**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

А.В. Ільєнко

« » 20 р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема:** Система захисту інформації в мережах IP-телефонії

|  |  |
| --- | --- |
| **Автор:** | К.І. Бекала |
| **Науковий керівник:** д.ф-м.н.проф. | О.В. Азаренко |
| **Нормоконтролер:** асистент | С.В. Єгоров |
|  |  |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Комп’ютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма:** «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_С.В. Казмірчук

«\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Бекала Катажини Іренеушівни**

1. Тема: *Система захисту інформації в мережах IP-телефонії*

затверджена наказом ректора від «02» жовтня 2019 № 2265/ст.

1. Термін виконання з 14.10.2019 р. по 09.02.2020 р.
2. Вихідні дані роботи: дані про мережу IP-телефонії, її склад, схему роботи та вразливості для визначення рівня захищеності системи.
3. Зміст пояснювальної записки: проведення аналізу нормативно-правового забезпечення України та міжнародних стандартів в сфері захисту інформації. Дослідження побудови мереж IP-телефонії, а також їх види та особливості. Визначення вразливостей та особливостей захисту мереж IP-телефонії. Аналіз компонентів системи IP-телефонії та визначення її рівня захищеності. Розробка системи захисту мережі IP-телефонії. Надання рекомендацій щодо посилення захисту системи.
4. Перелік обов'язкового ілюстративного матеріалу: таблиці, рисунки, графіки.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі | 14.10.19 | *Виконано* |
|  | Аналіз літературних джерел | 15.10.19-01.11.19 | *Виконано* |
|  | Обґрунтування вибору рішення | 02.11.19-07.11.19 | *Виконано* |
|  | Збір інформації | 08.11.19-21.11.19 | *Виконано* |
|  | Аналіз даних та їх класифікація | 22.11.19-10.12.19 | *Виконано* |
|  | Ознайомлення із загальними принципами роботи мереж IP-телефонії та їх вразливостями | 11.12.19-20.12.19 | *Виконано* |
|  | Розробка комплексу захисту вразливостей мережі IP-телефонії | 21.12.19-01.01.20 | *Виконано* |
|  | Розробка програмного модулю, що забезпечує захист мережі від несанкціонованого доступу за допомогою блокування IP-адрес | 02.01.20-18.01.20 | *Виконано* |
|  | Тестування програмної реалізації та її роботи в побудованій системі захисту | 19.01.20 | *Виконано* |
|  | Перевірка на антиплагіат | 20.01.20 | *Виконано* |
|  | Оформлення і друк пояснювальної записки | 21.01.20-26.01.20 | *Виконано* |
|  | Оформлення презентації | 27.01.20-29.01.20 | *Виконано* |
|  | Отримання рецензій від рецензента | 30.01.20 | *Виконано* |
|  | Підготування доповіді | 31.01.20-03.02.20 |  |
|  | Захист в ЕК | 04.02.20 | *Виконано* |

Магістрант К. Бекала

(підпис, дата)

Науковий керівник О. Азаренко

(підпис, дата)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, основної частини, що містить 3 розділи, загальних висновків і списку використаних джерел, додатків і має 92 сторінок основного тексту, 13 рисунків, 3 сторінки додатків. Список використаних джерел містить 40 найменування і займає 5 сторінки. Загальний обсяг роботи 95 сторінок.

Метою роботи є створення системи захисту мереж IP-телефонії.

Предмет дослідження: мережа IP-телефонії.

Об’єкт дослідження: захист мереж IP-телефонії.

Мета дипломної роботи: створення системи захисту мереж IP-телефонії.

Тема роботи є актуальною з огляду на те, що на сьогоднішній день розвиток мережі інтернет неухильно зростає, проблема захисту інформації в IP-мережах від зловмисників є досить назрілою на сьогоднішній день. Актуальність безпеки мереж IP-телефонії пов'язана з широким застосуванням в різних організаціях, підприємствах і установах та великим інтересом зловмисників до цієї галузі.

Наукова новизна дослідження полягає в наступному: вперше розроблено та реалізовано алгоритм блокування зловмисників та визначення інших необхідних складових системи захисту. За рахунок цього алгоритм сприяє більш ретельному захисту мережі, що дозволяє запобігати повторним атакам.

Практичне значення роботи полягає у тому, що сукупність засобів та методів, застосованих в системі, забезпечуюсь надійний захист від можливих загроз та створюють потужний відсіч атакам зловмисників. Завдяки цьому забезпечується стабільна робота мережі та захист персональних даних користувачів від витоку, а також таємниця телефонних розмов.

Ключові слова: IP-ТЕЛЕФОНІЯ, ЗАХИСТ МЕРЕЖ, БЕЗПЕКА IP-ТЕЛЕФОНІЇ, ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ, ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ, ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ, БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ, СИСТЕМА ЗАХИСТУ IP-МЕРЕЖІ.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7](#_Toc30416181)

[ВСТУП 9](#_Toc30416182)

[РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ ЩОДО ЗАХИСТУ МЕРЕЖIP-МЕРЕЖ 12](#_Toc30416183)

[1.1 Основи законодавства України в сфері захисту інформації 12](#_Toc30416184)

[1.2 Правові засади застосуваннятехнології IP-телефонії 15](#_Toc30416185)

[1.3 Статус IP- телефонії в законодавстві США 25](#_Toc30416186)

[1.4. Правове регулювання IP- телефонії в країнах Європи 27](#_Toc30416187)

[1.5. Висновок по розділу 28](#_Toc30416188)

[РОЗДІЛ 2. ОСНОВИ ЗАХИСТУ МЕРЕЖ IP-ТЕЛЕФОНІЇ 30](#_Toc30416189)

[2.1 Поняття IP-телефонії, базовихпринципів та протоколів 30](#_Toc30416190)

[2.2 Стандарти IP-телефонії та механізми їх безпеки 39](#_Toc30416191)

[2.3 IP-телефонія на базі АТС Asterisk 41](#_Toc30416192)

[2.4 Проблеми захисту IP-телефонії від загроз 43](#_Toc30416193)

[2.5 Вразливості мереж IP-телефонії та можливі загрози 48](#_Toc30416194)

[2.6 Безпека IP-телефонії 54](#_Toc30416195)

[2.7 Висновок по розділу 55](#_Toc30416196)

[РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ ЗАХИСТУ МЕРЕЖI IP-ТЕЛЕФОНІЇ 57](#_Toc30416197)

[3.1 Підвищення надійності IP-мереж 57](#_Toc30416198)

[3.2 Застосування мережевих екранів 62](#_Toc30416199)

[3.3 Встановлення безпечного зв'язку та шифрування розмов 64](#_Toc30416200)

[3.4 Застосування VPN-тунелів 67](#_Toc30416201)

[3.5 Захист за допомогою Dialplan 72](#_Toc30416202)

[3.6 Фізична безпека та контроль доступу 73](#_Toc30416203)

[3.7 Система фільтрації 75](#_Toc30416204)

[3.8 Перевірка та захист від небажаних IP-адрес 76](#_Toc30416205)

[3.9 Висновок по розділу 83](#_Toc30416206)

[ВИСНОВКИ 85](#_Toc30416207)

[СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ 88](#_Toc30416208)

[Додаток А. Блок-схема методу перевірки та блокування небажаних IP-адрес 92](#_Toc30416209)

[Додаток Б. Програмна реалізація методу перевірки та блокування небажаних IP-адрес(prog.conf ) 93](#_Toc30416210)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

IP – Internet Protocol – міжмережевий протокол;

VoIP – Voice over IP – IP-телефонія, технологія для організації зв’язку;

IVR – Interactive Voice Response – система голосової маршрутизації дзвінків;

