НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи
фахового молодшого бакалавра

на тему: **Аналіз рішень для впровадження IP-телефонії в корпоративному середовищі**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Остафій Остап Богданович

Керівник _____ Олександра ЗАГОРЯНСЬКА
(підпис)

Нормоконтролер _____ Володимир ПЛІШ
(підпис)

Рецензент _____ Олег ЛЕЩАК
(підпис)

Голова ЕК _____ Андрій ВАХ
(підпис)

Члени ЕК _____ Ігор ТИБЕЛЬ
(підпис)

_____ Володимир ПЛІШ
(підпис)

Дипломна робота захищена в ЕК «__» _____ 2025 р.

з оцінкою «_____»

Львів 2025

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Циклова комісія ***Телекомунікації***
Освітньо-професійний ступінь ***Фаховий молодший бакалавр***
Освітньо-професійна програма ***Телекомунікації та комп'ютерні технології***
Спеціальність ***172 Телекомунікації та радіотехніка***

ЗАТВЕРДЖУЮ
Завідувач відділення
«Телекомунікацій та
комп'ютерних технологій»
_____ Ігор ТИБЕЛЬ
« 25 » квітня 2025 року

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ ЗДОБУВАЧУ

Остафію Остапу Богдановичу
(прізвище, ім'я та по батькові)

1.Тема роботи *Аналіз рішень для впровадження IP-телефонії в корпоративному середовищі*

Керівник роботи *Олександра ЗАГОРЯНСЬКА*
викладач вищої категорії,
(ім'я, прізвище, науковий ступінь, вчене звання)

затверджені наказом директора від " 20 " березня 2025 року № 20-СТ

2. Строк подання студентом роботи "10" червня 2025 року

3. Вихідні дані до роботи *3.1 Дослідити основні принципи функціонування та використання технологій у мережах транспортного рівня*

3.2 Застосувати відмовні модулі у якості засобу забезпечення інформаційної безпеки

3.3 Проаналізувати принципи технології голосового передачі через інтернет VoIP та використання IP-телефонії

3.4 Виконати аналіз ризику нелегітимного доступу до безпечної IP-телефонії

4. Зміст розрахунково-пояснювальної записки

4.1 Аналіз безпеки передачі даних у комп'ютерних мережах на транспортному рівні

4.2 Сутність забезпечення інформаційної безпеки в сучасних умовах

4.3 Захист інформації в контексті технології Voice Over Internet Protocol

4.4Техніко-економічне обгрунтування.

4.5Охорона праці та безпека життедіяльності

5. Перелік графічного матеріалу

5.1.	*Структура складеної мережі*
5.2.	*Взаємодія мереж традиційної телефонії та IP-телефонії*
5.3.	*Компоненти інфраструктури мережі, що базується на протоколі SIP*
5.4.	*Можливий сценарій дій нелегітимного користувача під час атаки на обладнання оператора з метою захоплення контролю*
5.5	*Програмний механізм перевірки аутентифікаційного рядка*

6. Консультанти розділів дипломної роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	Завдання отримав
Техніко-економічне обґрунтовування	*Мар'яна СМУК викладач вищої категорії*	*25.04.2025р.*	*25.04.2025р*
Охорона праці та безпека життєдіяльності	*Олена МЕЛЬНИКОВА викладач першої категорії*	*25.04.2025р.*	*25.04.2025р.*

7. Дата видачі завдання « 25» квітня 2025 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання	Примітка
1	*Вступ.*	*25.04-01.05*	
2	*Аналіз безпеки передачі даних у комп'ютерних мережах на транспортному рівні*	*02.05-08.05*	
3	*Сутність забезпечення інформаційної безпеки в сучасних умовах*	*09.05-15.05*	
4	*Захист інформації в контексті технології Voice Over Internet Protocol*	*16.05-22.05*	
5	*Техніко – економічне обґрунтування*	*23.05-29.05*	
6	*Охорона праці та безпека життєдіяльності*	*30.05-03.06*	
7	*Висновки*	*04.06-05.06*	
8	*Підготовка графічного матеріалу.*	*06.06-09.06*	

Здобувач _____ *Остап ОСТАФІЙ*
(підпис) (ім'я, прізвище)

Керівник роботи _____ *Олександра ЗАГОРЯНСЬКА*
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Текстова частина дипломної роботи: 82 с., 18 рис., 4табл., 9 джерел.

Об’єкт дослідження – є телефонна мережа, виконана за технологією VoIP на базі протоколу SIP.

Мета роботи – полягає у вдосконаленні методу підвищення ефективності IP-протоколу розподілення секретної інформації ZRTP.

Метод дослідження – є аналіз літературних джерел, новітніх публікацій за темою дослідження, моделювання моделі несанкціонованого користувача.

Важливість даної роботи обумовлена значущістю телефонного спілкування у сучасних підприємствах, де пошук ефективних і економічних методів забезпечення якості та безпеки телефонних дзвінків стає пріоритетним завданням для управління. Методика дослідження полягає у критичному аналізі наукових джерел та останніх публікацій, а також у розробці моделей несанкціонованого користувача. Наукова новизна полягає у введенні методу підвищення безпеки IP-телефонії та програмного забезпечення, який використовує автоматизовану програмно-апаратну перевірку аутентифікаційного рядка, відмінний від існуючих методів виявлення несанкціонованих користувачів. Практичне значення роботи полягає у можливості використання її результатів корпоративними установами для забезпечення високого рівня безпеки IP-телефонії та програмного забезпечення загальної секретної інформації.

ЗАХИСТ ІНФОРМАЦІЇ, IP-ТЕЛЕФОНІЯ, VOICE OVER INTERNET PROTOCOL.

ЗМІСТ

ВСТУП…….. 7
1 АНАЛІЗ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ТРАНСПОРТНОМУ РІВНІ ……..…….. 8
1.1 Еволюція та застосування мережевої моделі OSI……..……..…….. 8
1.2 Дослідження принципів функціонування та використання технологій у мережах транспортного рівня ……..... 11
1.3 Основні протоколи інформаційно-комунікаційних систем……... 14
2 СУТНІСТЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ ……. 22
2.1 Аналіз заходів захисту даних в корпоративних мережах ……..... 22
2.2 Застосування відмовних модулів у якості засобу забезпечення інформаційної безпеки ……..……...……..... 25
2.3 Стратегії забезпечення безпеки для критичної інформаційної інфраструктури ……..…...……. 29
3 ЗАХИСТ ІНФОРМАЦІЇ В КОНТЕКСТІ ТЕХНОЛОГІЇ VOICE OVER INTERNET PROTOCOL ……..……..... 35
3.1 Принципи технології голосового передачі через Інтернет VoIP та використання IP-телефонії …….…….... 35
3.2 Аналіз ризику нелегітимного доступу до безпечної IP-телефонії ……... 47
3.3 Підвищення ефективності IP-протоколу ZRTP за допомогою автоматизованої перевірки аутентифікаційного рядка…… 59
4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ……..... 65
4.1 Розрахунок капітальних витрат на розробку……..... 65
4.2 Складові структури витрат на розробку…….. 65
4.3 Витрати на відлагодження розробки…….. 67
5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ…… 69
5.1 Загальні положення……... 69
5.2 Організація охорони праці на підприємстві…… 70

5.3 Заходи безпеки на робочому місці……... 72
5.4 Санітарно-гігієнічні вимоги…….. 73
ВИСНОВКИ …… 75
ПЕРЕЛІК ПОСИЛАНЬ……..... ……. 76
КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ…….…….. 77
Лист 1 Структура складеної мережі ……...……... 78
Лист 2 Взаємодія мереж традиційної телефонії та IP-телефонії …… 79
Лист 3 Компоненти інфраструктури мережі, що базується на протоколі SIP …….……..…….. 80
Лист 4 Можливий сценарій дій нелегітимного користувача під час атаки на обладнання оператора з метою захоплення контролю ……..… 81
Лист 5 Програмний механізм перевірки аутентифікаційного рядка ……. 82

ВСТУП

Сьогодні інформаційна безпека стає надзвичайно важливою для будь-якої компанії. Хоча вимоги нормативної бази в цій галузі вже відомі, багато компаній використовують додаткові засоби для забезпечення стійкості своїх інформаційних систем. Важливо розуміти, що захист інформації потребує серйозних ресурсів, особливо коли ставки високі. Сьогодні важливо не лише захищати окремі елементи, але і створювати комплексний захист всієї інформаційної інфраструктури, враховуючи взаємодію між ними.

В останні часи у джерелах інформації все частіше згадують поняття "системного підходу" при створенні систем захисту інформації. Системний підхід не обмежується лише встановленням захисних механізмів; це постійний процес, що охоплює всі етапи життєвого циклу інформаційної системи. Усі засоби, методи та заходи, які застосовуються для захисту інформації, об'єднуються в єдиний, цілісний механізм - систему захисту.

В сучасному світі фахівці з різних галузей часто змушені стикатися з проблемами забезпечення інформаційної безпеки. Це особливо актуально в організаціях, де користувачі мають різні рівні доступу до різноманітних інформаційних ресурсів. Завданням системних адміністраторів є захист усіх інформаційних ресурсів компанії від несанкціонованого доступу. Для цього потрібно впроваджувати сучасні технології інформаційної безпеки, що відповідають поточним вимогам. На ринку інформаційних технологій представлено різноманітні системи захисту, і вибір конкретної для вирішення певної задачі може бути складним завданням. Тому важливо коректно оцінювати існуючі та потенційні системи захисту, щоб забезпечити ефективний захист інформації.

1 АНАЛІЗ БЕЗПЕКИ ПЕРЕДАЧІ ДАНИХ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ТРАНСПОРТНОМУ РІВНІ

1.1 Еволюція та застосування мережевої моделі OSI

Модель OSI (Open Systems Interconnection) – стандартна мережева модель, що була розроблена Міжнародним комітетом зі стандартизації (ISO) у 1978 році для полегшення розробки мережевих протоколів та покращення взаємодії відкритих систем. Ця модель включає сім рівнів, кожен з яких виконує свої функції у процесі передачі даних. Однак, хоча модель OSI мала амбітні цілі, її реалізація ніколи не була повністю завершена через складність і великий обсяг роботи, що потрібен для її впровадження.

Незважаючи на те, що модель OSI не стала домінуючим стандартом, її вплив на розвиток мережевих технологій був значним. У 1984 році вона була прийнята як міжнародний стандарт для мережних комунікацій, а IEEE опублікував специфікацію 802, що детально описала механізми взаємодії фізичних пристроїв на канальному та фізичному рівнях моделі OSI.

У моделі OSI сім рівнів розташовані вертикально, кожен виконує свої функції та взаємодіє зі своїми сусідами. Наприклад, прикладний рівень (Application layer), що є верхнім рівнем, забезпечує взаємодію мережі та користувача, надаючи доступ до мережних служб та обробника запитів до баз даних.

Таблиця 1.1– Компоненти мережевої моделі OSI

Рівень моделі OSI	Функції
7. Прикладний	Забезпечує взаємодію мережі та користувача.
6. Представлення	Відповідає за перетворення даних в зручний для обробки формат та шифрування і дешифрування інформації.
5. Сеансовий	Контролює встановлення, управління та завершення сеансів між програмами на різних комп'ютерах.
4. Транспортний	Забезпечує безперервну передачу даних між комп'ютерами, відповідаючи за розбиття та збірку повідомлень.

Продовження таблиці 1.1

3. Мережевий	Відповідає за маршрутизацію даних в мережі, визначає найкращий шлях для доставки інформації.
2. Канальний	Організовує безпосередню передачу даних між пристроями на мережевому рівні, відповідає за адаптацію до фізичної мережі.
1. Фізичний	Відповідає за фізичне з'єднання між пристроями, передачу бітів через мережеве середовище.

Функції рівня представлення включають обробку протоколів та кодування/декодування даних. Цей рівень відповідає за перетворення запитів програм, отриманих з прикладного рівня, у формат для передачі по мережі, а також за перетворення отриманих з мережі даних у формат, зрозумілий застосункам. Тут може відбуватися стиснення/розпакування, кодування/декодування даних та перенаправлення запитів іншому мережевому ресурсу, якщо це необхідно.

Сеансовий рівень відповідає за керування сеансами зв'язку між програмами, забезпечуючи можливість взаємодії тривалий час. Він контролює створення/завершення сеансів, обмін інформацією, синхронізацію завдань і визначення прав доступу до даних. Сеансовий рівень також забезпечує синхронізацію передачі даних шляхом розміщення контрольних точок у потоці даних, що допомагає відновити процес у випадку виникнення проблем з взаємодією.

Рівень транспорту (Transport Layer) – це четвертий рівень мережевої моделі OSI, який забезпечує надійну доставку даних без помилок, втрати або дублювання у відповідній послідовності. Цей рівень відповідає за передачу блоків даних, що можуть бути розділені на фрагменти чи об'єднані в один, залежно від протоколу.

Мережевий рівень (Network Layer) – третій рівень мережевої моделі OSI, який визначає шлях передачі даних через мережу. Він здійснює трансляцію логічних адрес в фізичні, визначає найкоротші маршрути, здійснює комутацію та маршрутизацію пакетів, а також відслідковує помилки та затори у мережі.

Канальний рівень (Data Link Layer) – це другий рівень мережевої моделі OSI, що забезпечує взаємодію мереж на фізичному рівні та контроль за можливими помилками. Він упаковує отримані дані у кадри, перевіряє їх на

цілісність та виправляє помилки, якщо це необхідно, передаючи їх на мережевий рівень. Цей рівень також взаємодіє з фізичними рівнями, регулюючи і керуючи цією взаємодією.

Фізичний рівень (Physical layer) – це нижчий рівень моделі OSI, що забезпечує безпосередню передачу потоку даних через мережу. На цьому рівні відбувається передача електричних або оптичних сигналів через кабель, а також їхній прийом та перетворення в біти даних за допомогою методів кодування цифрових сигналів.

Фізичний рівень визначає тип середовища передачі (наприклад, мідний кабель або оптичне волокно), конектори, форму представлення бітів даних та схеми передавача і приймача. Він отримує кадр даних від канального рівня, кодує його у послідовність сигналів і передає через лінію зв'язку. Кадр даних не передається як єдине ціле, а представляється послідовністю сигналів, що передаються один за одним. Сигнали, в свою чергу, відображають біти даних кадру.

У сучасних мережах зазвичай використовуються три основних типи середовищ передачі: мідні кабелі, оптичні волокна та бездротове з'єднання. Тип сигналу, який використовується для передачі даних, залежить від обраного середовища передачі. Наприклад, для мідних кабелів сигнали зазвичай є електричними імпульсами, для оптичних волокон - світловими імпульсами, а для бездротових з'єднань - радіохвилями, що представляють собою електромагнітні хвилі.

Стандарти технологій фізичного рівня формуються і підтримуються провідними організаціями, такими як Міжнародна організація зі стандартизації (ISO), Інститут інженерів електротехніки та електроніки (IEEE), Американський національний інститут стандартів (ANSI), Міжнародний телекомунікаційний союз (ITU), Альянс електронної промисловості/Асоціація телекомунікаційної промисловості (EIA/TIA) та інші. Ці стандарти визначають параметри і вимоги до фізичних та електричних характеристик передавального середовища, механічні властивості, такі як матеріали та розміри конекторів, а також правила кодування

бітів у сигнали та управління інформацією. Усі складові апаратного забезпечення, такі як мережеві адаптери (Network Interface Card, NIC), інтерфейси та конектори, а також матеріали та конструкції кабелів, повинні відповідати цим стандартам. Важливо відзначити, що функціональні можливості фізичного рівня вбудовані безпосередньо у апаратне забезпечення мережі.

Фізичний рівень забезпечує основні функції, необхідні для передачі даних через мережу. Він включає в себе фізичне обладнання, таке як кабелі, пристрої передачі сигналів та конектори, які використовуються для передачі бітів даних. Одна з важливих функцій - це кодування даних, яке перетворює потік бітів у певний код. Це необхідно для забезпечення правильного розпізнавання переданих даних як відправником, так і отримувачем. Крім того, методи кодування також допомагають виявити та виправити помилки, які можуть виникнути під час передачі. Фізичний рівень взаємодіє з іншими рівнями мережі через інтерфейси та протоколи, забезпечуючи ефективну передачу даних.

1.2 Дослідження принципів функціонування та використання технологій у мережах транспортного рівня

Основні завдання мережного рівня, відповідно до моделі взаємодії відкритих систем, включають передачу пакетів між різними вузлами у складних мережах, вибір оптимального маршруту для передачі пакетів та узгодження протоколів канального рівня, які використовуються в різних підмережах однієї комплексної мережі.

Зазвичай протоколи мережного рівня реалізовані у вигляді програмних модулів, що запускаються на кінцевих вузлах, таких як комп'ютери (хости), а також на проміжних вузлах, наприклад, маршрутизаторах або шлюзах. Здійснення функцій маршрутизації може здійснюватися як спеціалізованими пристроями, так і загальнопризначеними комп'ютерами з відповідним програмним забезпеченням.

Основна мета введення мережного рівня полягає у вирішенні проблем, пов'язаних з управлінням складеними мережами. Система мережі розглядається

як сукупність декількох окремих мереж, що співпрацюють між собою, і отримує назву складеної мережі або інтермережі. Кожна окрема мережа в цій системі називається підмережею, складовою мережею або просто мережею рис. 1.1 [14].

