунку обсягу обладнання, необхідного для підключення шлюзів.

Таким чином, поставлене в дипломної роботі завдання по заміні аналогового обладнання на мультисервісне обладнання Alcatel-Lucent на міській телефонній мережі вирішено.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Krebs on Security
2. The Hacker News
3. Schneier on Security
4. Dark Reading
5. CyberScoop
6. SecurityWeek
7. Threat Intelligence
8. FireEye Threat Research
9. Trend Micro Blog
10. Symantec Blogs
11. CISA Insights
12. NIST Cybersecurity Insights
13. US-CERT
14. MIT Technology Review - Cybersecurity
15. Naked Security by Sophos
16. BleepingComputer
17. TechCrunch Security
18. Threatpost
19. ZDNet Security
20. CSO Online
21. InfoWorld Security
22. F-Secure Blog
23. Tenable Blog
24. ESET We Live Security Blog
25. SpiderLabs Blog
26. Fortinet Blog

27. Akamai Blog
28. CrowdStrike Blog
29. Carbon Black Blog
30. Cisco Umbrella Blog
31. Radware Blog
32. Guardicore Blog
33. Palo Alto Networks Unit 42 Blog
34. Malwarebytes Labs Blog
35. Kaspersky Lab Securelist Blog
36. BleepingComputer
37. TechCrunch Security
38. Threatpost
39. ZDNet Security
40. CSO Online
41. InfoWorld Security
42. The Register - Security
43. Secureworks Blog
44. IBM Security Intelligence
45. CyberArk Blog
46. SANS Internet Storm Center
47. Imperva Blog
48. Recorded Future Blog
49. Fidelis Cybersecurity Blog
50. Kaspersky Daily
51. NortonLifeLock Blog
52. McAfee Blogs
53. Security Magazine
54. Infosec Magazine
55. CIO Dive - Security

56. SC Media
57. Heimdal Security Blog
58. CyberArk Labs Blog
59. The Intercept - Cybersecurity
60. WIRED - Cybersecurity
61. The Guardian - Technology - Cybercrime
62. CyberScoop - Threats
63. The New York Times - Cybersecurity
64. Ars Technica - Security
65. BBC News - Technology - Cyber Security
66. The Wall Street Journal - Cybersecurity
67. Forbes - Cybersecurity
68. MIT Sloan Management Review - Cybersecurity
69. Infosecurity Magazine
70. TechTarget - Security
71. Krebs on Security
72. The Hacker News
73. Schneier on Security
74. Dark Reading
75. CyberScoop
76. SecurityWeek
77. Threat Intelligence
78. FireEye Threat Research
79. Trend Micro Blog
80. Symantec Blogs
81. CISA Insights
82. NIST Cybersecurity Insights
83. US-CERT
84. MIT Technology Review - Cybersecurity

85. Naked Security by Sophos
86. BleepingComputer
87. TechCrunch Security
88. Threatpost
89. ZDNet Security
90. CSO Online
91. InfoWorld Security
92. F-Secure Blog
93. Tenable Blog
94. ESET We Live Security Blog
95. SpiderLabs Blog
96. Fortinet Blog
97. Akamai Blog
98. CrowdStrike Blog
99. Carbon Black Blog
100. Cisco Umbrella Blog