MAC – Media Access Control – контроль доступу до середовища;

LLC – Logical Link Control – контроль логічного зв’язку;

ПД – Передача Даних;

UDP – User Datagram Protocol – протокол забезпечення надійності даних;

TCP — Transmission Control Protocol – протокол управління передачі даних;

RTP – Real-timeTransport Protocol – протокол передачі даних реального часу;

HTTP – HyperText Transfer Protocol – протокол передачі гіпертексту;

SIP – Session Initiation Protocol – протокол встановлення сеансу;

TLS - Transport Layer Security – протокол захисту транспортного рівня;

SRTP - Secure Real-time Transport Protocol – безпечний протокол передачі данихв режимі реального часу;

ZRTP - [Zimmermann Real-Time Transport Protocol](https://searchunifiedcommunications.techtarget.com/definition/ZRTP)– протокол передачі даних в режимі реального часу Зімермана;

SSL — Secure Sockets Layer – рівень захищених сокетів;

КС – Комп’ютерна Система;

АС – Автоматизована Система;

АТС – Автоматична Телефонна Станція;

PBX – Private Branch Exchange – відомча АТС;

DNS – Domain Name System – доменна система імен;

API – Application Programming Interface – програмний інтерфейс програмування;

AMI – Asterisk Management Interface – інтерфейс управління Asterisk;

VPN – Virtual Private Network – віртуальна приватна мережа;

AES — Advanced Encryption Standard – pозширений стандарт шифрування;

RSA — Riverst-Shamir-Adleman – алгоритм Рівеста-Шаміра-Адлемана;

SQL –Structured Query Language – структуризована мова запитів;

AH – Authentication Header – заголовок аутентифікації;

SPI – Security Parameters Index – індекс параметрів безпеки;

SN – Sequence Number – порядковий номер пакету даних;

ESP – Encapsulating Security Payload – інкапсуляція зашифрованих даних;

ISAKMP – Internet Security Association and Key Management Protocol – інтернет протокол асоціацій безпеки та керування ключами;

IKE – Internet Key Exchange – протокол обміну ключами;

CRM – Customer Relationship Management – система управління взаємо відносинами між клієнтами;

PSTN — Public Switched Telephone Network – телефонна мережа загального користування;

AEL – Asterisk Extension Language – мова розширень Asterisk;

DoS – Denial-of-service – атака типу «відмова в обслуговуванні»;

QoS –Quality-of-service – технологія якості обслуговування.

# ВСТУП

Сучасний світ характеризується динамічним розвитком галузі інформаційних технологій. Неможливо уявити підприємство або особу, яка б не користувалася здобутками цієї галузі. Чим ширше використовується технологія, тим більший інтерес кібер-злочинців.

Зацікавленість кібер-злочинцями мережами IP-телефонії зростає різкими темпами, паралельно збільшенню кількості користувачів. VoIP давно стала об’єктом атак, оскільки з кожним днем її популярність збільшується. Вона викликає великий інтерес у хакерів, адже має доступ до поштового серверу та банківського онлайн-рахунку.

Оскільки VoIP базується на технології IP та використовує Інтернет, вона також наслідує всі їх вразливості. Окрім наслідуваних, IP-телефонія має вразливості, які випливають з особливостей архітектури мереж VoIP. Сукупність усіх таких вразливостей створюють потребу у посиленні захисту та ретельному аналізі мережі. Наслідки атак на IP-телефонію, які до можуть бути: крадіжка викликів, збій у роботі серверів, а також крадіжка персональних даних та подальші дії з ними. Однак таке широке поширення VoIP спричинило за собою ряд проблем, найзначніші з яких пов'язані з інформаційною безпекою. На сьогоднішній день одним з важливишіх завдань IP-телефонії є забезпечення захисту мережі, вдосконалення існуючих або реалізація нових методів протидії атакам.

Таким чином, актуальність задачі забезпечення безпеки мереж IP-телефонії пов'язана з широким застосуванням в різних організаціях, підприємствах і установах та великим інтересом зловмисників до цієї галузі. З цього випливає, що одним з важливіших завдань IP-телефонії є забезпечення захисту мережі, вдосконалення існуючих або реалізація нових методів протидії атакам.

Метою роботи є створення системи захисту мереж IP-телефонії.

Відповідно до мети роботи необхідно вирішити наступні завдання:

* Дослідити мережу IP-телефонії;
* Аналіз вразливостей мережі IP-телефонії;
* Розробка системи захисту інформації в мережах IP-телефонії;
* Розробка додатку для блокування небажаних IP-адрес.

Об’єктом дослідження є захист мереж IP-телефонії. Предметом дослідження є мережа IP-телефонії.

Методи дослідження. Дослідження по даній роботі проводились за допомогою системного аналізу методів та засобів захисту інформації в мережах IP-телефонії. Даний метод спирається на комплекс загальнонаукових, експериментальних, статистичних, математичних [методів](https://uk.wikipedia.org/wiki/Метод).

Наукова новизна дослідження полягає в наступному: розроблено та реалізовано алгоритм блокування зловмисників та визначення інших необхідних складових системи захисту. Алгоритм сприяє більш ретельному захисту мережі, здатен запобігати повторним атакам.

Практичне значення роботи полягає у тому, що сукупність засобів та методів, застосованих в системі, забезпечуюсь надійний захист від можливих загроз та створюють потужний відсіч атакам зловмисників. Завдяки цьому забезпечується стабільна робота мережі та захист персональних даних користувачів від витоку, а також таємниця телефонних розмов. Було розроблено та реалізовано алгоритм блокування зловмисників та визначення інших необхідних складових системи захисту. Алгоритм сприяє більш ретельному захисту мережі, здатен запобігати повторним атакам.

Було опубліковано ряд наукових статей, присвячених темі, що розглядалася в магістерській атестаційній роботі:

1. Бекала К.И. Исследование уязвимостей сетей IP-телефонии / Б.Я. Корниенко, Л.П. Галата // Тенденции современной науки. – 2018. – с. 39-42.
2. Бекала К.І. Метод захисту інформації в мережах IP-телефонії від несанкціонованного доступу на базі АТС Asterisk / Б.Я. Корнієнко //Політ. Сучасні проблеми науки. – 2018. – с.5
3. Bekala Katarzyna Algorithm for protecting access to confidential information in IP-telephony networks // [Европейская наука XXI века](http://www.rusnauka.com/15_ENXII_2018/List.htm). – 2018.– с. 55-58.
4. Бекала К.И. Алгоритм защитысетей IP-телефонии от несанционированного доступа // Комп’ютерні системи і мережні технології. – 2018. –№ 11 – с. 9-10.
5. Bekala Katazhyna A method of protection of information in IP-telephony networks against unauthorized access based onAsterisk PBX // East European Science Journal. – 2019. – №8(48) – с. 21-24.

# РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ ЩОДО ЗАХИСТУ МЕРЕЖIP-МЕРЕЖ

## 1.1 Основи законодавства України в сфері захисту інформації

Відповідність до стандартів є лише однією з багатьох вимог, що пред'являються до сучасних мереж. Важливішим є виконання мережею певного набору послуг, наприклад, надання доступу до файлових архівів або веб-сторінок публічних Інтернет-сайтів, обмін електронноюпоштою в межах підприємства або в глобальних масштабах, інтерактивний обмін голосовими повідомленнями IP-телефонії тощо.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога що до захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України [1].

Під [інформаційною](http://ua-referat.com/Інформація) безпекою розуміється захищеність інформації та підтримує її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктурі.  Забезпечення захисту інформації є обов'язковою умовою успішного функціонування будь-якого підприємства [1].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» об’єктами кіберзахисту є: комунікаційнісистемивсіх форм власності, в яких обробляються національні інформаційні ресурси та/абоякі використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об’єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1].