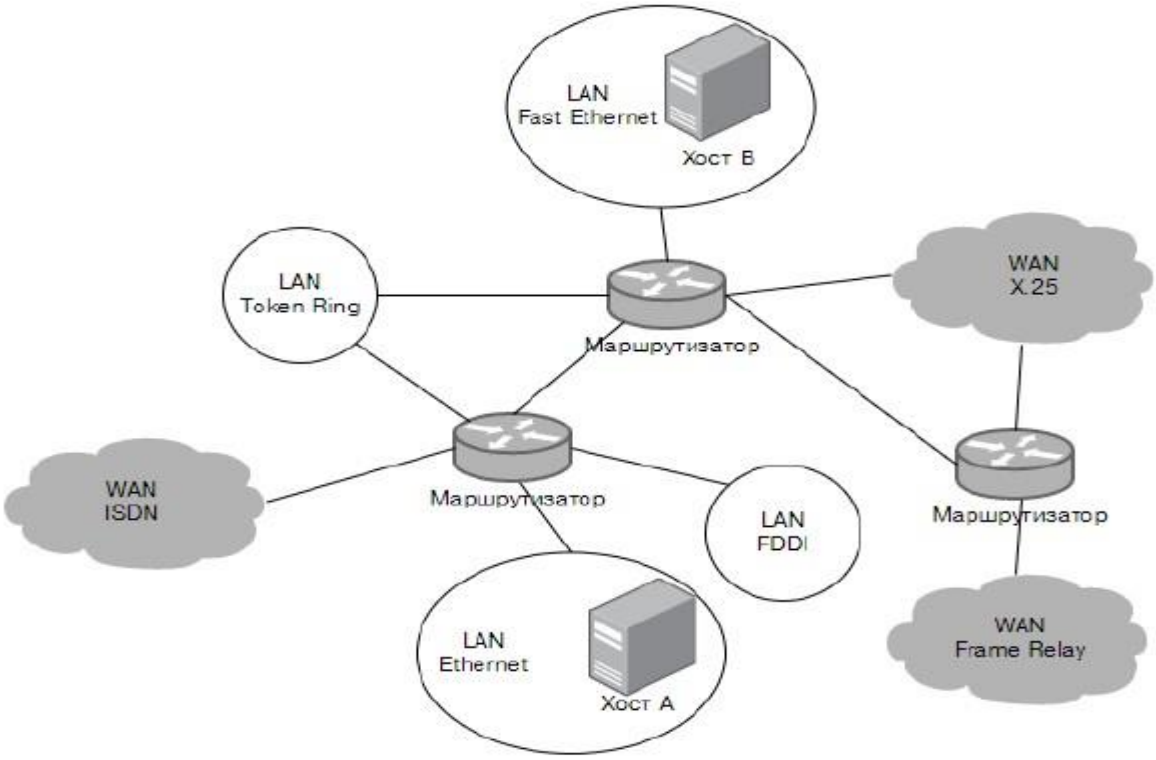

Рисунок 1.1 – Структура складеної мережі

Взаємозв'язок підмереж через маршрутизатори є ключовим аспектом складеної мережі. У такій мережі можуть бути представлені як локальні, так і глобальні мережі, кожна з яких має свою внутрішню структуру, що не відображена на діаграмі, оскільки не впливає на роботу мережного протоколу. Взаємодія вузлів у межах кожної підмережі забезпечується використанням відповідних технологій, таких як Ethernet, Fast Ethernet, Token Ring, FDDI для локальних мереж і Frame Relay, X.25, ISDN для глобальних. Однак для забезпечення зв'язку між вузлами різних підмереж необхідні додаткові засоби, що надає мережний рівень.

Роль мережного рівня полягає в організації спільної роботи всіх підмереж у складеній мережі для ефективного переміщення пакетів даних. Для використання

технологій, що домінують у підмережах, мережний рівень взаємодіє з їх системами адресації.

Хоча деякі технології локальних мереж (наприклад, Ethernet, Token Ring, FDDI, Fast Ethernet) використовують спільну систему MAC-адрес для ідентифікації вузлів, інші технології (такі як X.25, ATM, Frame Relay) мають свої власні схеми адресації. Адреси, призначені вузлам згідно з технологіями підмереж, вважаються локальними. Щоб мережний рівень міг ефективно працювати, йому потрібна власна система адресації, яка б не залежала від адресації вузлів у окремих підмережах, і дозволяла однозначно ідентифікувати будь-який вузол складеної мережі. Один із способів формування мережної адреси - це унікальне присвоєння номерів усім підмережам у складеній мережі та номерів вузлів у межах кожної підмережі. Отже, мережна адреса складається з номера мережі (підмережі) і номера вузла в цій мережі (підмережі).

Мережний рівень відповідає за передачу даних через складену мережу, забезпечуючи їхнє упаковування у пакети з заголовками мережного рівня. Уніфікований формат заголовка пакета мережного рівня дозволяє незалежно від типу мережі включати інформацію про призначення пакета. Мережний рівень обирає маршрут та керує переміщенням пакетів між підмережами.

Коли дві або більше мережі об'єднуються для спільної транспортної служби, цей вид взаємодії часто називається міжмережною взаємодією (internetworking).

Маршрутизатори використовують спеціальні протоколи маршрутизації для автоматичної побудови таблиць маршрутизації, обмінюючись інформацією про топологію складеної мережі. Ці протоколи, які включають RIP, OSPF, NLSP, забезпечують різні стратегії маршрутизації в мережі.

Протоколи маршрутизації відрізняються від звичайних мережних протоколів, таких як SP і IPX, оскільки вони спеціалізовані на передачі маршрутної інформації, а не користувацьких даних. Хоча обидва види протоколів виконують функції мережного рівня моделі OSI, протоколи маршрутизації використовуються для обміну маршрутною інформацією та включають дані у

пакети мережного рівня або транспортного рівня. З цього погляду, протоколи маршрутизації можна було б формально віднести до рівнів вище за мережний.

Протоколи маршрутизації допомагають маршрутизаторам побудувати карту зв'язків у мережі, визначити оптимальні маршрути для передачі пакетів і заповнити таблиці маршрутизації. Ця інформація допомагає визначити, куди направляти пакети для кожної мережі, забезпечуючи ефективну доставку.

Протоколи маршрутизації важливі для підтримки оптимального маршруту у мережі, особливо при зміні конфігурації мережі. Однак, неефективне використання цих протоколів може призвести до зациклення пакетів і втрати даних.

Транспортний рівень забезпечує передачу даних між вузлами мережі з необхідним рівнем надійності. Протоколи на цьому рівні відповідають за встановлення з’єднання, нумерацію, буферизацію та упорядкування пакетів, забезпечуючи ефективний обмін інформацією між процесами користувача.

Два ключові протоколи на транспортному рівні – це UDP (User Datagram Protocol), який забезпечує надсилання датаграм без встановлення з'єднання, та TCP (Transmission Control Protocol), який керує передачею даних з установленням з'єднання та перевіркою доставки.

При надходженні пакетів на транспортний рівень, операційна система організовує їх у черги до відповідних прикладних процесів. Ці черги в термінології TCP/IP відомі як порти. Кожен порт ідентифікує певний прикладний процес і має 16-бітний номер, що знаходиться у діапазоні від 1 до 65535. Комбінація номера порту, номера мережі та номера вузла однозначно визначає призначений процес у мережі. Цей набір параметрів називається сокетом.

1.3 Основні протоколи інформаційно-комунікаційних систем

Сучасний етап розвитку телекомунікацій характеризується новими напрямами, які відображають перехід від простого росту кількості до покращення

якості послуг. Це означає розширення асортименту телекомунікаційних послуг, які тепер інтегруються з різними інформаційними сервісами.

Крім того, мережі телекомунікацій починають інтегруватися, стають більш функціональними і отримують глобальний охоплюючий характер, аналогічно комп'ютерним мережам.

Давайте оглянемо ключові особливості телекомунікаційних систем та мереж, що важливі для переходу від традиційних мереж до мереж нового покоління NGN (Next Generation Networks):

– Використання програмних комутаторів Softswitch для управління послугами та потоками інформації, що дозволяє зробити мережу набагато більш гнучкою.

– Застосування надійних та безпечних протоколів, спеціально розроблених для верхніх рівнів телекомунікаційних мереж.

– Перехід до нової архітектури мережі NGN, яка орієнтована на гнучку та ефективну систему створення та надання різноманітних послуг, як телекомунікаційних, так і інформаційних.

Кожен тип трафіку потребує відповідного рівня пропускної здатності, гарантованої затримки та стандартної рівня варіацій. Забезпечення цих вимог від трафіку вимагає відповідних технологій передачі даних. Оскільки абстрактний трафік може бути різноманітним і нестабільним, виникає необхідність у його класифікації за номером або типом. Однак індивідуальна обробка кожного типу трафіку може бути витратною. Вирішення цієї проблеми може полягати в групуванні трафіку за номером або типом, що спрощує обробку та може зменшити витрати.

Індивідуальне або групове обслуговування передбачає введення управління затримками та може бути застосоване лише у випадку стабільного маршруту передачі. Проте для ефективного використання цих методів необхідно, щоб усі групи в мережі були однаковими. У випадку зміни маршруту передачі потрібно передавати параметри обслуговування разом з трафіком, що може стати викликом у складних мережах з багатьма підмережами.

У зв'язку з ростом використання вузькосмугових каналів виникла потреба встановлювати та підтримувати з'єднання (логічні канали) всередині мережі. У минулому, коли вузькосмугові канали не були настільки завантаженими, не виникало потреби передавати через них велику кількість потоків. Оскільки кожен користувач намагався використовувати максимальну доступну пропускну здатність, це призводило до конфліктів і хаосу в мережі. Для управління цим хаосом були розроблені методи чергування, які визначали, які потоки мають перевагу. Проте виникала проблема, коли великі блоки даних переміщувалися через канал, а раптово приходили маленькі, але дуже швидкі пакети, які вимагали негайного перевезення без черги.

Слово "маршрутизація" відноситься до процесу направлення інформації від джерела до призначення через мережу. Ключовою складовою системи протоколів Інтернет є протоколи маршрутизації. На сьогодні відомо 9 протоколів, кожен з яких, в залежності від своєї версії, виконує конкретні завдання. Проте виникає криза у розвитку протоколів маршрутизації, спричинена бажанням усіх учасників ринку інформаційних технологій використовувати Інтернет для передачі різних типів інформації, включаючи аудіо, відео, дані та графіку. Кожен з цих видів інформації має власні, часто взаємно виключні, вимоги до протоколів маршрутизації[14].

Протоколи маршрутизації стають основними місцями збоїв у сучасних мережах зв'язку через використання так званих "таблиць маршрутів" для навігації. В разі неполадок у обладнанні, розривів або перевантажень на лініях зв'язку потрібно динамічно змінювати ці таблиці, проте це може бути вкрай складно та навіть неможливо через унікальність ситуації. Це призводить до невідповідності результатів обчислень протоколів маршрутизації та виникнення інерції, що додатково ускладнює ситуацію [6].

Ще одним негативним явищем у мережі передачі даних є резонанс. Виникнення цього ефекту пов'язане з методом транспортування даних через канали зв'язку. У режимі негарантованої доставки, для стабільних з'єднань транспортний рівень використовує механізм повторних запитів. Коли користувачі

використовують подібні правила повторних запитів, це створює аналогію з багатьма майже ідентичними генераторами, що може призвести до ефекту резонансу в системах з великою кількістю джерел сигналів. Це може призвести до перенавантаження каналів зв'язку та ускладнити задачу підтримки коректного стану маршрутних таблиць. Одержання необхідної службової інформації та її передача тими ж каналами робить завдання забезпечення збіжності та стабільності ще більш складним.

Для підтримки ефективного впровадження нових технологій активно розробляються, уніфікуються та стандартизуються нові пристрої мережевого обладнання, такі як мости, комутатори (як апаратні, так і програмні), маршрутизатори, міжмережні екрани, шлюзи, а також вузли управління та комутації послуг. Один із таких типових пристроїв – це Softswitch, або програмний комутатор [7].

Програмний комутатор – це комплексне програмно-апаратне забезпечення, що стає головним інтелектуальним центром мережі. Він відповідає за керування обробкою телефонних викликів у різних мережах, включаючи мережі з комутацією пакетів. Softswitch надає мережі інтелектуальну основу, здатну керувати і координувати роботу інших елементів мережі, забезпечуючи кращу керованість та масштабованість всієї інфраструктури.

Термін Softswitch наразі охоплює широке різноманіття пристроїв, включаючи програмні комутатори, пристрої для розділення функцій управління з’єднаннями і комутації, а також високошвидкісні маршрутизатори.

Softswitch виконує різноманітні завдання, включаючи:

– функцію універсального конвертора протоколів сигналізації і контролю для забезпечення взаємодії між мережами з комутацією каналів та мережами з комутацією пакетів;

– розвантаження операторських мереж від Інтернет-трафіку та його обліку, маршрутизації телефонного трафіку через IP-мережі, та обробки трафіку комутованого доступу з міських мереж;

– доставку інтелектуальних послуг та транзит телефонного трафіку через IP-мережі;

– забезпечення доступу, включаючи широкосмуговий доступ та передачу великих обсягів даних через вузькосмугові абонентські лінії;

– оптимізацію транзиту на мережах мегаполісів та організацію єдиного білінгу для абонентів телефонних мереж загального користування та IP-мережі.

Початковий стандарт для протоколів, що визначають взаємодії вузлів у сфері IP-телефонії, був вироблений Комітетом зі стандартизації телекомунікаційного сектору Міжнародного телекомунікаційного союзу (ITU-T) у 1996 році. Цей стандарт, відомий як H.323, регулює такі взаємодії. Початкові рекомендації, які стосувалися передачі голосового та відеотрафіку, були розроблені на початку 90-х років, проте вони спрямовані на використання ISDN замість IP-мереж для транспорту цього трафіку. У 1998 році була прийнята друга версія цього стандарту - H.323 v.2 (Packet-based multimedia communication systems - мультимедійні системи зв’язку для мереж з комутацією пакетів). У вересні 1999 року була затверджена третя версія рекомендацій, а 17 листопада 2001 року була схвалена четверта версія стандарту H.323[8].

В даний час стандарт H.323 вважається одним із ключових у серії. Цей стандарт визначає рекомендації ITU-T для використання мультимедійних додатків у комп'ютерних мережах, які не мають гарантованої якості обслуговування (QoS). Серед таких мереж - IP- та IPX-мережі на основі Ethernet, Fast Ethernet та Token Ring.

Одночасно з рекомендаціями ITU-T Європейський інститут стандартизації телекомунікацій (ETSI) розпочав роботу над проектом TIPHON (Telecommunications and IP Harmonization over Network). Головним завданням цього проекту є вирішення проблем взаємодії між мережами пакетної комутації і мережами комутації каналів.

Крім того, Комітетом IETF (Internet Engineering Task Force) проводиться розробка протоколів і стандартів, спрямованих на розвиток мультимедійних можливостей Інтернету. Один з таких протоколів - протокол резервування

ресурсів RSVP (Resource Setup Reservation Protocol), який був представлений комітетом у документі RFC-2205.

Протокол RSVP відкриває можливість кінцевим системам резервувати мережні ресурси для забезпечення необхідної якості обслуговування. Відправники надсилають маршрутизаторам загальні параметри трафіку, такі як швидкість передачі даних та його варіабельність, тоді як одержувачі визначають потрібний рівень обслуговування. Маршрутизатори об'єднують запити на виділення ресурсів вздовж загальних маршрутів руху корисного навантаження.

Для забезпечення передачі даних у режимі реального часу був створений протокол RTP (Real-time Transport Protocol), який описаний у документі RFC-1889. При використанні RTP кожен переданий пакет даних містить інформацію про час його відправлення, що дозволяє приймаючій стороні правильно впорядковувати отримані пакети за часом.

Додатковим інструментом для адаптації застосувань до змінного навантаження на мережу є протокол RTCP (Real-time Transport Control Protocol). Цей протокол дозволяє застосуванням відстежувати пропускну здатність мережі і, при необхідності, переходити у режим кодування/декодування аудіосигналу меншої якості, коли навантаження на мережу значно зростає.

Декілька спеціалізованих робочих груп у складі IETF займаються розробкою протоколів, спрямованих на вузькоспеціалізовані області застосування. Одна з таких груп, MMUSIC (Multiparty Multimedia Session Control), розробила протокол прикладного рівня SIP (Session Initiation Protocol), який описаний у документі RFC-2543 і був прийнятий як стандарт у березні 1999 року.

Наразі декілька робочих груп у складі IETF активно працюють над проектами, що використовують концепцію класу обслуговування CoS (Class of Service). Одним із таких проектів є механізм MPLS (Multiprotocol Label Switching) та специфікація Diff-Serv (Differential Services). MPLS дозволяє призначити IP-пакетам спеціальну мітку, яка вказує шлях для їхнього проходження через мережу, що суттєво зменшує час пошуку маршруту. Технологія Diff-Serv

дозволяє різним застосуванням отримувати різний рівень обслуговування, встановлюючи для них відповідні значення параметрів QoS у IP-пакетах.

Додатково, в рамках IETF функціонують робочі групи, такі як MEGACO, яка розробила протокол управління шлюзами MGCP (Media Gateway Control Protocol). Також, для ефективної взаємодії між шлюзами, був розроблений протокол SCTP (Stream Control Transport Protocol) робочою групою IETF SIGTRAN. SCTP призначений для заміни протоколів TCP/UDP в мережах, побудованих на основі MGCP, щоб забезпечити оптимальну роботу системи.

У напрямку поліпшення протоколу MGCP, робоча група MEGACO у складі IETF та дослідна група SG 16 в рамках ITU-T запропонували розробку протоколу MEGACO/H.248. Цей протокол, спочатку базувався на протоколі MGCP, проте представляє собою більш функціональну та вдосконалену версію свого попередника.

Стек протоколів, який використовується для взаємодії за допомогою протоколу SIP, включає такі компоненти:

– протокол ініціювання сесійного зв'язку (Session Initiating Protocol) на рівні прикладного програмного забезпечення;

– протоколи TCP/UDP на рівні транспортного забезпечення;

– протоколи IPv4 і IPv6 на рівні мережевого забезпечення;

– кадри Ethernet та ATM на рівні канального забезпечення;

– фізичні середовища передачі, такі як UTPS та оптичний кабель, на рівні фізичного забезпечення.

У останні роки використання комп'ютерних технологій у різних сферах автоматизації та управління призвело до зростання проблеми забезпечення безпеки обміну інформацією в комп'ютерних системах, що працюють за моделлю OSI (Open System Interconnection). Однією з основних проблем протоколів транспортного рівня в таких системах є відсутність перевірки джерела інформації, що створює ризики її перехоплення та несанкціонованого доступу до відкритих портів транспортного рівня.

Для захисту від перехоплення та несанкціонованого доступу використовуються додаткові протоколи, які забезпечують шифрування даних та автентифікацію учасників обміну інформацією. Один з таких протоколів - SSL/TLS (Secure Socket Layer / Transport Layer Security), який забезпечує шифрування та автентифікацію між транспортними рівнями приймача і передавача даних.

Отже, протокол SSL/TLS забезпечує автентифікацію, шифрування даних і забезпечення цілісності даних. Автентифікація відбувається через обмін цифровими сертифікатами при встановленні з'єднання. Оскільки протокол SSL/TLS реалізується на транспортному рівні, захищене з'єднання утворюється «з кінця в кінець» через захищений віртуальний тунель транспортного рівня. Протокол на прикладному рівні SSL/TLS часто використовується для забезпечення шифрування трафіку HTTP (режим HTTPS).

Використання відкритих протоколів на прикладному рівні створює значні загрози безпеці інформації через передачу даних у нешифрованому вигляді. Процедури ідентифікації, автентифікації користувачів та їх подальша авторизація також стають об'єктом загроз, оскільки можуть бути піддані перехопленню або підбору. Додатковими загрозами є віруси, шпигунське програмне забезпечення, а також DoS та DDoS-атаки на інформаційні системи.

Відомі виробники мережевого обладнання пропонують спеціалізовані рішення для комплексного захисту корпоративних мереж. Наприклад, компанія Cisco пропонує рішення на основі технології NAC (Network Admission Control). Ця технологія дозволяє не лише перевіряти пристрої та користувачів на етапі підключення до мережі, але й блокувати доступ до комп'ютерів, які не відповідають встановленим політикам безпеки. Контроль відповідності політиці безпеки здійснюється на портах комутаторів, точках доступу Wi-Fi або маршрутизаторах, які підтримують технологію NAC.

2 СУТНІСТЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНИХ УМОВАХ

2.1 Аналіз заходів захисту даних в корпоративних мережах

Оцінка інформаційної безпеки є важливим аспектом в управлінні інформаційними технологіями. Ця область залучає значну увагу з моменту народження інформаційних технологій. Однією з ключових складових оцінки є нормативні документи, які встановлюють стандарти і критерії безпеки інформаційних систем. До найважливіших таких документів можна віднести: стандарт ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою; стандарт NIST SP 800-53, що містить керівні принципи та вимоги до захисту інформації в федеральних системах США; та інші національні та міжнародні стандарти, які визначають методики оцінки та вдосконалення безпеки інформаційних технологій [1].

Нормативні документи, що розглянуті, визначають фундаментальні принципи та методики для забезпечення інформаційної безпеки у різних сферах. Проте, для успішного досягнення цієї мети необхідно застосовувати широкий спектр підходів та методів. Це включає в себе формальні методи моделювання процесів та оцінки ефективності, а також неформальні методи декомпозиції та структуризації компонентів систем і процесів.

При впровадженні заходів захисту, важливо збалансувати можливий збиток від несанкціонованого доступу до інформації з розміром витрат на забезпечення безпеки. Ефективність захисту можна підвищити шляхом дослідження різних підходів до оцінки рівня захисту та вибору відповідних систем захисту. Ця оцінка завжди є індивідуальною і залежить від різних факторів, таких як вартість інформації, статус організації, важливість даних, існуючі технології та ресурси.

Інформаційні ресурси неможливо уявити без доступу до них, і в сучасному світі доступність інформації є ключовою складовою успішного функціонування.

Забезпечення доступності означає збереження нормальної взаємодії між користувачем та інформаційним ресурсом.

Для забезпечення конфіденційності інформації важливо встановити ефективний режим доступу до неї. Конфіденційність означає, що інформація залишається недоступною для тих, хто не має на це права. Це досягається через адекватність режиму доступу.

Сьогодні діяльність більшості організацій неможлива без мережі Інтернет. Однак разом з можливостями, які надає Інтернет, зростає і ризик збитку. Тому проблема забезпечення безпеки в інформаційних системах є дуже актуальною. Цей сегмент постійно розвивається і вдосконалюється для забезпечення найвищого рівня захисту від мережевих загроз.

На сьогоднішній день мережеві екрани (брандмауери, файерволи, фільтруючі маршрутизатори і т. д.) залишаються одними з основних інструментів захисту комп'ютерних інформаційних систем. Вони служать не лише засобом реалізації політики безпеки на мережевому рівні, але й надають певний рівень захисту.

Рівень безпеки, який забезпечується мережевим екраном, може варіюватися в залежності від потреб і вимог безпеки конкретної системи. Традиційно існує компроміс між безпекою, простотою використання, вартістю і складністю.

Одним з ефективних засобів забезпечення безпеки інформаційних систем в мережі Інтернет є використання VPN (віртуальних приватних мереж). VPN дозволяє об'єднувати різні локальні мережі в єдину віртуальну мережу, що забезпечує захищений канал передачі даних між ними. Це досягається за допомогою криптографічних методів, що забезпечують конфіденційність, цілісність та аутентифікацію даних.

Оцінка рівня захисту інформаційних ресурсів вимагає визначення їх поточного стану, що може бути здійснено двома різними підходами: «дослідженням знизу догори» та «дослідженням згори донизу».

При використанні першого підходу адміністратори проводять аналіз захисту, спрямований на виявлення різних видів можливих атак, які можуть бути

спробами порушення безпеки інформаційного ресурсу. Однак цей підхід може бути обмежений тим, що навіть найкращі адміністратори не можуть передбачити всі можливі методи атак та не завжди мають повну інформацію про програмно-апаратні засоби зловмисників.

Підхід «згори донизу» передбачає докладний аналіз схем зберігання та обробки даних. Спочатку визначаються всі інформаційні об’єкти та потоки захисту, а потім досліджується стан системи інформаційного захисту для визначення реалізованих методів захисту інформаційних ресурсів та їх рівня. Подальша класифікація всіх інформаційних об’єктів за рівнем конфіденційності, вимогами до доступності та цілісності допомагає забезпечити ефективний рівень захисту.

Останнім етапом є проведення оцінки ризиків, що передбачає визначення потенційних збитків для компанії внаслідок можливих порушень захисту інформаційних ресурсів. Наближений ризик обчислюється як добуток «потенційного збитку від атаки» на «ймовірність такої атаки». Зазвичай, оцінка ризиків включає аналіз ризиків та оцінку потенційного збитку.

Загальна методологія оцінки інформаційної безпеки передбачає три етапи: підготовчий, основний та завершальний.

На підготовчому етапі ключові учасники - замовник оцінки та експерт. Замовник інформує всіх зацікавлених сторін про необхідність проведення оцінки профілю захисту або об'єкта оцінки, надає експерту всю необхідну документацію та матеріали щодо профілю захисту й об'єкта оцінки. Завданням експерта є визначення можливості успішної оцінки на основі отриманих матеріалів та, за необхідності, отримання додаткових матеріалів від замовника чи розробника. Підсумком підготовчого етапу є укладання угоди між замовником та експертом на проведення робіт з оцінки об'єкта чи профілю захисту.

На завершальному етапі основної процедури розробляється технічний звіт з оцінки, який експерт передає для подальшого аналізу. Під час цього етапу експерт вивчає надані матеріали та досліджує профіль захисту або об’єкт оцінки. Він готує цілу низку звітів, в яких враховані вимоги органу контролю, виявлені

недоліки та інша інформація про процес оцінки. У той же час контролюючий орган здійснює безперервний моніторинг процесу відповідно до схеми оцінки.

Під час заключного етапу проводиться всебічний аналіз технічного звіту оцінки з боку контролюючого органу з урахуванням загальних критеріїв методології та вимог схем оцінки безпеки. На основі цього технічного звіту складається підсумковий звіт з оцінки, який містить рішення про відповідність необхідним вимогам. Усі учасники процесу оцінки мають право ознайомитися з підсумковим звітом і вимагати відповідних пояснень.

Багато компаній з різних причин часто не можуть провести повноцінну оцінку захисту своїх інформаційних ресурсів. Тому пропонується використовувати кількісну оцінку рівня захищеності, особливо на етапі впровадження. Застосування кількісної оцінки дозволяє точніше порівняти різні варіанти захисту та обрати найбільш ефективний. Для цього враховують ймовірність виникнення загроз і вразливостей, вартість захищених ресурсів (оцінка втрат при їх втраті) та частоту загроз кожного типу. Необхідно також встановити обмеження на вартість захисної системи та оцінити вплив на продуктивність.

2.2 Застосування відмовних модулів у якості засобу забезпечення інформаційної безпеки

Приманка Honeypot – це інноваційний інструмент у сфері мережевої безпеки, спрямований на виявлення та відстеження зловмисників, які намагаються зламати систему. Ця технологія відрізняється від звичайних методів захисту тим, що не виконує конкретних завдань, а замість цього створює ідеальне середовище для виявлення потенційних загроз. Назва 'Honeypot' відображає концепцію пристрою, який приваблює зловмисників, як мед приваблює бджіл. Протистояти приманкам може бути важко, проте це зовсім не неможливо.

Приманки можуть бути використані для виявлення незаконних дій, коли традиційні методи безпеки генерують багато записів журналу, більшість з яких не

мають значення. В таких випадках Honeypot забезпечує точне виявлення реальних атак або досліджень. Крім того, не всі технології можуть ефективно виявляти невідомі атаки, що робить Honeypot незамінним інструментом у цьому плані.

Пастки також можуть використовуватися для реагування на спроби зловмисників вторгнутися в мережу. Якщо атака виявляється, і одна з атакованих систем є пасткою, отримана корисна інформація дозволяє оперативно реагувати на зловмисника. Використання приманок Honeypot має безліч переваг, але важливо розуміти їхні обмеження і не переоцінювати їхню роль в системі безпеки [2].

Використання технології Honeypot дарує аналітикам безліч переваг. Вона дозволяє збирати цінну інформацію про хакерів, вимоги до системних ресурсів, при цьому маючи простоту управління та чіткість використання. У порівнянні з системами IDS (виявлення вторгнень), які можуть генерувати величезні обсяги інформації щоденно, Honeypot реєструє менші обсяги даних, проте цілком зосереджені на неправомірних діях. Це робить процес аналізу ефективнішим та менш витратним, оскільки інформація, яка потрапляє в Honeypot, має велику цінність та точність.

Одна з головних переваг Honeypot полягає в його ефективності та економічності. Він не потребує значних ресурсів на підтримку та оновлення, оскільки практично автономний після налаштування. Крім того, використання Honeypot демонструє доцільність витрат на безпеку, навіть у випадку, коли вороги не намагаються проникнути в мережу. Він слугує ефективним і доказовим засобом для показу та підтвердження необхідності безпекових витрат.

Програмні приманки можуть бути налаштовані відповідно до різних цілей, включаючи широкий спектр параметрів конфігурації. Від програмних рівнів, які не потребують складних налаштувань, до складних апаратних комплексів, можна виділити різні рівні складності і можливостей програмних приманок. Залежно від їх функціональних характеристик та рівня взаємодії з потенційними загрозами, програмні приманки можуть бути класифіковані на рівні слабкої, середньої та високої інтеграції.

Honeypot з низьким рівнем складності використання є дуже надійними засобами. Вони імітують лише обмежену частину функціоналу служб, що обмежує взаємодію зловмисників з ними. Наприклад, такі приманки можуть імітувати систему UNIX із запущеним сервісом telnet. При спробі підключення до такої приманки зловмисник отримає запит на введення і намагатиметься отримати доступ до системи. Також може бути імітований FTP-сервер з анонімним доступом і файликом, який містить надійно засховані дані, такі як номери кредитних карток. Будь-яка спроба отримати доступ до цього файлика буде зарахована як спроба несанкціонованого доступу. Система веде журнал інцидентів, включаючи час, IP-адресу та порт зловмисника, а також порт, яким він намагався скористатися. Основне завдання таких програмних приманок полягає у мінімізації ризику. Хоча ризик використання таких приманок мінімальний, він присутній через можливість вразливості програмного забезпечення. Проте, сила цих простих приманок полягає в їхній простоті, яка робить їх більш надійними. Такий підхід допомагає мінімізувати ризик, пов'язаний з можливими вразливостями та забезпечує більш високий рівень безпеки системи.

Приманки середнього рівня надають більше можливостей для відтворення дій зловмисника в більш складних та вразливих умовах. Наприклад, така система може імітувати веб-сервери з більш розвиненими функціями, які відповідають на нестандартні команди та мають більш досконалу систему реєстрації. Це розширює можливості зловмисника для взаємодії не лише з імітованими службами, але й з імітованою операційною системою. Проте такий підхід може створювати додаткові проблеми. По-перше, складність такої системи може призвести до помилок на етапі роботи або налаштування, що збільшить вразливість системи. По-друге, надання віртуальному середовищу функціональності реальної системи - це складне завдання. Чим більше функціональності та реалістичності має віртуальне середовище, тим легше зловмисникові обійти це середовище та отримати контроль над реальною операційною системою. Крім того, існує ризик втрати контролю над віртуальною

машиною, якщо шкідливий код вийде з-під контролю віртуальної машини, якщо він спеціально для нього розроблений.

Приманки з високим рівнем взаємодії є найбільш складними та ризикованими, проте вони надають максимальну кількість інформації про зловмисника. Ці приманки моделюють реальні системи, до яких зловмисник може отримати доступ. Вони складаються з вузла приманки, мережевого датчика та сховища інформації. Часто такі приманки розташовуються у мережі за брандмауером, що дозволяє здійснювати фактичний контроль за доступом через брандмауер. Проте неправильна настройка таких вузлів або непередбачені ситуації можуть призвести до ризику доступу зловмисника до мережі. Однак, недоліки такого підходу включають складність реалізації та високі витрати на підтримку.

Аналізуючи недоліки різних способів реалізації приманки, варто враховувати кілька ключових аспектів. Спочатку слід зазначити, що сама ідея приманки передбачає наявність ресурсу, який буде привертати увагу потенційних зловмисників, але будь-яке звернення до нього має викликати підозру. Проте ізольований вузол може також викликати підозру та бажання швидше його залишити. Крім того, якщо у приманки немає іншого трафіку, крім спроб злому, це також може бути підозрілим. Тому важливо створювати віртуальне середовище, яке виглядає як реальна мережа з різними рівнями складності злому, а також налаштовувати мережеві датчики належним чином для надійної реєстрації. Потрібно також бути обережним при роботі з віртуальними машинами, оскільки шкідливий код може вийти з-під контролю та спричинити непередбачені наслідки. Детальний аналіз і належне налаштування приманки на різних рівнях взаємодії є ключовими для успішного виявлення та аналізу потенційних загроз.

Взагалі, при використанні різних стратегій для зламу дуже серйозних ресурсів, таких як державні сайти або банківські системи, зловмисники можуть приховати свою ідентичність шляхом використання проксі-серверів. У такому випадку IP-адреса не є надійним показником, оскільки вона може бути адресою проксі-сервера. Таким чином, відстеження може бути ускладненим, оскільки

потрібно робити заміщення на проксі-серверах. Деякі зловмисники використовують мережу з декількох комп'ютерів, щоб отримати доступ до мережі через модем GPRS/EDGE у мобільному телефоні. Це дозволяє їм віддалено здійснювати атаки, уникнувши виявлення та відстеження їх місцеперебування. Крім того, якщо комп'ютер зловмисника є вразливим, приманка може відповісти контратакою, встановивши вірус або збираючи конфіденційну інформацію, таку як файли cookie [2].

Під час вибору потенційної жертви, зловмиснику необхідно детально вивчити топологію мережі. Важливо переконатися, що цей вузол обробляє зовнішній трафік, має відмінну конфігурацію від конфігурації за замовчуванням та активно використовується іншими учасниками мережі. Після цього зловмисник може провести докладне дослідження протягом кількох днів, скануючи порти та спробуючи викликати переповнення буфера. Він також може атакувати саму систему, використовуючи атаки, які маскують його IP-адресу, такі як DDoS, SYN або ECHO-death.

Honeypot може не вирішити всі проблеми безпеки, тому доведеться або дослідити рівень безпеки окремих частин інфраструктури, або використовувати кілька приманок. Існує певний ризик того, що зловмисник впізнає пастку як фіктивну. Це часто стається через недостатньо ретельну або неправильну постановку приманки, що свідчить про людський фактор в більшості випадків.