Цей Закон також надає взаємопов'язане визначення об'єкткритичної інформаційної інфраструктури: комунікаційна або технологічна система об'єкта критичної інфраструктури, [кібератака](https://uk.wikipedia.org/wiki/Кібератака) на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [1].

Також в цьому Законі вказано, що суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

* здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;
* здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;
* здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;
* розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;
* забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;
* здійснюють заходи із забезпечення розвитку і безпеки кіберпростору [1].

Вимоги до комплексної системи захисту інформації в АС в частині захисту від НСД мають бути викладені відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності комп'ютерних систем від несанкціонованого доступу». Згідно з цим документом в процесі оцінки захищеності АС розглядаються вимоги двох видів: вимоги до функцій (послуг) забезпечення безпеки і вимоги до рівня гарантій [2].

Має бути вказаний функціональний профіль захищеності, який передбачається реалізувати. Профіль може бути або вибраний із профілів, описаних в НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», або визначений як упорядкована сукупність рівнів послуг згідно з вимогами зазначеного документа. Повинен бути вказаний рівень гарантій, що передбачається досягти [2].

Інструкція користувача автоматизованої системи 3 класу регламентує роботу співробітників в частині захисту конфіденційної та іншої інформації, що є власністюдержави, під час користування автоматизованою системою 3 класу (АС 3) - окремою локальною підмережею, що приєднана до мережі Інтернет та електронної пошти. Положення Інструкції не поширюються на роботи, які пов'язані з обробленням інформації, що становить державну таємницю, а також інформації, що має криптографічний захист. З метою захисту інформації, щоциркулює в АС 3 відпошкодження. В Інструкції викладено організаційно-технічні заходи, що враховують і компенсують неможливість у сучасних умовах забезпечити програмно-технічними засобами надійний захист АС 3 з точки зору конфіденційності, цілісності і доступ ностіінформації, яка в ній циркулює. У зв'язку з неможливістю без використання криптографії гарантувати цілісність та авторизованість документів, отриманих електронною поштою, таку інформацію не дозволяється використовувати для прийняття державних рішень без додаткової перевірки [2]. Ця Інструкція розроблена на підставі:

* Закону України "Про захист інформації в автоматизованих системах";
* Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави;
* НД ТЗІ 1.1-002-99. Загальних положень щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;
* НД ТЗІ 2.5-005-99. Класифікації автоматизованих систем і стандартних функціональних профілей захищеності оброблюваної інформації від несанкціонованого доступу;
* НД ТЗІ 2.5-004-99. Критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [2].

Далі бачимо визначення щодо Державно-приватної взаємодії у сфері кібербезпеки, яка здійснюється шляхом створення системи своєчасного виявлення, запобігання та нейтралізації кібер-загроз, у тому числі із залученням волонтерських організацій тощо [2].

## 1.2 Правові засади застосуваннятехнології IP-телефонії

Закон України «Про зв’язок» встановлює правовi, економiчнi i органiзацiйнi основи дiяльностi в галузi зв'язку в Українi та визначає вiдносинипiдприємств, об'єднань, установ i органiзацiй зв'язку з органами державної виконавчої влади, мiсцевого самоврядування i споживачами послуг зв'язку, а також особливостiгалузi, пов'язанi з особливими суспiльнимиiнтересами. Закон захищає iнтереси держави, громадян, пiдприємств, об'єднань, установ i органiзацiй, що користуються послугами зв'язку, а також працiвникiвгалузi зв'язку [3].

Закон України «Про телекомунікації» встановлює правову основу діяльності у сфері телекомунікацій, яка здійснюється під юрисдикцією держави Україна. Телекомунікації разом з поштовим зв’язком відносяться до галузі зв’язку України. Закон визначає повноваження держави щодо регулювання вказаної діяльності, а також права та обов'язки фізичних та юридичних осіб, що приймають участь у даній діяльності або користуються телекомунікаційними послугами. Дія цього Закону поширюється на відносини між органами державної влади України, фізичними та юридичними особами, між юридичними особами щодо надання та отримання телекомунікаційних послуг, використання телекомунікаційних мереж загального доступу, інформаційних систем загального доступу, номерного ресурсу, виконання робіт у сфері телекомунікацій. Закон не поширюється на телекомунікаційні мережі закриті і спеціальні, за винятком питань регулювання їх взаємодії з телекомунікаційними мережами загального та обмеженого доступу, надання телекомунікаційних послуг в умовах надзвичайного стану та надзвичайної ситуації. На телекомунікаційні мережі закриті та спеціальні, які, крім основного призначення, використовуються для надання телекомунікаційних послуг, поширюються правові норми, що регулюють функціонування телекомунікаційних мереж загального доступу.

Порядок взаємоз'єднання та взаєморозрахунків операторів щодо здійснення діяльності з надання послуг фіксованого міжнародного, міжміського телефонного зв'язку із застосуванням технології IP-телефонії розроблено відповідно до Закону України "Про телекомунікації" та Ліцензійних умов провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного, міжміського, місцевого телефонного зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку, затверджених наказом Державного комітету зв'язку та інформатизації України від 17.06.2004 №132 та зареєстрованих в Міністерстві юстиції України 05.08.2004 за № 977/9576.

Порядок визначає вимоги до точок взаємоз'єднання телекомунікаційних мереж операторів, які надають послуги фіксованого міжнародного, міжміського телефонного зв'язку із застосуванням технології IP-телефонії на телекомунікаційній мережі загального користування, та принципи взаєморозрахунків між цими операторами. Дія Порядку поширюється на операторів, що задіяні в єдиному технологічному процесі з надання послуг фіксованого міжнародного, міжміського телефонного зв'язку із застосуванням технології IP-телефонії на телекомунікаційній мережі загального користування.

В порядку представлені терміни, які уживаються в конкретному значені відносно використання технології IP-телефонії.

Автоматизована система розрахунків - сукупність технічних і програмних засобів, методів оброблення інформації та дій персоналу, що забезпечує виконання автоматизованого оброблення облікової інформації та проведення розрахунків.

Оператор IP-телефонії - суб'єкт господарювання, який має ліцензію на здійснення діяльності з надання послуг фіксованого міжнародного, міжміського телефонного зв'язку із застосуванням технології IP-телефонії.

Технологія IP-телефонії - обмін інформацією голосом з використанням мережі передавання даних та IP-протоколу.

Трафік - потік інформації (мова, аудіо, факсимільні сигнали,   
а також сигнали управління, які необхідні під час встановлення або   
завершення з'єднання), що передається мережею, лінією або каналом   
зв'язку.

Шлюз - апаратно-програмний комплекс, що забезпечує взаємоз'єднання двох мереж з різними протоколами.

Рішення про застосування технології IP-телефонії втратило чинність на підставі Рішення Національної комісії з питань регулювання зв'язку № 396 від 02.09.2010.

Відповідно до статті № 27 Закону України «Про зв'язок» та статті № 8 Закону України «Про телекомунікації» визначаються засади охорони таємниці інформації, що передається засобами зв'язку та інформаційної безпеки телекомунікаційних мереж. Охорона таємниці телефонних з'єднань та розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантується Конституцією та Законами України. Зняття інформації з телекомунікаційних мереж заборонено, крім випадків, передбачених законом. Оператори, провайдери телекомунікацій зобов’язані вживати технічних та організаційних заходів щодо захисту телекомунікаційних мереж, засобів телекомунікацій та інформації, що передаються цими мережами та засобами, відповідно до закону [3].

Діяльність в сфері телекомунікацій здійснюється за умови включення до реєстру операторів, провайдерів телекомунікацій, а у визначених законом випадках також за наявності відповідних ліцензій та / або дозволів [4].

Суб'єкти господарювання, які бажають здійснювати діяльність у сфері телекомунікацій, зобов'язані не менше ніж за місяць до її початку подати в національній комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, заяву про включення до реєстру операторів, провайдерів телекомунікацій за формою, що затверджується національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації [4].

У разі якщо вид діяльності, який має намір здійснювати суб'єкт господарювання, потребує отримання ліцензії та / або дозволів, то одночасно із заявою на реєстрацію подається заява та пакет документів на отримання ліцензії та / або дозволів. Рішення про включення підприємства до реєстру операторів, провайдерів телекомунікацій приймається національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, протягом 10 робочих днів з дня реєстрації відповідної заяви суб'єкта господарювання [4].

Повідомлення про включення підприємства до реєстру операторів, провайдерів телекомунікацій національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, направляє заявнику протягом трьох робочих днів з дня прийняття відповідного рішення [4].

Про залишення заяви про включення до реєстру операторів, провайдерів телекомунікацій без розгляду заявник інформується в письмовій формі із зазначенням відповідних підстав протягом 10 робочих днів з дня реєстрації заяви [4].

У разі усунення причин, що стали підставою для залишення заяви без розгляду, суб'єкт господарювання може повторно подати заяву про включення до реєстру операторів, провайдерів телекомунікацій, яка розглядається національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, в порядку, встановленому частиною третьою цієї статті [4].

У разі зміни даних, зазначених у заяві про включення до реєстру операторів, провайдерів телекомунікацій, суб'єкт господарювання зобов'язаний повідомити про них національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації, протягом 30 робочих днів з дня виникнення змін. Рішення про внесення змін до реєстру операторів, провайдерів телекомунікацій приймається національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, протягом 10 робочих днів з дня реєстрації повідомлення суб'єкта господарювання [4].

Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації, має право самостійно вносити відповідні зміни до реєстру операторів, провайдерів телекомунікацій у разі припинення діяльності суб'єкта господарювання в сфері телекомунікацій [4].

Провайдери та оператори телекомунікацій зобов'язані:

- здійснювати діяльність у сфері телекомунікацій відповідно до законодавства за умови включення до реєстру операторів, провайдерів телекомунікацій, а у визначених законом випадках також за наявності відповідних ліцензій та / або дозволів;

- надавати безкоштовний доступ споживачам до телекомунікаційних мереж загального користування для виклику пожежної охорони, Національної поліції, швидкої допомоги, аварійних служб газу і підрозділів екстреної допомоги населенню за єдиним телефонним номером 112, а також для відправки благодійного телекомунікаційного повідомлення [4].

Безкоштовно провайдерам телекомунікацій надаються такі послуги як: послуги телефонного зв'язку або послуги з передачі текстових повідомлень, якщо вони надаються абонентам для надсилання (здійснення) ними благодійного телекомунікаційного повідомлення, послуги з перерахування коштів в якості благодійної пожертви на користь некомерційної організації, в тому числі благодійної організації (крім політичних партій та кредитних спілок), або територіальної громади на виконання благодійного телекомунікаційного відповідного повідомлення на ім'я (здійсненого) таким абонентом та послуги з публічного збору благодійних пожертвувань з використанням благодійного телекомунікаційного повідомлення згідно з договором, укладеним між оператором телекомунікацій та неприбутковою організацією, в тому числі благодійною організацією (крім політичних партій та кредитних спілок), або територіальною громадою [4].

При цьому на суму коштів, перераховану оператором на цілі благодійної діяльності, зібраних публічним збором благодійних пожертв з використанням благодійного телекомунікаційного повідомлення зменшується аванс абонента за телекомунікаційні послуги. Відповідна сума коштів списується з особового рахунку абонента [4].

Провайдери та оператори зобов’язані:

* надавати телекомунікаційні послуги за встановленими показниками якості;
* надавати споживачам вичерпну інформацію, необхідну для укладення договору, а також по телекомунікаційних послуг, які вони надають;
* надавати абонентам послугу перенесення абонентського номера, користування персональним номером у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації;
* вести достовірний облік телекомунікаційних послуг споживачеві;
* забезпечувати правильність застосування тарифів;
* зберігати записи про надані телекомунікаційні послуги протягом строку позовної давності, визначеного законом, та надавати інформацію про надані телекомунікаційні послуги в порядку, встановленому законом;
* не допускати порушень правил добросовісної конкуренції на ринку телекомунікацій;
* першочергово надавати телекомунікаційні послуги підрозділам Міністерства оборони України, Служби безпеки України, Державного бюро розслідувань, Національного антикорупційного бюро України, Служби зовнішньої розвідки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства внутрішніх справ України, Національної поліції, центрального органу виконавчої влади, який забезпечує формування та реалізує державну податкову і митну політику, центральних про рганов виконавчої влади, що забезпечує формування т а реалізують державну політику в сферах цивільного захисту, пожежної та техногенної безпеки, захисту державного кордону;
* забезпечувати готовність своїх телекомунікаційних мереж до роботи в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, в тому числі можливість оповіщення своїх споживачів у цих умовах;
* надавати щорічно до ЦОВЗ інформацію про свої телекомунікаційні мережі для відпрацювання мобілізаційних планів у межах, визначених Кабінетом Міністрів України;
* вести облікову та іншу, визначену законодавством, документацію щодо своїх телекомунікаційних мереж і взаємодії з іншими телекомунікаційними мережами;
* завчасно надавати ЦОВЗ та національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, звіти та інформацію в обсягах, порядку і строки, визначені законодавством;
* оприлюднювати тарифи на телекомунікаційні послуги, що встановлюються самим провайдером, не пізніше ніж за сім календарних днів до їх введення;
* забезпечувати використання наданого номерного ресурсу в терміни, визначені національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації;
* попереджати споживачів про можливе скорочення переліку телекомунікаційних послуг чи відключення їх кінцевого обладнання у випадках і порядку, передбачених правилами надання і отримання цих послуг;
* вживати заходів для недопущення несанкціонованого доступу до телекомунікаційних мереж та інформації, що передається цими мережами;
* на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії;
* невідкладно після отримання екстреного виклику від абонента рухомого (мобільного) зв'язку - дані про його номер і місцезнаходження;
* щомісяця надавати інформацію про абонентські номери фіксованого телефонного зв'язку, прізвища, імена, по батькові, найменування та адреси, що містяться в базі даних;
* виконувати інші обов'язки відповідно до законодавства України [4].

Оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом [4].

У разі якщо оператор, провайдер телекомунікацій встановлює плату за телекомунікаційні послуги згідно з погодинними тарифами, то при розрахунках із споживачами він зобов'язаний враховувати лише повні тарифні одиниці часу. Оператори телекомунікацій зобов'язані за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також в межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Провайдер телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [4].

Оператори та провайдери телекомунікацій не мають права відмовляти в подальшому наданні загальнодоступних послуг інвалідам I і II груп усіх категорій, поточна заборгованість яких за отримані послуги не перевищує трьох мінімальних пенсій за віком. Провайдери телекомунікацій, які надають послуги рухомого (мобільного) зв'язку на території України, за умови укладення відповідної письмового договору між собою зобов'язані надавати можливість абонентам отримувати послугу національного роумінгу [4].