2.3 Стратегії забезпечення безпеки для критичної інформаційної інфраструктури

Сучасні виклики у сфері кібербезпеки відзначаються складністю та постійним еволюційним характером. Кібератаки вже давно перетворилися на інструмент для досягнення різноманітних цілей, які можуть бути пов'язані з порушенням конфіденційності, цілісності або доступності інформації. Об'єктами в цьому контексті є критична інфраструктура та інформаційні системи, що мають важливе значення для функціонування держави та суспільства.

Забезпечення конфіденційності, цілісності та доступності (КЦД) на об’єктах критичної інфраструктури є однією з ключових завдань у сфері кіберзахисту. Для цього необхідно вжити ряд заходів, що спрямовані на створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури (КІІ). Серед таких заходів можуть бути [4]:

– аналіз та визначення переліку інформаційних, програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури, оцінка їх критичності та потенційних наслідків у разі порушення КЦД;

– здійснення передачі даних через бездротові мережі лише захищеними з'єднаннями з метою забезпечення конфіденційності та цілісності інформації. Використання технологій Wi-Fi та Bluetooth на об’єктах критичної інформаційної інфраструктури забороняється;

– використання захищених з'єднань для захисту даних, що передаються між віддаленими користувачами, адміністраторами та об’єктом критичної інформаційної інфраструктури, а також між різними компонентами об’єкта та іншими (зовнішніми) інформаційно-технічними системами.

Забезпечення конфіденційності та безпеки інформації, що стосується конфліктів, є важливою складовою безпеки країни. Для цього розглянемо деякі методи та рішення, які можуть бути застосовані:

1. Перевірка на допуск та достовірність. Для забезпечення безпеки інформації держава може регулювати доступ до конфіденційної інформації, що стосується конфліктів. Це може включати видання дозволів на доступ до секретної інформації для ключових учасників, а також встановлення критеріїв для нових учасників, наприклад, на основі згоди існуючих учасників або вимагати перевірку відповідності з державними органами.

2. Системи класифікації. Для контролю за поширенням інформації використовуються системи класифікації, які вказують ступінь доступності. Наприклад, Протокол світлофора (TLP) має чотири кольори, які позначають рівень конфіденційності: червоний, бурштиновий, зелений та білий.

3. Використання електронних інструментів. Деякі платформи використовують електронні інструменти, наприклад, екстранет, для обміну даними між сторонами, які знаходяться на відстані. Ці інструменти дозволяють проводити обмін даними в безпечному середовищі, забезпечуючи аутентифікацію учасників та захист інформації.

Різноманітні країни використовують різні підходи до захисту конфіденційної інформації, що стосується конфліктів [5]:

– Австралія. Уряд Австралії у 2003 році створив довірену мережу обміну інформацією (TISN), яка є основним механізмом взаємодії між бізнесом і урядом. TISN забезпечує безпечне середовище для власників та операторів КВОІ, дозволяючи їм обмінюватися інформацією та співпрацювати для вирішення проблем безпеки та безперервності бізнесу. Крім того, існують спеціалізовані форуми та експертно-консультативна група, що допомагають вивчати складні питання та організовувати стабільність.

– Франція. В рамках національної системи забезпечення безпеки життєдіяльності (SAIV) приймаються директиви та плани, класифіковані за рівнями конфіденційного захисту. Оператори КВОІ мають забезпечити знищення секретних документів, які більше не потрібні, зокрема тоді, коли вони переглянуті, скасовані або втрачається їхній статус «життєво важливого оператора.

– Канада. Визначила своєю однією з головних мет цілісний обмін інформацією та захист між учасниками критично важливої інфраструктури (КВІ). Для досягнення цієї мети уряд Канади пропонує створення Інформаційного центру критично важливої інфраструктури (CI Gateway), який буде розміщений на платформі громадської безпеки Канади. Мета CI Gateway полягає в забезпеченні участі ключових секторів КВІ та інших зацікавлених сторін, стимулюючи їх до приєднання та сприяючи обміну інформацією та передовим практикам через галузеві мережі. На що стосується доступу до конфіденційної інформації для приватного сектора, то більшість інформації, зібраної у співтоваристві безпеки та розвідки, є конфіденційною та доступною лише особам із відповідним допуском.

Державна безпека Канади активно співпрацює з провідними федеральними департаментами та агентствами для залучення більшої кількості зацікавлених сторін із приватного сектора.

Один із ключових інструментів регулювання кібербезпеки в Європейському Союзі (ЄС) - Директива (ЄС) 2016/1148 Європарламенту та Ради від 6 липня 2016 року про заходи для встановлення високого загального рівня безпеки мереж та інформаційних систем в усій Союзі (NISD). Однак ця директива - лише один з інструментів регулювання кібербезпеки в ЄС, адже інші директиви та регламенти, такі як GDPR, також впливають на захист критичної інформаційної інфраструктури (КІІ).

Згідно зі статтею 5 NISD, держави-члени мають широкі можливості в управлінні відповідно до власних обставин. Вони можуть встановлювати ще більш жорсткі стандарти безпеки, ніж ті, що передбачені у директиві. Навіть в пункті 6 Преамбули NISD зазначається, що для операторів життєво важливих послуг та провайдерів цифрових послуг можуть бути застосовані ще більш суворі заходи захисту.

Різноманітні країни Європейського Союзу, такі як Німеччина та Великобританія, прийняли відповідні закони та стратегії для регулювання захисту критичної інфраструктури. Наприклад, в Німеччині це питання урегульоване Законом про забезпечення безпеки інформації (BSIG) та відповідним указом щодо класифікації критичної інфраструктури. Схожий підхід має і Великобританія, яка взяла на озброєння відповідний Статут № 506. Більшість країн ЄС також мають національні стратегії з кібербезпеки, в яких відводиться значна увага захисту критичної інфраструктури. У цих стратегіях передбачені заходи для забезпечення безпеки як найбільш важливих організацій і компаній, так і органів державної влади, які беруть активну участь у цьому процесі.

У 2015 році постійний комітет загальнокитайських зборів народних представників прийняв ряд законів, спрямованих на забезпечення національної безпеки та захист інформаційної інфраструктури. Закон про національну безпеку вперше визначив "захист національного суверенітету в кіберпросторі" як одну з

важливих складових національної безпеки, а також створив систему перевірки для розгляду питань, пов'язаних з інформаційною безпекою. Закон про боротьбу з тероризмом, що набрав чинності у 2017 році, встановив механізми для боротьби з терористичною діяльністю, зокрема, зобов'язав телекомунікаційні та Інтернет-підприємства співпрацювати з державними органами у розслідуванні терористичних подій.

Закон про кібербезпеку встановлює ряд вимог для мережевих операторів, зокрема, вимоги щодо багаторівневих систем безпеки, перевірки особи користувача, розробки планів реагування на надзвичайні ситуації та сприяння слідчим органам у розслідуванні злочинів. Цей закон також передбачає підвищені вимоги щодо захисту особистої інформації та іншої важливої інформації, зокрема, захищене зберігання даних та проходження перевірок безпеки для мережевих продуктів і послуг.

У травні 1998 року була введена в дію директива Президента США № 63, яка встановлювала стратегію спільних дій між урядом США та приватним сектором для захисту критичної інфраструктури. Ця стратегія передбачала вирішення завдань щодо захисту національної інфраструктури від потенційних загроз та атак.

Директива супроводжувалася двома адміністративними указами президента: №13130, що створив Національну раду з критичної інфраструктури, і №13231, що регулював захист національних критичних інформаційних систем.

Ці документи сприяли створенню центрів обміну інформацією та аналізу, а також Національної ради з критичної інфраструктури. У кінці 2001 року був створений Національний центр аналізу та імітаційного моделювання інфраструктури, а в листопаді 2002 року було утворено Міністерство внутрішньої безпеки США, якому було покладено координацію заходів забезпечення захисту національної інфраструктури від різних загроз.

У 2018 році в Україні був прийнятий Закон «Про основні засади забезпечення кібербезпеки України», який встановлює основні принципи та правові засади забезпечення кібербезпеки. Закон визначає об'єкти критичної

інфраструктури, такі як підприємства та установи в енергетичній, хімічній, транспортній, ІКТ, банківській та фінансовій сферах.

Міністерство економічного розвитку та торгівлі розробило проект закону «Про захист критичної інформаційної інфраструктури», який передбачає визначення основних принципів державної політики в цій сфері, регулювання правових та господарських відносин, а також повноваження органів управління. Зокрема, Адміністрація Держспецзв'язку матиме повноваження формувати та реалізовувати державну політику щодо захисту критичної технологічної інформації, контролювати та поновлювати перелік об'єктів критичної інфраструктури та забезпечувати їх актуалізацію.

Також було опубліковано «Порядок віднесення об'єктів до об'єктів критичної інфраструктури», який регламентує механізм внесення об'єктів до державного реєстру, та Методику категоризації об'єктів критичної інфраструктури, що визначає критерії для віднесення об'єктів до різних категорій критичності.

3 ЗАХИСТ ІНФОРМАЦІЇ В КОНТЕКСТІ ТЕХНОЛОГІЇ VOICE OVER INTERNET PROTOCOL

3.1 Принципи технології голосового передачі через Інтернет VoIP та використання IP-телефонії

Перспективи телефонії варто розглядати з двох позицій: для користувача це доступна послуга, для оператора – це технологічний аспект надання цієї послуги. Основна мета телефонії - забезпечити надійний голосовий зв'язок між віддаленими абонентами з мінімальною затримкою. Якість голосової передачі повинна бути максимально наближена до реального спілкування лице до лиця. Голосовий сигнал передається за допомогою сучасних електронних засобів.

Ще однією важливою функцією телефонії є передача та обробка службової інформації або сигналізація. Для здійснення дзвінка до співрозмовника потрібно ввести його номер на телефоні. Обробка цього номера визначає маршрут передачі голосової інформації від одного абонента до іншого. Під час цього процесу звучить дзвінок на телефоні співрозмовника, а особа, що здійснює дзвінок, отримує інформацію про стан з'єднання (наприклад, зайнято чи недоступно). Типовий сценарій телефонної розмови відтворено на рис.3.1. Перший успішний випадок використання телефонії полягав у передачі голосу на великі відстані. У перших поколіннях телефонних систем голос людини перетворювався на електричний сигнал за допомогою мікрофону.

Рисунок 3.1 – Процес телефонного спілкування у традиційній телефонній системі

Для забезпечення безвтратної передачі електричного сигналу через дроти на великі відстані використовувалися електричні підсилювачі. На завершення передачі електричний сигнал перетворювався у звуковий за допомогою акустичного динаміка рис.3.2.

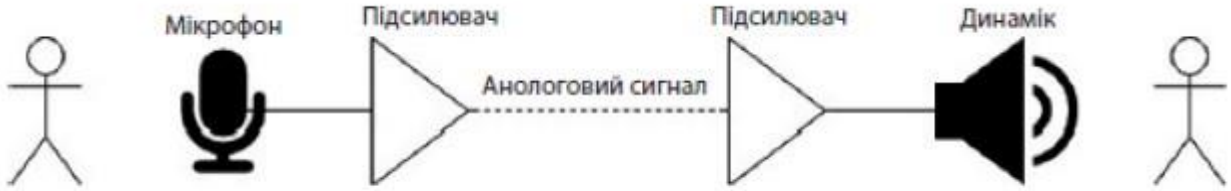

Рисунок 3.2 – Голосова комунікація через аналоговий електричний канал

Протягом розвитку технології телефонії, мікрофон та динамік залишалися сталими компонентами, не зазнаючи принципових змін. Проте інші елементи системи піддавались постійним вдосконаленням. Сигнал, що передавався через мережу, спочатку був аналоговим, і змінювався в залежності від сили акустичного тиску, генерованого голосом. Така технологія отримала назву "аналогова телефонія". На великі відстані якість передачі голосу погіршувалася через шуми та спотворення, а також через втрату сигналу від проміжних підсилювачів.

Проблему вирішено за допомогою переходу до цифрового коду для передачі голосу рис.3.3 [8]. Голосовий сигнал перетворюється у цифровий код через аналогово-цифровий перетворювач (АЦП), а потім зворотно у звук через цифро-аналоговий перетворювач (ЦАП). Цифровий зв'язок значно покращив якість передачі голосу, оскільки цифровий сигнал не піддається впливу шумів та спотворень, які характерні для аналогових мереж. Сьогодні цифровий зв'язок переважає, замінюючи застарілі аналогові системи.

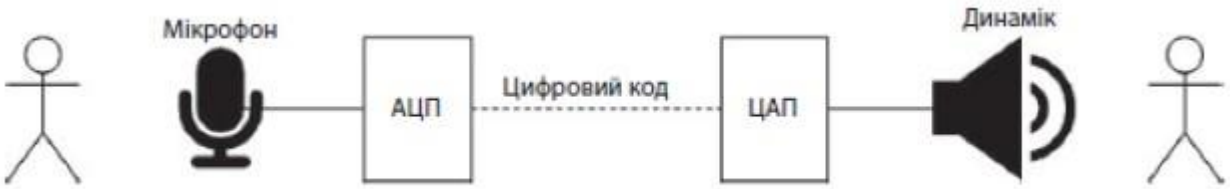

Рисунок 3.3 – Голосова комунікація з використанням цифрової технології передачі сигналу

Для забезпечення зв'язку між багатьма абонентами у телефонній мережі використовується комутація, що дозволяє операторові створювати шлях передачі голосу між абонентами, об'єднуючи ділянки мережі у єдиний канал. У цифровій формі голосовий сигнал передається як послідовність цифрових відліків замість неперервного аналогового сигналу. Ця технологія, відома як часове мультиплексування (TDM), рис. 3.4 дозволяє передавати декілька розмов через один канал, оптимізуючи використання ресурсів мережі.

На сьогоднішній день для базового формату TDM існують два стандарти: T1 та E1. У стандарті T1 один канал передає відліки 23 телефонних розмов та службову інформацію, тоді як у стандарті E1 ця кількість становить 30 телефонних розмов та службова інформація. T1 широко використовується в США та Японії, тоді як E1 популярний в Європі. Кожен проміжок часу, в якому передається відлік однієї телефонної розмови, відомий як часовий слот (time slot). У стандарті T1 доступно 24 часових слотів (з урахуванням передачі службової інформації), а в стандарті E1 - 30 часових слотів. Система стандартів Synchronous

Digital Hierarchy/Synchronous Optical Network (SDH/SONET) регламентує багаторівневе часове ущільнення в технології TDM [8].

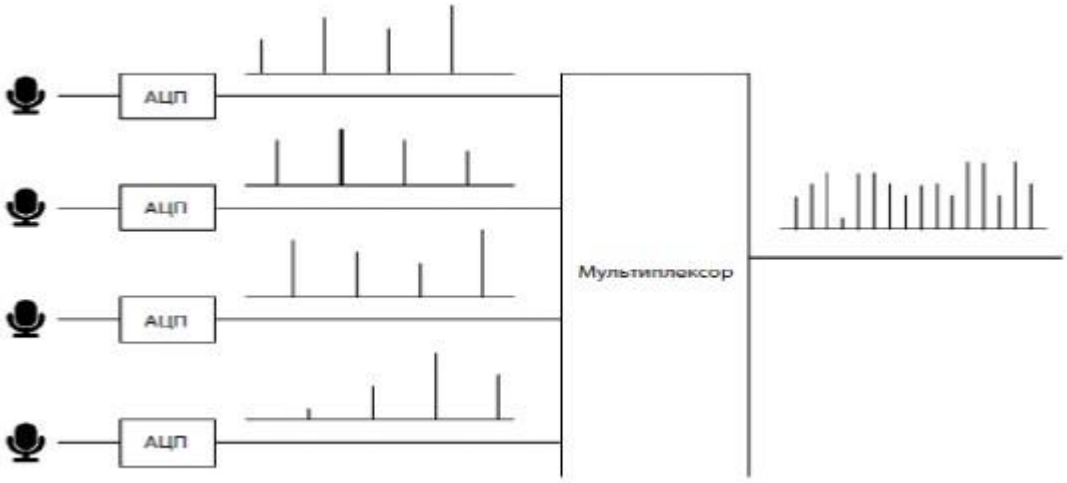

Рисунок 3.4 – Оптимізована передача голосових даних за допомогою технології TDM

Технологія голосової передачі по мережах IP, відома як Voice-over-IP (VoIP), є ключовою складовою сучасних IP-телефонних систем. Окрім голосової передачі, IP-телефонія включає також сигналізаційні функції.

IP-телефонія, що ґрунтується на технології VoIP, швидко стала популярною завдяки ряду переваг у порівнянні з традиційною телефонією:

– ефективне використання ресурсів мережі: передача голосу через IP-пакети дозволяє оптимізувати використання каналів зв'язку та обладнання без потреби у спеціальному резервуванні ресурсів;

– зниження вартості міжнародних дзвінків: відміна резервування ресурсів на дорогих проміжних TDM-комутаторах дозволяє перейти до сплати за підключення до Інтернету, що зменшує витрати на дзвінки на великі відстані;

– єдина технологічна база: IP-телефонія дозволяє використовувати однакові комутатори, маршрутизатори та сервери для обробки як голосових, так і даних;

– розширені можливості для користувачів: інтеграція телефонії та Інтернету відкриває широкий спектр нових сервісів та додаткових послуг для абонентів.

Проте важливо зауважити, що IP-телефонія не виключає традиційну телефонію. На сьогодні обидві технології існують паралельно в різних мережах. Інтеграція різних типів телефонних мереж здійснюється за допомогою транкових голосових шлюзів, які встановлюються на межах цих мереж рис.3.5.

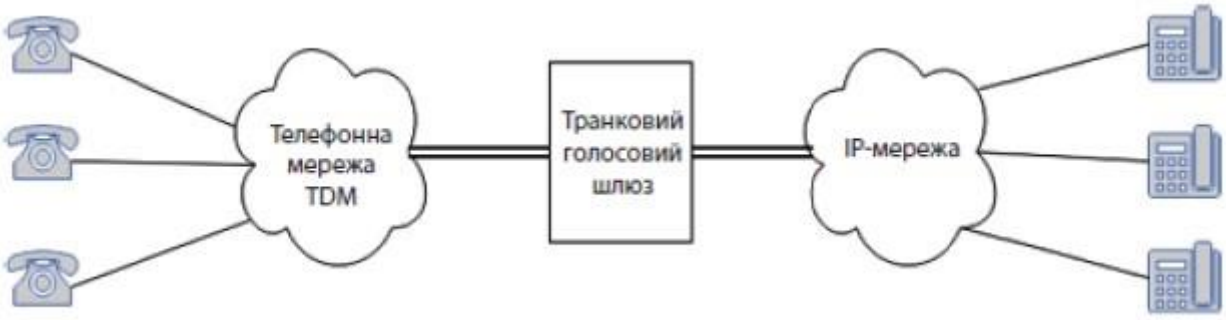

Рисунок 3.5 – Взаємодія мереж традиційної телефонії та IP-телефонії

Процес цифрової передачі голосу в системах IP-телефонії включає перетворення початкового аналогового сигналу у цифровий формат, що представляє собою послідовність цифрових відліків, які передаються в IP-пакетах. Цей процес складається з трьох етапів: дискретизація, кодування та компресія динамічного діапазону.

Дискретизація означає фіксацію точок у аналоговому сигналі, які будуть представлені цифровими відліками для подальшої передачі. Щоб точно відтворити сигнал з цих відліків, дискретизація має проводитися достатньо щільно. Згідно теорії дискретизації сигналів, розробленої, зокрема, американським вченим Гаррі Найквістом та російським вченим В.О. Котельниковим, для збереження повної інформації про сигнал необхідно фіксувати відліки з частотою, яка не менша вдвічі, ніж верхня частота спектру сигналу. Частотний спектр голосу людини зазвичай знаходиться у діапазоні від 300 Гц до 3,5 кГц, тому частота дискретизації повинна бути не менша за 7 кГц.

У цифровій телефонії та VoIP використовується частота дискретизації 8 кГц, що означає фіксацію 8000 відліків кожної секунди [8].

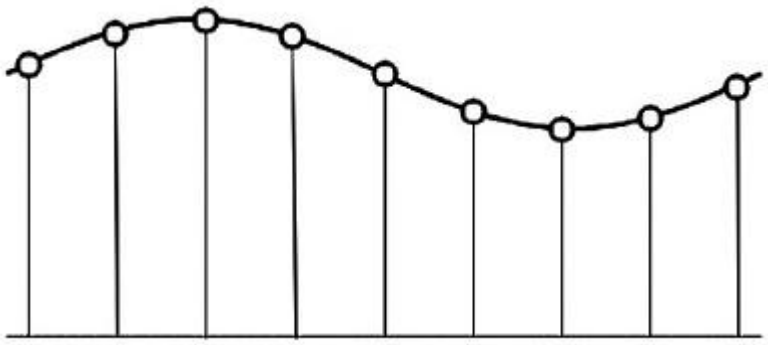

Рисунок 3.6 – Процес перетворення аналогового сигналу у цифрову форму

В побутовій техніці зазвичай відтворюються звукові сигнали, які мають спектр відбиття приблизно від 20 Гц до 20 кГц. З цієї причини стандартна частота дискретизації для запису цифрових аудіодисків складає 44,1 кГц.

Кодування полягає у визначенні цифрового коду для кожного відліку сигналу. Оскільки кожна система обчислення має обмежену точність через кінцеву кількість розрядів числа, значення сигналу у відліках, отриманих під час дискретизації, округлюються до найближчого значення, яке може бути представлене в даній системі обчислення. Цей процес називається квантуванням рис.3.7.

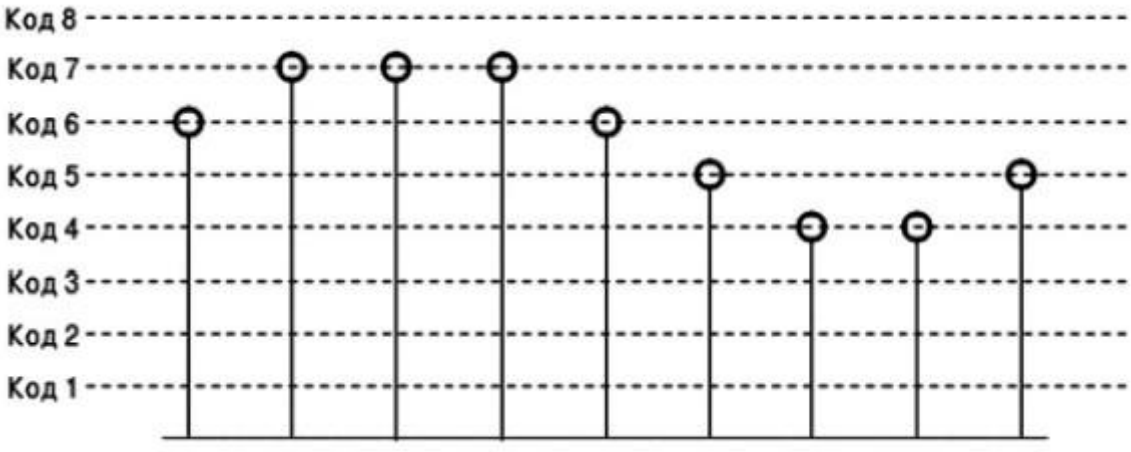

Рисунок 3.7 – Процес присвоєння цифрового коду кожному відліку

Для покращення якості кодування відліків потрібно використовувати більшу кількість розрядів. Наприклад, на цифрових аудіодисках відліки зазвичай

кодуються за допомогою 16-бітних двійкових кодів. У телефонії для кодування голосу часто використовуються 8-бітні коди.

Компресія динамічного діапазону використовує нелінійну функцію кодування відліків. Замість лінійної функції, де кожне значення відповідає однаковому рівню кодування, застосовується нелінійна функція, яка ефективно використовує сітку можливих значень кодів. Оскільки більшість сигналів знаходиться в середньому діапазоні, а сплески менш часті, ця стратегія зберігає більше інформації про сигнал.

Використання рівномірної сітки значень кодів при лінійній функції кодування призводить до надмірного використання значень для кодування сплесків сигналу.

Ефективніше кодування можливе за допомогою нелінійної функції кодування, де для середнього діапазону сигналу використовується більш щільна сітка значень, ніж для сплесків. Це дозволяє оптимізувати використання значень кодів.

Динамічний діапазон, що визначається як різниця між максимальним та мінімальним рівнями сигналу, може бути стиснутий за допомогою нелінійної функції кодування. Ця стратегія відома як компресія (стискання) динамічного діапазону сигналу. Сьогодні використовуються дві стандартні нелінійні функції кодування відомі як a-law, що популярна в Європі, та μ-law, що застосовується в США та Японії.

Цифрове перетворення аналогового сигналу, відоме як імпульсно-кодова модуляція (PCM), є ключовою процедурою у звуковій технології. У форматі PCM аналоговий сигнал представляється у вигляді 8-бітових цифрових кодів, які передаються з частотою 8000 за секунду.

Під час відтворення голосу отримані цифрові коди піддаються зворотному процесу цифро-аналогового перетворення. Ця процедура включає відновлення динамічного діапазону, формування рівнів сигналу та згладжування для отримання аналогового сигналу з дискретних відліків.

Для зниження обсягу даних використовуються кодеки, які проводять стиснення голосових даних. Це дозволяє зменшити потрібну пропускну здатність для передачі даних. На боці отримувача здійснюється зворотний процес, під час якого стиснуті дані відновлюються до початкових відліків, які потім використовуються для відтворення голосового сигналу.

Термін «кодек» походить від слів «кодування» та «декодування» і використовується для опису набору функцій, які забезпечують зменшення обсягу голосових даних, що передаються, шляхом кодування та декодування цих даних на різних кінцях передачі.

Існує широкий спектр кодеків, які відрізняються за рівнем стиснення даних, складністю обробки, впливом на якість сигналу та оптимальними умовами використання. Деякі з них мають стандартний статус і описані в документах Міжнародного Телекомунікаційного Союзу (ITU), що позначені кодами виду G.7xx (наприклад, G.711, G.726, G.729 та інші). Також існують пропрієтарні кодеки, які потребують використання обладнання певного виробника на обох кінцях передачі голосових даних. У табл. 3.1 наведені характеристики деяких поширених кодеків [13].

При передачі голосу через мережі VoIP важно враховувати, що окрім цифрових відліків передається також службова інформація, яка включає заголовки IP-пакетів і фреймів канального рівня. Для оцінки потрібної пропускної здатності мережі необхідно враховувати не лише значення, вказані в табл. 3.1, але й додаткову пропускну здатність для передачі цієї службової інформації.

Наприклад, можемо розглянути розрахунок потрібної пропускної здатності Ethernet мережі для передачі однієї голосової розмови з використанням кодеку G.711 [8].

Таблиція 3.1 – Кодеки

Кодек	Потрібна пропускна здатність. Кбіт/с	Якість передачі голосу за 5-бальною шкалою	Типове використання
G.726r32	32,0	3,8	Передача розмов
G.736r24	24,0	3,75	Передача розмов
G.726r16	16,0	3.7	Передача розмов
G.728	16,0	3,75	Передача розмов
iLBC	13,3 або 15,2	4,14	Використання в мережах з нестабільною якістю передачі пакетів
GSM Full Rate	13,0	3,5	Голосові меню, голосова пошта
G.729a	8,0	3.7	Передача розмов
G.723r63	6,3	3.7	Передача голосу та мультимедіа
G.723r53	5,3	3,65	Передача голосу та мультимедіа
G.722	64,0	4,5	Передача сигналу ширшого спектру – до 7кГц, та кращої якості кодування - 14 біт на відлік
G.722.1	32,0 або 24,0	4,09	Передача сигналу ширшого спектру – до 7кГц, та кращої якості кодування - 14 біт на відлік
G.722.2	16,0	3,98	Системи сумісного передачі голосу і файлів зі змінними умовами щодо швидкості передачі даних

Умови передачі:

– часовий інтервал фрагменту голосової розмови, що передається одним пакетом IP (визначає затримку голосового сигналу) – 20 мілісекунд;

– розмір заголовка контейнера протоколу RTP (Real-time Transport Protocol) - 12 байт;

– розмір заголовка датаграми UDP (User Datagram Protocol) – 8 байт;

– розмір заголовка пакета IP - 20 байт;

– розмір заголовка та контрольної інформації Ethernet-фрейму – 18 байт.

Фрагмент голосової розмови тривалістю 20 мілісекунд потребує 160 відліків, що відповідає 160 байтам голосових даних. Після додавання накладних витрат протоколів RTP, UDP, IP та Ethernet-фреймів отримуємо загальний розмір пакета - 218 байт.

Передача фрагментів кожні 20 мілісекунд вимагає їх відправки з частотою 1 / 0.02 = 50 пакетів на секунду. Таким чином, передача 50 пакетів розміром 218 байт на секунду потребує пропускної здатності мережі 10900 байт/с або 87.2 Кбіт/с.

Як можна помітити, реальна потреба в пропускній здатності (87,2 Кбіт/с) перевищує швидкість, необхідну для передачі лише голосових даних (64 Кбіт/с) на 36%. Це пояснюється тим, що крім голосових даних також передаються пакети з додатковою інформацією через протокол RTCP (Real-Time Control Protocol), яка, однак, має невеликий внесок в загальну пропускну здатність мережі.

При використанні кодеків з високим ступенем стиснення голосових даних, таких як G.729a, який передає голос із швидкістю 8 Кбіт/с, накладні витрати стають ще вищими. Наприклад, для фрагменту тривалістю 20 мс пропускна здатність складе 31,2 Кбіт/с, що відповідає зростанню накладних витрат на 290%. Якщо тривалість фрагменту збільшити до 30 мс, пропускна здатність зменшиться до 23,5 Кбіт/с, що все ще становить 193% від необхідної пропускної здатності. Незважаючи на це, в порівнянні з кодеком G.711, який використовується для передачі голосових даних з швидкістю 64 Кбіт/с, економія все одно залишається значною – 23,5 Кбіт/с проти 87,2 Кбіт/с для кожного голосового з'єднання.

Важливо враховувати, що для ефективної комунікації між абонентами важливо, щоб їхні пристрої підтримували однакові кодеки. Відсутність відповідності кодеків вимагає перетворення між ними під час передачі голосових даних. Ця процедура може збільшити затримку сигналу і погіршити його якість. Зазвичай у телефонних мережах встановлюється єдиний базовий кодек для всіх розмов, що полегшує взаємодію. У випадку зв'язку між абонентами різних мереж із різними кодеками необхідно забезпечити підтримку обох кодеків кінцевими

пристроями абонентів або виконати конвертацію кодеків на межі мережі. Для передачі голосу через мережевий протокол IP між VoIP-шлюзами абонентів використовуються раніше згадані протоколи RTP та RTCP.

Індустріальний стандарт ITU H.323 став першим широко використовуваним протоколом службової сигналізації. Початково розроблений для відеоконференцій в IP-мережах, протокол H.323 швидко став основою для всіх типових сценаріїв IP-телефонії. Його гнучкість дозволяла використовувати його як у мережах з виділеними контролерами зон, так і в універсальних шлюзах, що поєднували функції передачі голосу та сигналізації.

У порівнянні з H.323, MGCP та H.248, які працюють з централізованими елементами керування, протокол ініціювання сеансів зв'язку (SIP) призначений для симетричної взаємодії рівноправних пристроїв. У простіших випадках SIP може забезпечувати взаємодію між двома кінцевими пристроями, наприклад, голосовими шлюзами, без додаткових елементів керування. Також, за відміну від MGCP, SIP дозволяє більшу інтелектуальну взаємодію між кінцевими пристроями та може керувати передачею викликів через багато проміжних пристрої.

Порівняно з протоколом H.323, який також здатен підтримувати симетричну взаємодію, SIP пропонує додаткові можливості:

– знаходження фактичного місця підключення (реєстрації) користувача в телефонній мережі, що дозволяє підтримувати мобільних користувачів;

– обмін інформацією щодо підтримуваних функцій між пристроями, які беруть участь у сеансі зв'язку, що забезпечує ефективну взаємодію між пристроями різних виробників та узгоджене впровадження підтримки нових функцій;

– визначення готовності абонента, якого викликають, до початку сеансу взаємодії;

– можливість динамічної зміни параметрів виклику під час сеансу взаємодії, наприклад, додавання та вилучення учасників.

SIP володіє спрощеною системою службових повідомлень у порівнянні з H.323. Ці повідомлення передаються у вигляді простого тексту, аналогічно до

протоколу передачі гіпертексту HTTP. В якості транспортного протоколу часто використовується UDP, що має менше накладних витрат порівняно з TCP.

Основними компонентами мережі на основі SIP є такі (рис. 3.8) [12]:

– Агент користувача (User Agent) – це модуль, що інтерактивно працює з агентами користувача інших пристроїв. Він може виступати як клієнт, що ініціює взаємодію, або сервер, що відповідає на запити.

– Сервер реєстрації (Registrar) – це компонент, який зберігає інформацію про доступні агенти користувача в мережі і надає можливість їхнього пошуку.

– Проксі-сервер (Proxy Server) – це посередник на шляху передачі виклику, який маршрутизує його і виконує різноманітні технологічні та безпекові функції.

– Сервер переадресації (Redirect Server) – це агент користувача, що вказує на необхідність перенаправлення запиту до іншого агента користувача, наприклад, в іншій мережі.

– Прикордонний контролер сеансів зв'язку (Session Border Controller або SBC) – це посередник, який розташовується на межі мереж з різним адміністративним керуванням і відповідає за безпеку, анонімізацію топології мережі та інші технологічні функції.

Рисунок 3.8 – Компоненти інфраструктури мережі, що базується на протоколі SIP

3.2 Аналіз ризику нелегітимного доступу до безпечної IP-телефонії

Оцінка загроз нелегітимного доступу до безпечної IP-телефонії. Аналіз ймовірності успішної атаки нелегітимним користувачем.

Рівень потенційних загроз для інформаційної безпеки враховується через модель нелегітимного користувача. Розглянемо таку модель, де нелегітимні користувачі, такі як сторонні особи, представники іноземних держав, агенти розвідувальних служб або злочинні організації, не мають відповідного доступу до послуг IP-телефонії."

Для аналізу моделі нелегітимного користувача ми спробуємо з'ясувати їхні цілі та мотивацію. Сформулюємо декілька потенційних цілей, які можуть переслідувати такі користувачі, проводячи атаки для отримання несанкціонованого доступу до даних IP-телефонії. Зокрема, ми визначимо Ціль_О (отримання доступу до обладнання оператора) та Ціль_М (отримання доступу до моніторингу абонентів). Усі цілі спрямовані на незаконне отримання доступу до потоку даних IP-телефонії."

Після аналізу алгоритмів, які можуть бути використані нелегітимними користувачами, ми розробимо модель порушника інформаційної безпеки для кожної з вищезазначених цілей."