Провайдер телекомунікацій несе майнову відповідальність перед користувачами за ненадання або неналежне надання телекомунікаційних послуг, яка включає:

* за ненадання оплачених телекомунікаційних послуг або надання їх в обсязі менш оплачений, в розмірі сплаченої вартості наданих послуг і штрафу в розмірі 25 відсотків вартості послуг;
* за затримку передавання телеграми, що призвело до її невручення або до несвоєчасного вручення;
* штраф у розмірі 50 відсотків вартості оплаченої послуги, а також повернення споживачу отриманих за послугу грошей;
* за безпідставне відключення кінцевого обладнання, в розмірі абонентської плати за весь період відключення;
* за безпідставні скорочення чи зміну переліку послуг;
* в розмірі абонентської плати за один місяць;
* в інших випадках - у розмірах, передбачених договором про надання телекомунікаційних послуг [4].

У разі не усунення протягом доби з моменту подання абонентом заявки щодо пошкодження телекомунікаційної мережі, яке зробило доступ споживача до послуги або знизило до неприпустимих значень показники якості телекомунікаційної послуги, абонентська плата за весь період пошкодження не нараховується, а оператор телекомунікацій у разі не усунення пошкодження протягом п'яти діб з моменту подання абонентом відповідної заявки сплачує споживачу штраф у розмірі 25 відсотків добової абонентної й плати за кожну добу перевищення цього терміну, але не більше ніж за три місяці [4].

Оператори, провайдери телекомунікацій не несуть майнової відповідальності перед користувачами телекомунікаційних послуг за невиконання або неналежне виконання зобов'язань з надання телекомунікаційних послуг унаслідок дії непереборної сили, викрадення чи пошкодження зловмисниками лінійних та станційних споруд, що використовуються оператором телекомунікацій, або з вини споживача у випадках, передбачених цим Законом [4].

Питання відшкодування завданих споживачеві фактичних збитків, моральної шкоди, втраченої вигоди через неналежне виконання оператором, провайдером телекомунікацій обов'язків за договором про надання телекомунікаційних послуг вирішуються в судовому порядку [4].

Оператори, провайдери телекомунікацій здійснюють свою діяльність відповідно до законодавства про зв'язок.

Віднесення операторів і провайдерів телекомунікацій до операторів і провайдерів, які займають монопольне, тобто домінуюче становище на ринку телекомунікацій, проводиться Антимонопольним комітетом України на підставі законодавства про захист економічної конкуренції [4].

Згідно з статтею № 35 Закону України «Про телекомунікації» визначаються основи захисту інформації про користувача. Оператори, провайдери телекомунікацій повинні забезпечувати і несуть відповідальність за збереженнысть відомостей щодо користувача, що були отримані при укладенні угоди та наданні телекомунікаційних послуг, а також часу отримання послуг, їх тривалості, змісту, маршрутів передавання тощо. Призначені для оприлюднення телефонні довідники, включаючи електронні версії та бази даних інформаційно-довідкових служб, можуть містити інформацію про прізвище, ім'я, по батькові, найменування, адресу та номер телефону користувача у тому випадку, якщо в угоді про надання телекомунікаційних послуг міститься згода споживача на опублікування такої інформації [4].

Під час автоматизованої обробки інформації про користувачів провайдер телекомунікацій забезпечує її захист відповідно до закону. Інформація про користувача та про телекомунікаційні послуги, що він отримав, може надаватися на письмові запити у випадках і в порядку, визначених законом. У всіх інших випадках зазначена вище інформація може поширюватися лише за наявності письмової згоди користувача послуг. Письмовий запит на отримання інформації про користувача телекомунікаційних послуг повинен бути викладений на бланку встановленої форми відповідного органу, підписаний керівником або його заступником цього органу, скріплений печаткою та містити передбачені законом підстави для запиту, посилання на положення законів України, відповідно до яких даний орган має право на отримання інформації [4].

Керівним нормативним документом є «Система автоматизованого телефонного зв’язку для мереж загального користування». Даний Порядок встановлює вимоги щодо маршрутизації даних голосової телефонії провайдерами телекомунікацій на телекомунікаційній мережі загального користування України (ТМЗК) незалежно від технологій, які при цьому застосовуються. Дія цього Порядку поширюється на діяльність суб’єктів ринку телекомунікацій та не поширюється на телекомунікаційні мережі, що не взаємодіють з ТМЗК України. Маршрутизація даних голосової телефонії в ТМЗК України без дотримання вказаних в Порядку вимог не допускається. Технічні вимоги щодо порядку пропускання та маршрутизації даних голосової телефонії встановлює Центральний орган виконавчої влади в галузі зв’язку [4].

У статтях № 31 та 32 Закону України «Про зв'язок» встановлюються правові, організаційні, технологічні та фінансові відносини з міжнародними організаціями зв'язку. Міжнародне співробітництво в галузі зв'язку здійснюється на основі чинного законодавства та відповідних міжнародних договорів України [4].

## 1.3 Статус IP- телефонії в законодавстві США

У США прийнято ділити послуги зв'язку на так звані «базові» (basic services) та «розширені» (enhanced services). За визначенням Федеральної комісії США по зв'язку:

Базові послуги - це забезпечення чистою передачі по лінії зв'язку, яка «прозора» з точки зору взаємодії дії з інформацією клієнта.

Розширені послуги - це послуги, пропоновані поверх існуючих мереж зв'язку, тобто надають базові послуги і:

* використовують комп'ютерні програми, які змінюють формат, зміст, код, протокол або будь-який інший атрибут інформації клієнта;
* надають додаткову або змінену інформацію;
* потребують діалогу користувача для отримання інформації, що зберігається.

Іншими словами, базові послуги - це «передача без змін в електричних сигналах», а розширені - «Створення, видалення і зміна інформації». Перші підлягають суворому регулювання, другі є предметом вільної конкуренції провайдерів Інтернет.

Питання щодо Інтернет-телефонії розглядався Федеральною комісією США по зв'язку на основі аналітичної записки, підготовленої Коаліцією передачі голосу через мережі. На підставі цього документа і раніше розглянутих прецедентів передача голосу через мережі пакетної передачі даних відноситься до «розширеним», оскільки: компресія і придушення пауз, які використовуються в інтернет-телефонії - це є аналіз і видалення «зайвої» інформації, що не відповідає визначенню «базових послуг», оскільки пов'язано зі зміною вихідних даних; пакетизація і додавання протокольної інформації на підставі розділу 64.702 Правил і обмежень комісії, згідно документів 55 RR 2d 104 і 95 FCC 2d 584, є «розширена послуга». Передача голосу через мережі пакетної ПД пов'язана з тимчасовим зберіганням інформації в обладнанні оператора, що суперечить основному ознакою «базових послуг» - «чистої передачі» інформації, оскільки ця затримка не наслідком самої передачі по мережі або встановленого користувачем пріоритету. Компенсація втрачених пакетів і помилок при передачі голосу по мережах пакетної ПД призводить до створення додаткової інформації, що не міститься спочатку в інформації користувача, що автоматичному відносить даний вид послуг до «розширенні». Саме так і працюють сьогодні серйозні постачальники послуг IP-телефонії [5].

Таким чином, для великих оператора IP-телефонія своїм клієнтам сучасного спектру додаткових послуг (голосова пошта, конференція пошук номерів, контроль за розрахунками і багато іншого), які не реалізовуються в традиційної телефонної мережі, і за рахунок яких оператор може отримати додаткові.

Тому, незважаючи на які сьогодні мають в світі місце перевищення обсягів трафіку даних над обсягами голосового трафіку в найближчі роки не очікується будь-яких революційних змін, наприклад, як традиційних технологій передачі голосу.

## 1.4. Правове регулювання IP- телефонії в країнах Європи

В Європі статус IP-телефонії розглядається в контексті дерегуляції і демонополізації послуг традиційної «голосової телефонії». 20 жовтня 1995 р спеціальна комісія ЄС опублікувала Комюніке, адресоване Європейському Парламенту та Раді щодо статусу та виконання Директиви 90/388 / ЄС про конкуренцію на ринках телекомунікаційних послуг. У цьому документі комісія виклала свій підхід до визначення «голосової телефонії», даним у статті 1 Директиви 90/388 / ЄЕС. В цій Директиві описані послуги, які держави-члени ЄС можуть зберігати за своїми регульованими державою телекоммунікаціонними операторами.

У зв’язку появи нових технологій передачі голосу через Інтернет комісія прийняла нове Доповнення до Комюніке з приводу таких послуг. У документі OJ № С6 від 10.1.1998 дається наступна оцінка послуг інтернет-телефонії на підставі виділення «голосової телефонії», даного вищевказаної Директиви 90/388 / ЄС: «Комісія вважає, що визначення «Голосова телефонія» в Директиві 90/388 / ЄС, що розглядається разом з існуючими прецедентами, дає хороше керівництво для оцінки позиції послуг по голосовому повідомленням в Інтернеті в умовах близько-лібералізаційна ситуації по відношенню до наявного законодавства. Послуги інтернет-телефонії не можуть розглядатися як «голосова телефонія» в тій трактуванні, яка викладена в Директиві і, таким чином, вони вже переходять в, так звану, «вільну зону» дерегулювання [5].

У підсумку до цього документа також сказано: «на підставі того, що голосове повідомлення в Інтернеті розглядається як послуга, відмінна від послуги «голосовий телефону» в трактуванні Директиви, по ньому не може бути затребувано ніяких додаткових зборів і ліцензій від провайдерів послуг Інтернет».

## 1.5. Висновок по розділу

Істотні недоліки в сучасному українському законодавстві викликають значні труднощі у регулюванні та захист телекомунікаційних систем, зокрема систем IP-телефонії. Системи VoIP майже повністю регулються Законом «Про телекомунікації» та Законом «Про зв’язок», оскільки існує невелика кількість документів, що регулюють саме систему IP-телефонії, та навіть вони поступово втрачають свою чинність. Телефонія, побудована на основі глобальної мережі, потребує конкретних стандартів та правових бар’єрів, які повинні юридично затвержуватися. Загалом VoIP телефонія тільки розвивається на території України і на даний час її можна вважати майже нерегульованою та неконтрольованою.

Стандарти не були прийняті для використання VoIP за допомогою агентств громадської безпеки. В результаті, дані, закодовані за допомогою пристрою одного виробника буде, як LY не може бути береться стверджувати за допомогою пристрою іншого виробника.

Так як оператори IP-телефонії складають сильну конкуренцію традиційним операторам зв'язку, останні абсолютно обгрунтовано бачать у розвитку IP-телефонії пряму загрозу своїм прибуткам. Природно, вони намагаються цього розвитку перешкодити, використовуючи всі доступні їм способи. Одним з таких способів є державні інструкції, що обмежують діяльність конкурентів. Деякі монополісти, які безпосередньо пов'язані з владою, приймають угодні їм закони. Цим можна пояснити різке втрачання чинності багатьох законів щодо дій системи VoIP. Internet Protocol (IP) мережу підтримуються всі види мереж - корпоративний, приватний, громадський, кабель, і навіть провід- менше мереж. Не обманюйте «Інтернет» частина абревіатури. VoIP буде працювати над будь-яким типом мережі. В даний час в корпоративному секторі приватного виділений варіантом мережі є кращим типом.

Кілька функцій VoIP, такі як голосова пошта і переадресація виклику, які були популярними в світі протягом досить довгого часу. З іншого боку, інтеграція даних, голосу і відео додатків для запуску через єдину мережу і можливість працювати з бездротовими телефонами є пізніші нововведення зробили можливим завдяки IP-телефонії. В результаті, багато нові функції в рамках IP-телефонії стали доступні.

Щодо захисту дана система може також регулюватися законами «Про основні засади забезпечення кібербезпеки України» та «Про захист інформації в автоматизованих системах». Система захисту будується на основі НД ТЗІ, а саме як система захистуінформації в АС 3. Також існують безліч готових рішень щодо захисту таких систем, однак конкретних єдиних стандартів або рекомендацій не існує.

Отже, для захисту VoIP можна застосовувати ті ж самі технічні та організаційні рішення, які були розроблені для стандартних ситуацій. Але слід зазначити, щo не можна бездумно копіювати чужі системи — вони розроблялися для інших умов та систем.

# РОЗДІЛ 2. ОСНОВИ ЗАХИСТУ МЕРЕЖ IP-ТЕЛЕФОНІЇ

## 2.1 Поняття IP-телефонії, базових принципів та протоколів

На сьогоднішній день кількість інформації, що передається та оброблюваної інформації в одиницю часу в Світі досягла на стільки великих обсягів, що проконтролювати чи відстежити передачу даних дуже складно. Саме з цих міркувань на передачу інформації накладається додаткова важлива вимога — високий рівень безпеки передачі даних. Особливо критично дане питання поставлено по відношенню до мульти медіа даних, де часто виникає необхідність у миттєвій передачі, а обсяг інформації відносно великий.

Життя сучасної людини складно уявити без телефонних дзвінків, адже ми використовуємо дзвінки для спілкування з рідними і близькими, ділові контакти, отримання інформації. Більшість людей традиційно використовують пропозиції операторів мобільного та стаціонарного зв'язку. Однак вартість їх послуг часто змушує обмежувати кількість і обсяг контактів. Постійне удосконалення та розповсюдження мережі Інтернет спровокувало зародження нового виду з’язку, що базується на використані протоколу IP, який здатен перетворювати голосовий пакет даних у цифровий сигнал. Новий вид зв’язку має назву IP-телефонія, та є альтернативою вищевказаних видів зв'язку. Використання даної технології дозволило виконувати перетворення медіа-коммунікацій у зручній, високоякісний та універсальний спосіб спілкування, який до того ж є дешевшим і доступним практично кожному.

IP-телефонія – сукупність комунікаційних протоколів, технологій та методів, що забезпечують традиційні для телефонії двостороннє голосове повідомлення, а також відеоповідомлення мережею Інтернет або іншими IP-мережами. Станом на сьогодні більшість підприємств застосовують VoIP як для зовнішнього, так і внутрішнього зв’язку. Застосування систем IP-телефонії дозволяє компаніям значно знизити вартість дзвінків, особливо міжнародних, та інтегрувати телефонію сервісами Інтернету, надавати інтелектуальні послуги. Технологія приносить з собою кілька нових можливостей, які дійсно змінюють зміст фрази телефонний дзвінок. В принципі, VoIP означає «голос передається по цифровій мережі.»

VoIP часто називають IP-телефонія тому що він використовує найостанніші VoIP часто називають IP-телефонія тому що він використовує найостанніші VoIP часто називають IP-телефонія тому що він використовує найостанніші інновації з популярними і знайомими протоколами IP, щоб зробити можливі розширені голосові комунікації по всьому підприємству. IP мережі підтримує корпоративні, приватні, державні, кабель, і навіть бездротові мережі. IP-телефонія об'єднує багатьох місцях, в тому числі організації мобільного workers- в єдину мережу конвергентних комунікацій. На відміну від комутованих ТфОП, які завжди вимагають використання комутованої телефонної мережі загального користування (PSTN), технологія VoIP дозволила телефонію та інші нові і нові функції і сервіси для роботи з виділеним і бездротовим мережам Якщо враховувати навіть вашої комп'ютерної мережі. Ці нові типи мереж використовують з комутацією пакетів протоколів. З комутацією пакетів VoIP поміщає голосові сигнали в пакети. Поряд з мовними сигналами, пакети VoIP включають в себе як мережеві адреси відправника і одержувача. пакети VoIP може пройти будь-якою VoIP-сумісної мережі. По дорозі, вони можуть вибирати альтернативні шляхи, так як адреса призначення включений в пакет. Маршрутизації пакетів не залежить від будь-якого конкретного мережевого маршруту. Оскільки VoIP сумісний і портативний, що робить можливим безліч нових додатків для кінцевих користувачів, які перевизначення, як ви можете зробити телефонні дзвінки. Оскільки VoIP є вельми «роботи в мережі," корисно розрізняти два основних типи мережі, які використовуються в більшості, якщо не у всіх компаніях.