Давайте розглянемо сценарій захоплення обладнання оператора нелегітимним користувачем. Цей користувач працює над активними атаками з метою отримання несанкціонованого доступу до даних IP-телефонії. Успішний результат такої атаки означатиме захоплення обладнання оператора.

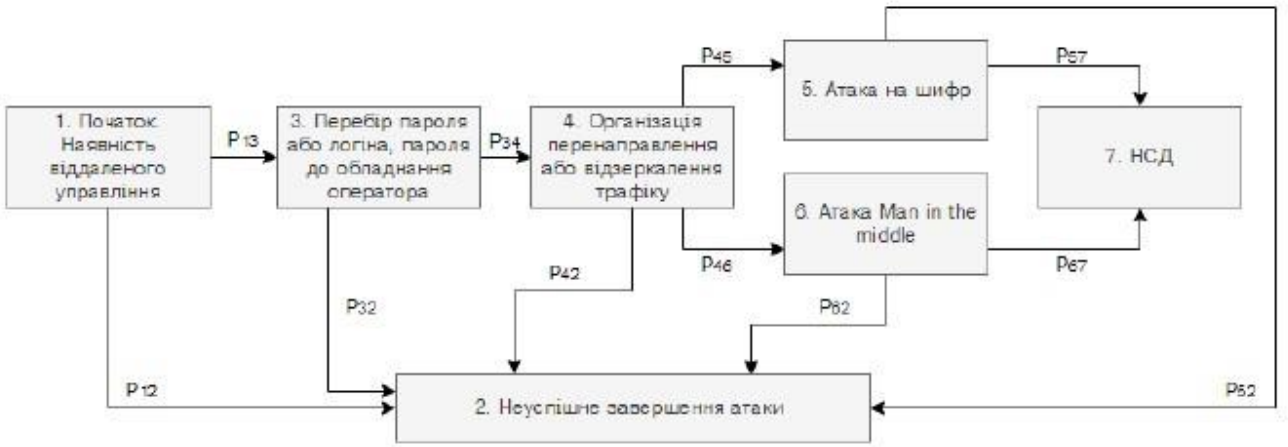

Рисунок 3.9 – Можливий сценарій дій нелегітимного користувача під час атаки на обладнання оператора з метою захоплення контролю

Сценарій дій нелегітимного користувача відображено на рис. 3.9. Для ініціювання атаки, зловмиснику потрібно спочатку визначити, на який саме сервіс IP-телефонії він планує здійснити активну атаку. Один з можливих методів - використання команди tracert для отримання інформації про проміжні вузли між об’єктом атаки та самим зловмисником. Ця інформація дозволить зловмиснику виявити вузли, які беруть участь у поточному обміні даними між абонентами.

Після вибору сервісу IP-телефонії зловмиснику слід спробувати отримати контроль над цим сервісом. Один з методів цього може включати активну атаку, таку як перебір паролю. Однак за наявності списків доступу (ACL) у оператора, віддалене управління може бути технічно недоступним для зловмисника. Ймовірність проведення активної атаки на сервіси IP-телефонії при наявності ACL в оператора визначається як p12, а ймовірність наявності віддаленого підключення до сервісів IP-телефонії визначається як p13, що є оберненою подією до p12 [7].

Для виконання активної атаки віддаленого управління сервісами IP-телефонії, зловмиснику слід вибрати доступний протокол (наприклад, telnet, http або https, ssh, SNMP) для атак типу «перебір пароля». Для визначення ймовірності успішного завершення атаки «перебір пароля» за певний час, необхідно розрахувати формулу:

$$p34\text{зх\_о} = Func(L, T, D, C), \quad (3.1)$$

де L – кількість символів у логіні чи паролі;

T – час, що був відведений для успішного завершення атаки, тобто для перебору пароля;

D – механізми, програмно-апаратні та технічні можливості порушника, а також обмеження IP-протоколу, які ускладнюють або унеможливлюють успішне завершення атаки "перебір пароля" за відведений час;

C – швидкість каналу зв'язку Інтернет мережі, при виконанні атаки зловмисником;

$p34\text{зх\_о}$ – ймовірність успішного завершення активної атаки "перебір пароля" і надання нелегітимному користувачеві доступу до обладнання оператора;

$p32$ – ймовірність того, що атака "перебір пароля" завершилася неуспішно протягом відведеного для неї часу.

Несанкціонований доступ до потоку даних IP-телефонії може бути отриманий зловмисником, якщо він успішно захопить віддалене управління сервісами. Це може статися через один із наступних способів:

1) здійснення атаки "перебір пароля" для доступу до медіатрафіку, що передається через Інтернет, та прослуховування цього трафіку;

2) атака на механізм програмного розмоділу загальної секретної інформації, наприклад, ключів, для отримання можливості дешифрування трафіку.

Однак успішність таких атак може не завжди привести зловмисника до його основної мети. Якщо він не може виконати атаку "Зустріч по середині" і налаштувати обладнання оператора для пропуску трафіку через своє обладнання, то ці атаки можуть виявитися малоефективними.

Для визначення ймовірності успішної атаки нелегітимним користувачем на медіа-трафік з метою отримання несанкціонованого доступу до потоку даних (для атаки "зустріч по середині" або організації проксінгу) можна скористатися наступною формулою:

$$1 - p42\text{зх}_0 = \begin{cases} 1 \\ 0 \end{cases} \quad (3.2)$$

Активна атака з боку несанкціонованого користувача включає у себе втручання у маршрутизацію потоку даних, що передаються у вигляді пакетів мультимедійних файлів. Це дозволяє зловмиснику перенаправляти трафік через своє обладнання.

Під час такої атаки враховуються наступні ймовірності:

– p45 – ймовірність того, що несанкціонований користувач розпочне процес підбору пароля до переданого медіатрафіку;

– p46 – ймовірність того, що несанкціонований користувач виконає атаку на механізм програмного розподілу секретних ключів у IP-телефонії.

Імовірність p57 – успішна атака «підбір пароля» несанкціонованого користувача до переданого медіатрафіку. Підступник отримує змогу перехоплювати потік даних IP-телефонії або атакувати механізм програмного розподілу секретних ключів, що дозволяє йому розшифрувати трафік за допомогою цих ключів.

Імовірність p52 – спроба атаки на пароль, проведена над переданим через Інтернет медіа-трафіком, завершилася невдачею. Час збереження актуальності даних (Тзб_акт) визначається призначенням цих даних. Час, необхідний для успішного підбору пароля (Тпд), залежить від технічних можливостей та ресурсів, які доступні атакуючому, включаючи потужність обладнання (Рот), застосовані криптографічні методи (Ркрипт), довжину ключа (Рдовж), а також додаткові заходи ускладнення, такі як використання додаткових лічильників і т.п. (Рдодат).

$$p57 = Func(T\text{злв\_акт}, T\text{злв\_прл}) =$$
$$= Func(T\text{злв\_акт}, \text{ЗЛВпотуж}, \text{ЗЛВкрипт}, \text{ЗЛВдовж}, \text{ЗЛВптж}) \quad (3.3)$$

$$p52 = 1 - p57 \quad (3.4)$$

Імовірність p67 відображає ймовірність успішної атаки на механізм програмного розподілу секретних ключів, а також дешифрації трафіку з використанням отриманої секретної інформації через механізм розподілу ключів. У випадку, коли зловмисник втручається в канал зв’язку під час обміну секретною інформацією між користувачами IP-телефонії, ця ситуація розглядається як атака. Нелегітимний абонент має можливість створити по два секретних ключа для обміну інформацією з кожним абонентом незалежно один від одного. Використовуючи цю секретну інформацію, зловмисник може шифрувати та дешифрувати потік даних, включаючи мультимедійні дані під час розмови двох користувачів IP-телефонії. Ймовірність успішної атаки "зустріч по середині" на протокол розподілу секретної інформації між користувачами IP-телефонії залежить від потужності технічних та програмних засобів, що використовуються зловмисником.

Необхідно врахувати, що для проведення активної атаки зловмисник мусить розробити відповідне програмне забезпечення. Імовірність p62 визначається як ймовірність неуспішної атаки типу «зустріч по середині», що здійснюється нелегітимним абонентом:

$$p62 = 1 - p67 \tag{3.5}$$

На рис. 3.3 наведено імовірнісний граф, який ілюструє можливий алгоритм дій зловмисника під час атаки типу «зустріч по середині». Для аналізу цього алгоритму використовується математичний апарат теорії імовірнісних графів. Він допомагає отримати інформацію, що сприяє оцінці часу, необхідного для успішного завершення атаки, а також ймовірності її успішності. Імовірнісний граф у цьому випадку допомагає отримати утворюючу функцію і розв'язати задачу переходу системи від початкового стану до кінцевого. Кожна гілка графа відповідає певній утворюючій функції.

Після аналізу можливих дій зловмисника отримано результат, який дозволяє оцінити ймовірність отримання несанкціонованого доступу до конфіденційної

інформації. Відповідний граф представлено на рис. 3.10. У цьому графі для гілки, що відповідає успішному виконанню атаки з метою отримання несанкціонованого доступу до потоку даних IP-телефонії, складено утворюючу функцію H(x). Для імовірнісного графа, показаного на рис. 3.2, представлено Рнсд = H(x=1).

$$P\text{нсдц} = p13p34(p45p57 + p46p67), \quad (3.6)$$

де *Pij* – ймовірність переходу з вершини *i* графу в вершину *j*.

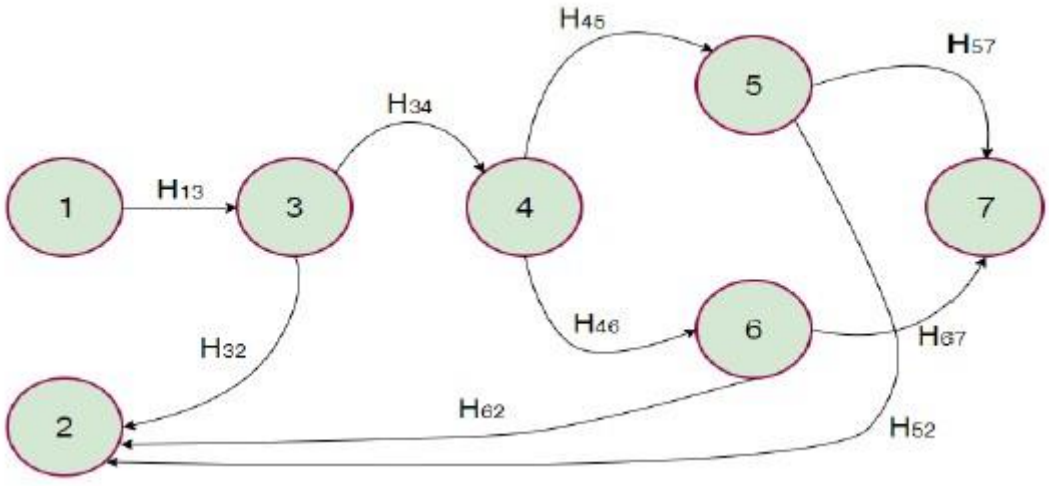

Рисунок 3.10 – Граф імовірностей дій під час атаки на захоплення обладнання оператора, яку виконує незаконний користувач

Алгоритм можливих дій зловмисника під час цієї атаки відображений на рис. 3.11. Результати аналізу дозволили докладніше розглянути різновиди атак, які може здійснити нелегітимний абонент, залежно від того, чи має він доступ до шлюзу чи персонального комп'ютера користувача. Якщо зловмисник має доступ до шлюзу, найбільш ймовірним є здійснення активної атаки з проксінгом всього трафіку за допомогою обладнання зловмисника. Ця атака виконується за схемою, показаною на рис. 3.12. На цій схемі зображені IP1 та IP2, що є шлюзами користувача, а SH є сервером зловмисника, де встановлено спеціалізоване програмне забезпечення.

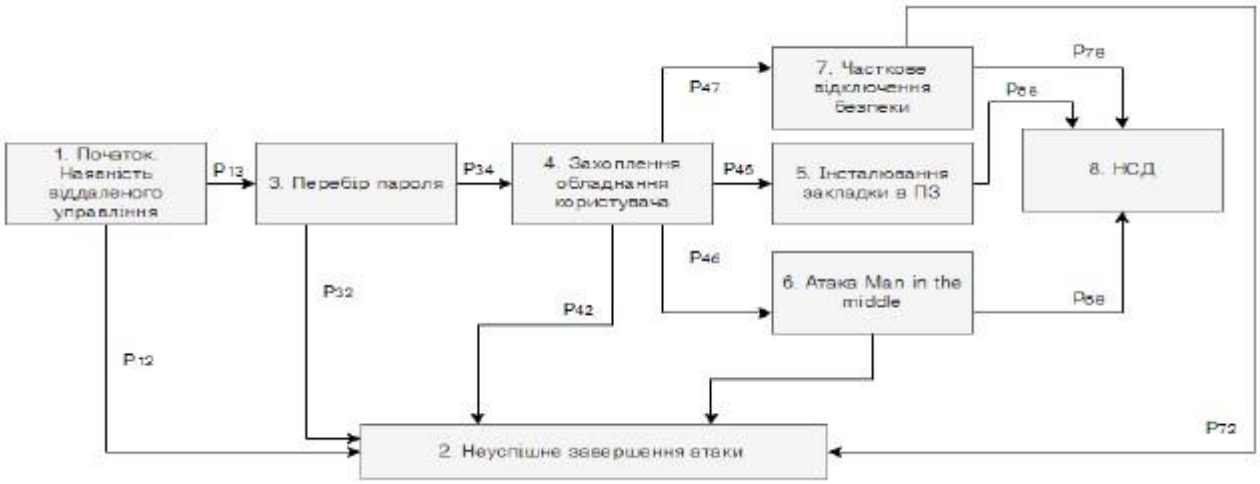

Рисунок 3.11 – Сценарій можливих дій у випадку атаки на захоплення монітора користувача зловмисником

Для вдалого завершення цієї атаки, зловмиснику спочатку потрібно отримати доступ до монітора користувача та отримати контроль над управлінням VoIP монітором. Після цього необхідно встановити та налаштувати відповідне спеціалізоване програмне забезпечення.

Рисунок 3.12 – Під час атаки на захоплення монітора, варіанти використання проксінгу включають: а) передача загальної секретної інформації та б) налагодження захищеного каналу для голосової комунікації

Якщо зловмисник використовує VoIP монітор з програмним шлюзом IP-телефонії, найбільш імовірним варіантом активної атаки є наступне:

Зловмисник може здійснити атаку з проксінгом, перенаправляючи потік медіа-трафіку користувачів через свій сервер, позначений як SH. Використовуючи

цю атаку, зловмисник може встановити спеціалізоване програмне забезпечення на VoIP моніторі, що дозволить передавати голосову інформацію у відкритому вигляді з монітора або перехоплювати пакети з мережевого інтерфейсу IP-телефонії. Ці дані потім будуть відправлені на сервер зловмисника для подальшої маніпуляції. Для цього зловмиснику потрібно вимкнути на VoIP моніторі IP-протоколи безпеки або змінити налаштування протокола IP-телефонії SRTP, а також відключити опцію шифрування голосової інформації.

Це показує, що успішність атаки залежить від кількох факторів, включаючи рівень захисту IP-телефонії та потужність спеціалізованого програмного забезпечення та методів взлому, використаних зловмисником. Ймовірність успішної атаки можна представити як наступне: Р34зм_м = [1, 0], де 1 вказує на наявність віддаленого управління на терміналі користувача без налаштованого списку ACL на всі віддалені протоколи, а 0 вказує на включене віддалене управління з налаштованими списками ACL на всі віддалені протоколи або на відсутність віддаленого управління взагалі. Якщо віддалене управління доступне, зловмиснику потрібно використовувати спеціалізоване ПЗ для підбору логіну/пароля для доступу на монітор користувача VoIP. Імовірність успіху такої атаки залежить від рівня захисту IP-телефонії та методів взлому, використаних зловмисником визачається за формулою:

$$p42\text{зах\_м} = Func(L, T, D, C) \tag{3.7}$$

де L – кількість символів у логіні/паролі;

T – максимальний час, який зловмисник може витратити на перебір для успішної атаки;

D – додаткові заходи та засоби, що ускладнюють атаку перебором пароля протягом виділеного часу, а також технічні можливості зловмисника;

C – швидкість передачі даних по каналу зв'язку Інтернету мережі IP-телефонії під час виконання атаки.

У разі успішного перехоплення пароля та отримання доступу до VoIP монітора користувача, зловмисник може незаконно звернутися до потоку даних IP-телефонії через один із двох методів: внедрення програмної вразливості в спеціалізоване ПЗ користувача або модифікація програмного забезпечення VoIP монітора; налаштування VoIP монітора користувача; проведення атаки типу "зустріч по середині" на всі протоколи безпеки IP-телефонії. Можливість успішної атаки залежить від рівня забезпечення технічними та програмними засобами зловмисника.

Перша атака дозволяє зловмиснику перехопити голосові дані, обходячи IP-протоколи або впливаючи на режим роботи або відключаючи їх. Друга атака дозволяє змінити налаштування VoIP монітора користувача для проведення атаки "зустріч по середині". Під час цієї атаки зловмисник по черзі підключається до кожного абонента, використовуючи IP-протоколи безпеки IP-телефонії. Дана схема зображена на рис. 3.13.

Рисунок 3.13 – Стратегія виконання атаки «зустріч по середині» на захищені протоколи IP-телефонії

При виборі будь-якої з перерахованих атак, зловмисник може мати можливість незаконно отримати доступ до потоку даних, якщо атака завершиться успішно. Проте існує ризик невдачі обраної атаки, який відображається ймовірностями p72 і p62 відповідно. Крім того, якщо користувач помітить зміни в налаштуваннях VoIP-монітора, змінить паролі доступу та відключить віддалене управління, відновивши налаштування, атака типу «модифікація налаштувань»

також буде неуспішною. Згідно аналізу можливих дій нелегітимного абонента, був побудований ймовірнісний граф, який зображено на рис. 3.14.

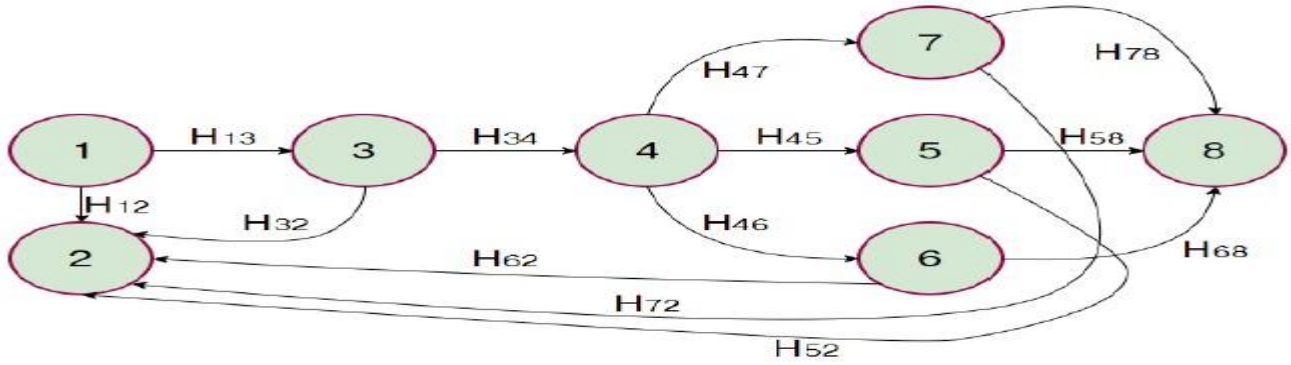

Рисунок 3.14 – Граф імовірностей можливих дій зловмисника під час здійснення атаки на захоплення VoIP-монітора

У цьому графі представлений шлях, що вказує на успішне завершення атаки для отримання несанкціонованого доступу до потоку даних. Для цієї гілки була розроблена функція H(x). Для графа імовірностей, показаного на рис. 3.14, ймовірність успішного завершення атаки позначається як Рнсд і обчислюється за значенням H(x=1):

$$Рнсдц(зх\_м) = p13p34(p45p58 + p46p68 + p47p78) \quad (3.8)$$

де *Pij* – ймовірність переходу з вершини *i* графа в вершину *j*.

Для аналізу ймовірносно-часових характеристик необхідно ретельно розглянути та оцінити протоколи, що використовуються для розподілу загальної секретної інформації (ключів) у захищеній IP-телефонії. Вони повинні відповідати певним вимогам, а саме:

– протокол має підтримувати різноманітні топології, такі як клієнт-сервер та клієнт-клієнт, у Інтернет-мережах IP-телефонії;

– протокол може функціонувати між абонентами без потреби у використанні додаткових IP-протоколів для розподілу загальної секретної інформації (ключів);

– протокол може працювати без передачі секретної інформації у відкритому вигляді по каналах зв'язку;

– протокол має вбудований механізм виявлення атак типу "зустріч по середині" без необхідності передплати секретних ключів між користувачами або використання сертифікатів;

– протокол використовує TCP/UDP порти, що визначені у стеку протоколів для IP-телефонії, такі як SIP/RTP, або інші порти, які встановлюються в результаті узгодження при підключенні.

Порівняння IP - протоколів по вище вказаним критеріям зображено в табл. 3.2.

Фінальну оцінку нашого аналізу кожного з протоколів визначимо за формулою:

$$Q_{\text{ПРК}}: Q_{\text{ПРК}} = \sum_{i=1}^{5} Ki \qquad (3.9)$$

Таблиця 3.2 – Співвідношення протоколів розподілу ключового матеріалу з вищезазначеними вимогами Кі

Вимоги до ПРК	Протоколи			
	SDES	MIKEY	DTLS	ZRTP
К1	0	1	1	1
К2	0	0	1	1
К3	0	1	1	1
К4	0	0	0	1
К5	1	1	1	1
QПРК	1	3	4	5

Протокол DTLS не відповідає вимозі К4, оскільки він призначений для роботи в топології клієнт-сервер і використовує сертифікати для захисту від атаки типу «зустріч по середині» для обох користувачів. У порівнянні з іншими протоколами, ZRTP має вбудований механізм SAS (Short Authentication String), спрямований на захист від атаки типу «зустріч по середині». Протоколи SDES і MIKEY не відповідають вимозі К4, а також MIKEY не відповідає вимозі К2. MIKEY може передавати повідомлення або у SIP/SDP-повідомленнях, або поверх RTSP (Real Time Streaming Protocol), але для цього останнього потрібна підтримка протоколу RTSP. Вимога К5 не виконується при роботі поверх протоколу RTSP, але виконується вимога К2. При роботі MIKEY поверх SIP/SDP-повідомлень вимога К5 виконується, але не виконується вимога К2. Протокол SDES не відповідає вимогам К1 та К3, оскільки ключ передається між абонентами у відкритому вигляді в повідомленнях SDP і потребує додаткового захисту (зазвичай використовується додатковий IP-протокол SISP). У випадку з’єднання клієнт-клієнт, коли у абонентів немає розподіленого загального секретного ключа, SDES не може організувати SIPS з'єднання з захистом від атаки типу «зустріч по середині». Крім того, протокол SDES не відповідає вимозі К2, оскільки використовуються повідомлення SIP/SDP для передавання даних протоколу SDES.

Враховуючи результати аналізу, представлені в табл. 3.2, можемо рекомендувати використання IP-протоколів ZRTP і DTLS. Ці протоколи мають найкращі показники QПРК. Проте, зауважимо, що найбільш поширені IP-протоколи розподілу секретних ключів потребують покращень як у своїх базових характеристиках, так і у забезпеченні інформаційної безпеки IP-телефонії.

Особливу увагу слід звернути на атаки на IP-протоколи розподілу секретних ключів типу «зустріч по середині». Ця атака особливо небезпечна через використання сценарію незалежності випадкових чисел у різних точках IP-телефонії для формування загальної секретної інформації між абонентами. Основу цих протоколів становить асиметричний алгоритм Діффі-Хелмана, і обмін секретною інформацією відбувається на мережевому рівні моделі OSI.

Для забезпечення безпеки IP-протоколу розподілу секретних ключів рекомендується вживання кількох паралельних незалежних каналів сеансів зв'язку в Інтернет-мережах IP-телефонії. Ці канали мають бути повністю незалежними один від одного, щоб у разі захоплення зловмисником одного каналу не давали йому можливості одночасно атакувати інші.

3.3 Підвищення ефективності IP-протоколу ZRTP за допомогою автоматизованої перевірки аутентифікаційного рядка

Для запобігання успішним атакам на асиметричний алгоритм Діффі-Хелмана під час обміну секретною інформацією, необхідно забезпечити захищені канали передачі голосової інформації. Використання протоколу Діффі-Хелмана у захищених каналах дозволить уникнути несанкціонованого доступу, модифікації чи заміни даних. Однак, може виникнути ситуація, коли два абоненти, які не мають загальних сертифікатів або протоколів секретної інформації, спробують встановити захищене з’єднання без захищеного каналу для встановлення зв’язку один з одним[15].

У ситуації, коли абоненти мають сертифікати від різних центрів сертифікації, перевірка достовірності кожного сертифікату стає складною, оскільки кожен абонент може не довіряти центру сертифікації іншого. Для встановлення захищеного зв’язку між ними необхідно згенерувати та розподілити секретну інформацію (ключі). У таких ситуаціях можуть застосовуватись як асиметричні, так і симетричні алгоритми шифрування. Але використання симетричного шифрування має ризик, оскільки ключі потрібно передавати по відкритим каналам зв’язку, що може дозволити нелегітимному абоненту отримати доступ до голосової інформації. Використання асиметричного шифрування забезпечує безпеку переданої інформації, але при обміні відкритими ключами користувачі не можуть бути впевнені, що ключ передається між ними без модифікацій нелегітимним абонентом, як показано на рис. 3.15.

Рисунок 3.15 – Ситуація, коли атака «зустріч по середині» стає можливою під час використання асиметричного шифрування

Використання асиметричного шифрування має свої обмеження через великий розмір відкритого та секретного ключів, що ускладнює їх передавання через Інтернет. Для підвищення безпеки можна застосувати такі методи: перевірку аутентифікаційного рядка SAS абонентів за допомогою додаткового каналу зв'язку, використання декількох каналів зв'язку для передачі секретних ключів.

У сценарії клієнт-клієнт захист від зловмисника можна забезпечити за рахунок перевірки аутентифікаційного рядка абонентів із застосуванням додаткового каналу зв'язку. Однак автоматизація цього процесу на сьогодні не може гарантувати потрібного рівня безпеки, оскільки використовується лише один канал зв'язку між абонентами сесії IP-телефонії. Крім того, існують засоби аналізу і синтезу голосових даних, які можуть бути використані зловмисником для викрадення чи модифікації інформації в потоці даних.

В результаті аналізу і досліджень виявлено, що існує значна ймовірність наявності незалежних каналів зв'язку між абонентами, які не перетинаються. Дослідження показали перевагу легітимних абонентів над нелегітимними, оскільки вони мають доступ до голосових даних з кількох каналів одночасно. Пропонований метод покращення алгоритмів розподілу секретних ключів не забезпечує абсолютної безпеки, але сприятиме підвищенню захищеності даних. Для оцінки ефективності покращення алгоритму можна використовувати такі критерії ймовірності: ймовірність успішної атаки «зустріч по середині»,

ймовірність виявлення цієї атаки та ймовірність успішного генерування та розподілення секретного ключа.

Протокол ZRTP вбудовує механізм захисту від активних атак типу «зустріч по середині». Цей механізм використовує вербальну перевірку короткого аутентифікаційного рядка SAS через голосовий канал між абонентами сесії. Користувачі, що проводять сесію без сервера в топології клієнт-клієнт, отримують аутентифікаційний рядок SAS, який вимовляється одним із учасників і порівнюється з візуальною версією іншим учасником на екрані свого VoIP-пристрою. У разі збігу рядків, можна впевнено стверджувати відсутність активної атаки. Однак існує ризик підробки аутентифікаційного рядка через голосовий канал, і у випадку незбігу рядків може бути виявлена активна атака. При з'єднанні двох абонентів без сервера, автентифікація здійснюється на основі відомих голосових характеристик іншого абонента та немодифікованої передачі даних по двом каналам: для голосового зв'язку і передачі даних SRTP.

За допомогою сучасних технологій та програмно-апаратного забезпечення можна легко аналізувати голос учасників сесії зв'язку та проводити аналіз їх голосу. Проте важливо враховувати дві можливі ситуації. В першій, коли абоненти знають характеристики голосових даних один одного, вербальна перевірка аутентифікаційного рядка SAS може бути уразливою до атаки, оскільки голосова інформація може бути синтезована для модифікації рядка SAS. У другій ситуації, коли учасники сесії не мають інформації про голос один одного, синтез голосу може бути виконаний за умови наявності будь-яких голосових даних. Для покращення захисту протоколу ZRTP може бути використана автоматизована програмно-апаратна перевірка аутентифікаційного рядка SAS, особливо при використанні декількох каналів зв'язку, що дозволяє виявляти порушників інформаційної безпеки рис.3.16.

Рисунок 3.16 – Можливість заміни аутентифікаційного рядка зловмисником під час передачі через голосовий канал зв'язку

Щодо організації захищеного каналу зв’язку, інформацію про IP-адресу можна передавати різними способами, такими як електронна пошта, телефонні розмови або особисті зустрічі. Ця інформація не є секретною для зловмисників і може передаватися через відкриті канали зв’язку. Однак загальна секретна інформація для алгоритмів симетричного шифрування залишається конфіденційною, і в разі її розкриття нелегітимний користувач може розшифрувати потік даних IP – телефонії. Якщо зловмисник отримає секретний симетричний ключ шифрування, він може витворити дані легітимного користувача, представляючи себе як іншого легітимного користувача. Для підвищення захисту даних можна використовувати IP-адреси для забезпечення безпеки IP – телефонії або дозволити отримання даних, які передаються через кілька каналів, легітимним користувачам за умови, що атака «зустріч по середині» відсутня. Цей метод підвищення захисту інформації в IP – телефонії з використанням протоколу ZRTP передбачає передачу повідомлень від користувачів сесії через інший канал зв’язку. Однією з переваг цього методу є його простота у реалізації з використанням програмного забезпечення. Після виконання протоколу ZRTP, аутентифікаційний рядок надсилається до спеціалізованого програмного забезпечення для автоматичної перевірки. Однак є недолік у цьому методі, а саме, що виявити порушника можна лише після успішного завершення протоколу, а не під час його виконання.

Для оцінки можливості застосування двох або більше каналів зв'язку для підвищення захищеності інформації, перш за все, потрібно провести оцінку

ймовірності того, що в маршруті існує загальна точка, де можуть з'єднуватись декілька каналів зв'язку. Також важливо розглянути різні варіанти операторів зв'язку між учасниками сесії та розробити алгоритм для прийняття рішень щодо виявлення порушника в каналі зв'язку і вибору найбільш правильного рішення. Для вирішення цих завдань можна використати програмну автоматичну перевірку аутентифікаційного рядка SAS та виявлення присутності зловмисника, який намагається отримати несанкціонований доступ через один із каналів зв'язку.

Для налагодження захищеного з'єднання в IP-телефонії між абонентами A та B, спочатку вони обмінюються IP-адресами: IPA1, IPA2, IPB1, IPB2, а потім налаштовують таблицю маршрутизації. Після цього вони застосовують IP-протокол ZRTP через канал зв'язку IPA1 - IPB1. Коли протокол ZRTP завершено, генерується аутентифікаційний рядок рис.3.17. Потім абонент A відправляє свій аутентифікаційний рядок SASA по каналу зв'язку IPA2 - IPB2 абоненту B, який отримує його як SASA’. Тоді абонент B відправляє свій аутентифікаційний рядок SASB через канал зв'язку IPA2 - IPB2 до абонента A, який його отримує як SASB.

Рисунок 3.19 – Програмний механізм перевірки аутентифікаційного рядка

Після обміну аутентифікаційними рядками SASA і SASB, абонент B проводить порівняння цих рядків. Якщо значення обох рядків співпадають, можна зробити висновок, що в мережі відсутній активний нелегітимний абонент на каналах зв'язку. Однак, існує можливість, що нелегітимний абонент може присутній одночасно на каналах зв'язку. У випадку, коли аутентифікаційні рядки SASA і SASB не співпадають, абонент B отримує повідомлення від VoIP-монітора IP – телефонії про присутність зловмисника в каналі зв'язку. Абонент A також перевіряє аутентифікаційні рядки SASA і SASB’. Якщо їх значення співпадають,

можна зробити висновок, що в мережі відсутній активний нелегітимний абонент на каналах зв'язку. Однак, існує можливість, що нелегітимний абонент може присутній одночасно на каналах зв'язку. У випадку, коли аутентифікаційні рядки не співпадають, абонент А отримує повідомлення від VoIP-монітора IP – телефонії про присутність зловмисника в каналі зв'язку. Цей протокол дозволяє отримати інформацію про можливу присутність нелегітимного абонента на каналі зв’язку, який може проводити атаку в одному з двох каналів зв’язку. Також важливо розрахувати ймовірності за цим алгоритмом: РУспАт_ЗС – ймовірність успішної атаки «зустріч по середині» з боку нелегітимного абонента; РВиявА_ЗС – ймовірність виявлення активної атаки зловмисника типу «зустріч по середині»; РУсп_СекК – ймовірність успішного згенерування та розподілення загального секретного ключа.

Якщо атака типу «зустріч по середині» була успішною і зловмисник не був виявлений, це означає, що зловмисник здійснив обмін загальною секретною інформацією між учасниками сесії, використовуючи декілька каналів зв'язку. Такий сценарій можливий лише в тому випадку, якщо зловмисник має контроль над потоками даних кожного з використовуваних каналів зв'язку і одночасно модифікує їх.

У випадку протоколу з автоматизованою програмною перевіркою аутентифікаційного рядка SAS, успішність атаки зловмисника може полягати в здатності порушника виконувати синхронну модифікацію потоку даних в кожному з каналів зв'язку під час прослуховування.

4 ТЕХНІКО – ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

4.1 Розрахунок капітальних витрат на розробку

Капітальні витрати на розробку становлять:

$$К=К1+К2 \quad (4.1)$$

де: К1– витрати на розробку, грн.;

К2– витрати на налагодження і дослідну експлуатацію програмного засобу на ПК, грн.;

4.2 Складові структури витрат на розробку

Складові структури витрат на розробку та реалізацію розробки розраховуються за формулою:

$$К1=Зз+Нз+Ві, \quad (4.2)$$

де: Зз – загальна зарплата розробників, грн;

Нз – нарахування на зарплату, грн;

Ві – інші витрати, грн;

Для проведення розрахунків зарплати (Зз) необхідно визначити спеціальність робітників, чисельність робітників і трудомісткість цих робіт. Для розробки проектного рішення потрібно чотири спеціалісти розробники:

– Керівник проекту(К);

–Студент-дипломник(СД);

– Консультант з економічне ї частини(КЕ);

– Консультант з охорони праці(КОП);

Згідно з штатним розписом сума витрат на оплату праці робітників, з 01.01.2025р. складає:

– Керівник (викладач вищої категорії) – 107,93 грн/год;

– Консультант з економічної частини (викладач вищої категорії) – 107,93 грн/год;

– Консультант з охорони праці(викладач першої категорії) 93,70 грн/год;

– Час витрачений керівником – tk = 14 годин.