Основними вимогами до таких мереж є маршрутизатор, пропускна здатність каналу, VoIP-обладнання, якість сервісу, а також наявність обладнання. VoIP є мережевими додатками, які відносяться до прикладного рівня. Він є технологія, який призначений для передачі медіа на базі пакетів в IP-мережах. Деякі протоколи прикладного рівня, такі як HTTP, FTP й інші протоколи є відкритими (з загальним доступом). Тому ці протоколи доступні для будь-якого браузера, який підтримує протокол HTTP та FTP (HTTP призначений для перепосилання веб-сторінок, а FTP – файлів, що розміщується на сайтах). Деякі протоколи VoIP є загальнодоступними, а інші – приватними або закритими, тому вони не є доступними для всіх прикладних програм.

На відміну від класичної телефонії, де використовується комутація каналів, ІР-телефонія базується на мережевих протоколах з комутацією пакетів. У процесі передачі даних по IP-мережі вони проходять через певну кількість недостатньо захищених серверів, до того ж з’єднаних між собою незахищеними каналами.

Водночас ІР-телефонія певним чином відрізняється і від звичайної передачі даних ІР-мережами. Це пов’язано з необхідністю виконання аналого-цифрових перетворень даних в реальному часі. Зважаючи на необхідність дотримання вимог щодо якості зв’язку, такі перетворення, включаючи стискання, шифрування та інші, повинні відбуватися за мінімально короткий час. Від того, наскільки існуючі системи відповідають усім цим вимогам, залежать, значною мірою, перспективи подальшого розвитку IP-телефонії.

Передача голосу через традиційні IP-мережі з комутацією пакетів - одна з найшвидших тенденцій у телекомунікаціях. Хоча більшість комп'ютерів можуть надавати VoIP і багато пропонують додатки VoIP, термін "VoIP over IP", як правило, пов'язаний з обладнанням, яке дозволяє користувачам набирати телефонні номери та спілкуватися з сторонами на іншому кінці, які мають систему VoIP або традиційний аналоговий телефон. Коли пакети прибувають в пункт призначення локальної мережі, в перервах пристрої крайовими вниз пакетів VoIP і пересилає їх нарешті на сервер, який керує послугами IP-телефонії в локальній мережі. З цієї точки, інша частина процесу аналогічна послуг IP-телефонії. Телефон дзвонить. Людина, якого називають відповідями, і віртуальний канал встановлюється між абонентом і особами, які отримують викликом. Замість того, щоб підтримувати окрему мережу для комп'ютерів і телефонів, компанії можуть зійтися обидва цих мережі в єдину мережу з використанням IP-телефонії та VoIP.

Добре спроектований мережевий порт IP може перенаправляти дані оминаючи перевантаження мережевих шляхів, тому цілісність зв'язку підтримується, що означає підвищену надійсність. Протоколи IP для маршрутизації даних оснащені покращеною масштабованістю для підтримки великого числа користувачів. На основі радіо сумісності обладнання часто використовується для з'єднання старих або різних приватних систем радіозв'язку, якщо не можуть бути використані традиційними методами телекомунікацій. Голос і передача інших даних можуть бути об'єднані в єдину, добре спроектовану мережу.

Побудова мережі VoIP доволі проста та представляє собою звичайну IP-мережу, приклад такої мережі зображено на рис. 2.1. Ініціатором зв’язку є комп’ютер або IP-телефон, де повідомлення оцифровується та стискається. Наступний шлях повідомлення проходить через сервер АТС 1, який забезпечує передачу даних мережею Інтернет. Сервер АТС 2 приймає через Інтернет дані та передає до комп’ютера, IP-телефону або шлюзу, де повідомлення перетворюється на спеціальні сигнали, які коректні для кінцевого пристрою. Потім відновлюється та озвучується через кінцевий пристрій. Кінцевими пристроями при цьому можуть бути комп’ютер, телефон або факс. IP-телефон являє собою пристрій, який має вбудовану підтримку VoIP і дає можливість підключатися безпосередньо до безпосередньо до мережі IP, що дозволяє пристрою мати дуже якісний зв’язок. Сервер забезпечує управління і адміністративні функціх для підтримки маршрутизації викликів по всій мережі. Після того, як зв’язок буде встановлений, дані будуть оцифровані, а потім передаються по мережів якості IP-пакетів. Мовні зразки інкапсулюються в RTP та UDP.



Рис 2.1 Загальна схема роботи мережі IP-телефонії

Основний принцип дії серверів IP-телефонії такий: з одного боку, сервер пов'язаний з телефонними лiнiями та може з'єднатися з будь-яким телефоном світу. З iншого боку, сервер пов'язаний з Iнтернетом та можезв'язатися з будь-якимкомп'ютерoм в свiтi, завдякийого підключенню до глобальної мережі. Сeрвeр приймає cтандаpтний телефoнний сигнал, оцифровує його, значно стискaє, рoзбиває на пакети і вiдправляє через Iнтернет з використанням протоколу TCP/IP за призначенням. Для пакетів, які прибувають з мережі на телефонний сервер i що йдуть в телефонну лiнiю, операцiя відбувається в зворотному порядку. Обидві представлені операції (вхід сигналу в телефонну мережу і його вихід з телефонної мережі) відбуваються майже одночасно, що забезпечує повнодуплексну розмову.

На основі даних базових операцій можна побудувати багатоішних різних конфігурацій. Наприклад, дзвінок телефон-комп'ютер або комп'ютер-телефон може забезпечувати один сервер телефонії. Для організації зв'язку типу телефон-телефон потрібно два сервери. Тобто принцип роботи VoIP полягає в тому, що при здійсненні дзвінка голосовий сигнал перетворюється в стисненний кодований пакет даних. Після стиснення відбувається пересилання таких пакетів по мережі. При отриманні пакетів отримувачем, вони декодуються в оригінальні голосові сигнали [6].

IP-телефонія складається з трьох рівнів: фізичний, канальний, мережевий, транспортний.

На фізичному рівні відбувається передача потоку бітів по фізичному середовищу через відповідний інтерфейс. У якості середовища найчастіше використовується вита пара категорії 5, оптичне волокно або коаксиальний кабель.

Канальний рівень поділяється на два підрівні: MAC, який забезпечує взаємодію з фізичним рівнем та LLC, що обслуговує мережевий рівень. На канальному рівні працюють комутатори [6].

На мережевому рівні відбувається маршрутизація, тобто основними пристроями даного рівня є маршрутизатори. Саме на мережевому рівні визначається шлях даних до отримувача з визначеною IP-адресою. Основним протоколом, щомаршрутиризується є IP, на основіякого і побудована IP-телефонія.

Транспортний рівень характеризується сегментацією даних додатками вищого рівня, забезпечення наскрізного з'єднання та гарантія надійності даних. Основні протоколи рівня: UDP та RTP. UDP забезпечує негарантоване отримання данних. Його суть полягає у тому, що при відправленні та отриманніданих не потребується ніяких підтвержень. Основне ж завдання RTP – присвоєння кожному вихідному пакету тимчасові позначки, що оброблюються на стороні призначення пакетів.