– Час витрачений консультантом з охорони праці – tko= 1 година.

– Час витрачений консультантом з економічної частини–tke = 1 година.

– Час витрачений студентом дипломником tc = 3×50= 150 годин.

Витрати на оплату праці керівника проекту:

Ск = 14 роб.год.× 107,93 грн.год.=1511,02 грн.

Витрати на оплату праці консультанта з економічної частини:

Ске = 1 роб.год.×107,93грн.год.= 107,93 грн.

Витрати на оплату праці консультанта з охорони праці :

Ско = 1 роб.год×93,70грн.год.= 93,70грн.

Денна оплата студента дипломника :

1510/173=8,73 грн.

1510 – стипендія

173 – місячний фонд робочого часу, годин.

Витрати на оплату праці студента дипломника

Сс = 8,73×150= 1310 грн.

Витрати на оплату праці робітників проектустановлять

Зз= Ск+Ске+Ско+Сс= 1511,02 +107,93 +93,70 +1310= 3022,65 грн.

Нарахування на зарплату визначаються в розмірі 22% від фонду оплати праці

Нз = Зз×22% = (3022,65 ×22)/100 = 664,98 грн.

де 22 – норматив нарахування на зарплату, %

Інші витрати Ві відображають витрати які, не враховані в попередніх статтях витрат. Ці витрати розраховуються згідно структури витрат(5%)

Ві = 0.05×(Зз+Нз)= 0.05×(3022,65 +664,98)=1843,93 грн.

К1 = Зз+Нз+Ві= 3022,65 +664,98 +1843,93 =5578,56 грн.

4.3 Витрати на відлагодження розробки

Витрати на від лагодження та дослідну експлуатацію розробки

$$К2 = Sм\text{-}г. \times t \quad (4.3)$$

де Sм-г. – вартість однієї машино-години роботи конкретно ПК, грн./год.;

t–машинний час, витрачений на накладку та дослідну експлуатацію програмного засобу, год.

Вартісь 1 машинно-години роботи ПК розраховуємо за складовими витрат на таку роботу:

$$Sм\text{-}г =(А+Ен)/Фд \quad (4.4)$$

де А – амортизація використаного ПК, грн;

Ен – вартість електроенергії, яку споживає ПК, грн.;

Фд – дійсний час від лагодження програми, год.;

Розрахунок складових вартості 1 машино-години роботи ПК:

а) амортизація ПК становить

А= (Кт×На)/100 = (670,31 ×15%)/100= 100,55 грн.

Де Кт – вартість використання ПК, грн..

На – норма амортизації (На=15%)

Кт = (Кс×Тексп)/Твик = (14625×2,2)/48= 670,31 грн.

де Кс – вартість компютероної системи,грн.

Тексп – період експлуатації системи 2.2 місяців(50 робочих днів)

Твик – термін корисного використання 4 роки (48 місяців):

Кс= Ркомп×Р$ = 500×41,00=14625 грн.

де Ркомп –вартість комп'ютерної системи у доларах США;

Р$ – курс долара США по курсу НБУ на момент купівлі системи.

б) вартість використання електроенергії розраховується за формулою:

Ен = (Р×Тф)×Фд×Квик=(0,25 ×5,60)×150×0,8=154,8грн.

де Р – потужність обчислювальної системи, кВт (Р=0,25)

Квик – коефіцієнт використання ПК

Тф – ціна за 1кВт/год.,грн..(Тф = 5,16 грн.)

Фд – дійсний час від лагодження програми

Фд = пр.д.×Тсер= 50р.дн.×3год. = 150год.

Де пр.д. – кількість робочих днів ПК

Тсер = 3 год – середній щоденний час роботи ПК

Отже вартість 1 машино-години роботи і від лагодження на ПК становить

Sм-г=(100,55+154,8)/150= 1,70 грн.

Таким чином сумарні витрати на від лагодження і дослідну експлуатацію проектного рішення становлять:

К2=Sм-г×Фд= 1.70×150=255 грн.

Отже, капітальні витрати на розробку проектного рішення за формулою становлять:

К=К1+К2 = 5578,56 + 255 = 5833,56 грн.

Загальний кошторис витрат на розробку проектного рішення приведений в таблиці 4.1

Таблиця 4.1 – Кошторис витрат на розробку проектного рішення

Складові елементи витрат	Умовне позначення	Сума витрат, грн
Витрати на оплату праці	Зз	3022,65
Нарахування на зарплату	Нз	664,98
Інші витрати	Ві	1843,93
Разом	К1	5578,56
Витрати на відлагодження	К2	255
Разом К=К1+К2	К	5833,56

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЕДІЯЛЬНОСТІ

5.1 Загальні положення

Визначення поняття охорони праці дається в ст. 1 Закону України від 14 жовтня 1992 р. «Про охорону праці». Охорона праці – це система правових, соціально-економічних, організаційно-технічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. В поняття охорони праці входять і всі ті заходи, що спеціально призначені для створення особливих полегшених умов праці для жінок і неповнолітніх, а також працівників зі зниженою працездатністю. Охорону праці і здоров'я громадян віднесено до пріоритетних напрямків соціальної політики України. Так, Конституція України одним з основних соціальних прав громадян визначає право кожного на належні, безпечні й здорові умови праці, встановлює, що використання праці жінок і неповнолітніх на небезпечних для їхнього здоров'я роботах забороняється. Завдання охорони праці:

– проектування підприємств, технологічних процесів і конструювання обладнання з обов'язковим виконанням вимог охорони праці;

– знаходження оптимальних співвідношень між різними факторами виробничого середовища, що дозволяє забезпечити мінімум несприятливого впливу їх на здоров'я працівників;

– розробка конкретних заходів щодо покращення умов праці та забезпечення її безпеки на основі застосування у виробництві новітніх досягнень науки і техніки;

– застосування раціональних засобів захисту працівників від впливу несприятливих факторів виробничого середовища, а також втілення організаційних заходів, які нейтралізують або послаблюють ступінь їх впливу на організм людини;

– розробка та застосування методів і засобів оцінки ефективності заходів з охорони праці, що плануються і здійснюються.

5.2 Організація охорони праці на підприємстві

На сучасному етапі науково-технічного розвитку нашої держави питання охорони праці на підприємствах є одним із найактуальніших.

Належна організація охорони праці, яка відповідає вимогам нормативно-правових актів, є основним заходом профілактики та запобігання виробничому травматизму й професійній захворюваності. Крім того, кожним трудовим договором передбачаються зобов’язання роботодавця щодо забезпечення найманих працівників безпечними умовами праці.

Законодавство України покладає на всіх роботодавців обов'язок щодо забезпечення безпечних і нешкідливих умов праці. Витрати на охорону праці на підприємстві згідно зі ст. 19 Закону повинні становити не менше 0,5% від фонду оплати праці за попередній рік, а за невиконання законодавства про охорону праці до підприємства можуть бути застосовані санкції аж до заборони його експлуатації.

Для того щоб не поставити під загрозу існування підприємства, роботодавцю необхідно:

– створити службу охорони праці.

Згідно зі ст. 15 Закону така служба обов'язково повинна бути створена на підприємстві з кількістю працюючих 50 і більше осіб відповідно до Типового положення про службу охорони праці, затвердженого наказом Держкомітету з нагляду за охороною праці від 15.11.2004 № 255. На підставі цього документа також має бути розроблено Положення про службу охорони праці цього підприємства, визначено структуру такої служби, її чисельність, основні завдання, функції та права її працівників. На підприємствах із кількістю працівників менше 50 осіб функції служби охорони праці можуть виконувати в порядку сумісництва особи, які мають відповідну підготовку.

– Розробити та затвердити на підприємстві положення, інструкції та інші акти з охорони праці.

Обов'язок роботодавця стосовно розробки та затвердження документів, які повинні встановлювати правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майдан-чиках і робочих місцях, передбачений ст. 13 Закону про охорону праці.

– Організувати проведення інструктажів з питань охорони праці.

Перед початком роботи нового працівника роботодавець згідно зі ст. 29 КЗпП зобов'язаний проінформувати його під розпис про умови праці, наявні на його робочому місці, у тому числі про всі небезпечні чи шкідливі виробничі фактори, які ще не усунуто, та про можливі наслідки їх впливу на здоров'я працівника, а також про можливі пільги та компенсації за роботу в таких умовах.

– Забезпечити навчання і перевірку знань з питань охорони праці.

Згідно зі ст. 18 Закону працівники, зайняті на роботах з підвищеною небезпекою або там, де є потреба у професійному доборі, проходять спеціальне навчання і перевірку знань відповідних нормативно-правових актів з охорони праці. Таке навчання з питань охорони праці може проводитись як безпосередньо на підприємстві, так і навчальним центром.

– Подбати про проведення медичних оглядів.

Згідно зі ст. 169 КЗпП роботодавець зобов'язаний за свої кошти організувати проведення попереднього (при прийнятті на роботу) та періодичних (протягом трудової діяльності) медоглядів працівників, зайнятих на важких роботах, роботах із шкідливими чи небезпечними умовами праці або таких, де є потреба у професійному доборі. Також він зобов'язаний проводити щорічний обов'язковий медогляд осіб віком до 21 року.

– Забезпечити працівників засобами індивідуального захисту.

На роботах із шкідливими й небезпечними умовами праці, а також на роботах, пов'язаних із забрудненням або несприятливими температурними умовами, працівникам згідно зі ст. 164 КЗпП необхідно безкоштовно видавати спеціальний одяг, взуття та інші ЗІЗ.

– Провести атестацію робочих місць.

На підприємствах, де технологічний процес, використовуване обладнання, сировина, матеріали є потенційними джерелами шкідливих і небезпечних виробничих факторів, які можуть негативно впливати на стан здоров'я працюючих, повинна проводитись атестація робочих місць за умовами праці. Така атестація повинна проводитися атестаційною комісією, склад і повноваження якої визначаються наказом по підприємству в строки, передбачені колективним договором, але не рідше одного разу на 5 років. Порядок проведення такої атестації передбачений постановою КМУ від 01.08.1992 № 442. Відомості про результати атестації заносяться в картку умов праці.

– Налагодити облік нещасних випадків.

Згідно зі ст. 22 Закону «Про охорону праці» роботодавець зобов'язаний організувати розслідування та вести облік нещасних випадків, професійних захворювань і аварій у порядку, встановленому постановою КМУ від 30.11.2011 № 1232. За результатами такого розслідування роботодавець повинен складати акт за формою Н-5 (якщо нещасний випадок визнано таким, що не пов'язаний з виробництвом) або Н-1 (якщо він визнаний пов'язаним з виробництвом). Один із примірників повинен видатися потерпілому або іншій зацікавленій особі не пізніше трьох днів з моменту закінчення розслідування.

5.3 Заходи безпеки на робочому місці

Конструкція робочого місця, його розміри та взаємне розташування його елементів повинні відповідати антропометричним, фізіологічним І психофізіологічним характеристикам людини, а також характеру роботи.

Організація робочих місць повинна забезпечувати стійке положення та вільність рухів працівника, безпеку виконання трудових операції виключати або допускати лише в деяких випадках роботу в незручну позиціях, котрі зумовлюють підвищену втомлюваність.

Загальні принципи організації робочого місця:

– на робочому місці не повинно бути нічого зайвого; всі необхідні для роботи предмети повинні знаходитись поряд з працівником, але не заважати йому;

– ті предмети, котрими користуються частіше, розташовуються ближче, ніж ті предмети, котрими користуються рідше;

– предмети, котрі беруть лівою рукою, повинні знаходитись зліва а ті предмети, котрі беруть правою рукою, повинні знаходитись справа;

– якщо використовують обидві руки, то місце розташування інструментів вибирається з врахуванням зручності захоплювання його двома руками;

– небезпечніше, з точки зору можливості травмування обладнання повинне розташовуватись вище, ніж менш небезпечне. Однак слід враховувати, що важкі предмети під час роботи зручніше опускати, ніж піднімати.

5.4 Санітарно-гігієнічні вимоги

Санітарно-гігієнічні вимоги до умов праці під час виконання роботи мають відповідати визначеним нормативам:

– параметри мікроклімату у приміщенні забезпечували комфортне самопочуття організму. Параметри мікроклімату закритих приміщень унормовані за санітарні норми ДСН 3.3.6.042-99.

– освітлення приміщень та робочих місць забезпечене відповідно до встановлених вимог. Відносно вікна робоче місце розміщено так, що природне світло збоку, переважно з лівого та забезпечувало коефіцієнт природної освітленості не нижче 1,5 %. Освітленість за штучного освітлення в площині робочої поверхні становила 300 – 500 Лк. Відношення яскравості робочих поверхонь було 3:1, а яскравість робочих поверхонь і стін (іншого обладнання) – 5:1. Використана система вимикачів, що дозволяє регулювати інтенсивність штучного освітлення залежно від інтенсивності природного, а також дозволяє освітлювати тільки потрібні для роботи зони приміщення.

– Дотримані вимоги до рівнів шуму та вібрації. Було дотримано допустимих рівнів звукового тиску в октавних смугах частот, еквівалентні рівні звуку на робочих місцях встановлені санітарними нормами виробничого 17 шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99.

– Надходження свіжого повітря регульоване, виходячи із відповідних нормативних.

– Передбачений захист від шуму та вібрацій.

Дотримані заходи особистої гігієни на робочому місці (підтримання чистоти, миття рук тощо). Заходи особистої гігієни на робочому місці передбачають щоденне вологе прибирання, утримання у чистоті робочого місця, наявність на робочому місці тільки необхідних для роботи засобів. На робочому місці необхідно дотримуватись вимог правил внутрішнього трудового розпорядку.

ВИСНОВКИ

Телефонний зв'язок став невід'ємною складовою сучасного життя, відіграючи ключову роль у всіх сферах діяльності. Якість телефонного зв'язку визначає багато аспектів, включаючи відносини в сім'ї, успіх в бізнесі та загальний комфорт людей. З цієї причини безпека телефонного зв'язку є критично важливою.

IP-телефонія, яка базується на передачі голосу через мережі IP, відкрила нові можливості для побудови ефективної та зручної системи зв'язку. Ця технологія дозволяє значно знизити витрати на дзвінки між різними пунктами, спрощує організацію номерного плану та забезпечує інтеграцію телефонії із системами передачі даних.

У роботі проведено аналіз та дослідження основних аспектів побудови мереж IP-телефонії, включаючи розгляд архітектури, протоколів і методів з'єднання. Були розглянуті існуючі проблеми та запропоновані методи їх вирішення, зокрема, метод виявлення нелегітимних користувачів та захист від атак «зустріч по середині».

Запропонований метод підвищення безпеки IP-телефонії передбачає автоматизовану програмно-апаратну перевірку аутентифікаційного рядка та виявлення потенційних загроз безпеці. Цей підхід сприяє забезпеченню високого рівня захисту інформації та підвищує відповідальність за безпеку в сеансах безпечної IP-телефонії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кононова В.О. Оцінка засобів захисту інформаційних ресурсів /Кононова В.О., Харкянен О. В., Грибков С. В. / Національний університет харчових технологій, кафедра інформаційних систем – 2014. – с.99-105;

2. Опірський І.Р. Аналіз використання програмних приманок як засобу забезпечення інформаційної безпеки / Опірський І.Р., Василишин С.І., Піскозуб А.З. / Кібербезпека:освіта, наука, техніка - №2 (10) – 2020. – с.88-97;

3. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні). Мікросистеми, електроніка та акустика - 2017. № 6. Том 22. С. 64-70.

4. Гнатюк С.О. Базові аспекти захисту конфіденційної інформації на об'єктах критичної інформаційної інфраструктури/ Гнатюк С.О., Сидоренко В.М., Сотніченко Ю.О./ Кібербезпека:освіта, наука, техніка - №1 (9) – 2020. – с.170-181;

5. Гнатюк С.О. Аналіз кращих світових практик щодо захисту критичної інформаційної інфраструктури / Гнатюк С.О., Поліщук Ю.Я., Сотніченко Ю.О., Жаксигулова Д.Д. / Кібербезпека:освіта, наука, техніка - №2 (10) – 2020. – с.184-196;

6. Литвинов В.В. Сучасний стан захисту інформації в ір-телефонії / В.В. Литвинов, В.В. Казимир, Є.В. Риндич / Математичні машини і системи - №2 – 2009. – с.76-84;

7. Н.І. Алішов / Застосування нерозкривних шифрів для убезпечення VOIP- Телефонії / Н.І. Алішов, С.В. Зінченко, А.Н. Алішов, Н.О. Сапунова / Системи управління, навігації та зв'язку - випуск 1(41) – 2017. - с. 3-7;

8. Черкасов Дмитро / Основи технології VoIP та IP-телефонії / Черкасов Д., Інструктор Cisco, Національний Університет «Києво-Могилянська Академія» / Телеком военная связь – №2 – 2017. – с.98-104;

9. І.О. Золотарьова, А.І. Костюков / Інтернет-телефонія як сучасний засіб комунікацій в бізнесі / Харківський національний економічний університет, Харків // Системи обробки інформації – Випуск 7 (97) – 2011 – с.16-18;

КОПІЇ ОБОВ’ЯЗКОВИХ КРЕСЛЕНЬ