Рівні VoIP завершуються рівнями даних. На цих рівнях працює один з найважливіших протоколів телефонії – SIP. Даний протокол призначений для встановлення, зміни та завершення сеансів зв'язку. SIP є незалежним від технологій транспортного рівня, однак рекомендується вствновлювати сеанс за допомогою саме транспортних протоколів.

SIP протокол дозволяє двом системам ініціювати та керувати медіапотоком між кінцевими точками. SIP підтримує аутентифікацію, ідентифікатор абонента та контроль потоку медіа.

SIP- канали налаштовані в sip.conf. SIP- дзвінки, як і будь-який інший виклик, керуються планом набору номера, який знаходиться в extensions.conf. Усі дзвінки надходять на канал, наприклад, на SIP- канал. Вхідний SIP- дзвінок починається з підключення до SIP- каналу. Існує файл конфігурації для кожного типу каналу, наприклад sip.conf для SIP- каналів. Ось приклад sip.conf. Цей приклад має єдиний контекст, названий загальним. Контекст в даному прикладі пов'язує цей sip.conf контекст контекст в extensions.conf. Будь-який дзвінок на SIP- каналі буде за замовчуванням оброблятися контекстом з SIP у extensions.conf. Коли пакети прибувають в пункт призначення локальної мережі, в перервах пристрої крайовими вниз пакетів VoIP і пересилає їх інтер нарешті на сервер, який керує послугами IP-телефонії в локальній мережі. З цієї точки, інша частина процесу аналогічна послуг IP-телефонії. Телефон дзвонить. Людина, якого називають відповідями, і віртуальний канал встановлюється між абонентом і особами, які отримують викликом. Замість того, щоб підтримувати окрему мережу для комп'ютерів і телефонів, компанії можуть зійтися обидва цих мережі в єдину мережу з використанням IP-телефонії та VoIP.

В IP-телефонії було прийнято застосовувати стандарт H.323, що був розроблений в 1996 році. В стандарті описане обладнання, мережеві служби та термінальні пристрої, призначені для здійснення аудіо або відео зв'язку в мережах з комутацією пакетів. Для кожного пристрою даного стандарту обов'язкова підтримка обміну медіа інформації. Вказаний стандарт будується на принципах:

* незалежність платформи;
* стандарти кодування аналогових даних;
* управління смугою пропускання;
* гнучкість та сумісність.

Згідно стандарту H.323 основними елементами мережі VoIP є шлюз, диспетчер та монітор [7].

Шлюз (Gateway) –базовий пристрій, що підключений до IP-мережі та до телефонної мережі. Даний пристрій не є обов’язковим компонентом. Він є необхідним тільки при умові, якщо є потреба встановити з’єднання з терміналом іншого стандарту. До його функцій входять:

* відповідь на виклики виклику абонента;
* встановлення з'єднання з віддаленим шлюзом;
* забезпечення та встановлення зв'язку з викликаним абонентом;
* стиснення, пакетування та відновлення сигналу-голосу.

Таким чином, шлюз є основною та невід'ємною частиною архітектури IP-телефонії, безпосередньо з'єднуючий телефонні мережі з мережею IP.

Шлюзи різних виробників відрізняються способом підключення до телефонної мережі, ємністю, апаратною платформою, реалізованими кодеками, інтерфейсом та іншими характеристиками. Але все вони виконують перераховані вище функції, які є базовими для технології IP-телефонії.

Монітор - необов'язковий додатковий модуль мережі IP-телефонії, підключається тільки до IP-мережі, що використовується для віддаленого настроювання та підтримки інших пристроїв мереж-шлюзів і диспетчерів. Монітор є інтерфейсом для віддаленого налаштування IP-мережею параметрів шлюзів і диспетчерів мережі IP-телефонії.

Монітор є зручним засобом конфігурування та адміністрування мережі. В перших шлюзах для цього просто використовувалися стандартні мережеві програми. Пізніше в цілях оптимізації роботи виробники обладнання IP-телефонії стали випускати власні додатки для цих цілей.

Мережі IP-телефонії надають можливість зв’язку чотирьох різних типів:

1. «телефон-телефон», в цьому випадку виклик здійснюється з звичайного телефоного апарату до АТС, на один з виходів якої підключений шлюз VoIP, та IP-мережею доходить до іншого шлюза, що здійснює зворотні перетворення;
2. «комп’ютер-телефон», де комп’ютер, що має програмне забезпечення IP-телефонії підключається до мережі IP, шлюз телефонії має з’єднання через АТС з звичайним телефоном;
3. «комп’ютер-комп’ютер», в такому випадку зв’язок встановлюється через мережу між двома комп’ютерами, що має програмне забезпечення IP-телефонії;
4. «браузер-телефон», з’єднання за допомогою клавіші на веб-сторінці.

Протоколи забезпечують реєстрацію IP-пристрою на сервері провайдера, виклику або переадресацію виклику, встановлення голосового або відео з’єднання, передачу імені та номера абонента. Основними протоколами технології є:

* SIP - протокол сеансового встановлення з’язку, що забезпечує передачу голосу, видео, повідомлень систем миттєвого обміну повідомлень та похідного навантаження, для сигнализації зазвичай використовується порт 5060 UDP. Підтримується контроль присутності.
* H.323 - протокол, більш зв’язаний з системами традиційної телефонії, ніж SIP, сигнализація по порту 1720 TCP, та 1719 TCP для регістрації терміналів на гейткипері.
* IAX 2 - через 4569 UDP-порт та сигналізація, і медіатрафік.
* Jingle
* MGCP (MediaGatewayControlProtocol) - протокол управління медіашлюзами.Являж собою протокол з’вязку в розподілених системахVoIP, де передача голосу відбувається по IP-протоколу.
* Megaco/H.248 - протокол управління медіашлюзами, развиток MGCP.
* SIGTRAN - протокол тунелювання PSTN - сигналізації ОКС-7 через IP на програмний комутатор (SoftSwitch).
* SCTP(StreamControlTransmissionProtocol) - протокол для організації гарантированного постачання пакетів в IP-мережах.
* SGCP(SignalGatewayControlProtocol)– протокол управління шлюзами сигналізації, що забезпечує доставку сигнального пакету до пункту призначення.
* SCCP (SkinnyCallControlProtocol) - закритий протокол управління терміналами (IP-телефонами и медіашлюзами) в продуктах компанії Cisco.
* Unistim - закритий протокол передачі сигнального трафіку в продуктах компанії Nortel [8].

## 2.2 Стандарти IP-телефонії та механізми їх безпеки

Відсутність єдиних загально-прийнятих стандартів в галузі Інтернет телефонії не дозволяє розробити і універсальні рекомендації щодо захисту пристроїв системи. Кожна корпорація або виробник вирішує за власним розсудом завдання забезпечення безпеки шлюзів і диспетчерів, що призводить до необхідності ретельного їх вивчення перед вибором адекватних заходів для захисту.

H.323 - протокол, який дозволяє побудувати VoIP-систему від початку і до кінця. H.323 включає в себе ряд специфікацій, в т.ч. і H.235, яка реалізує деякі механізми безпеки (аутентифікацію, цілісність, конфіденційність і неможливість відмови від повідомлень) для голосових даних. Аутентифікація в рамках стандарту H.323 може бути реалізована як за допомогою алгоритмів симетричною криптографії (в цьому випадку не потрібно ніякого попереднього обміну між пристроями і не так інтенсивно навантажується центральний процесор), так і за допомогою сертифікатів або паролів. Крім того, специфікація H.235 дозволяє використовувати в якості механізму аутентифікації IPSec, який також рекомендується до застосування і в інших стандартах IP-телефонії. Після установки захищеного з'єднання, яке відбувається через 1300 tcp-порт, вузли, які беруть участь в обміні голосовими даними, обмінюються інформацією про метод шифрування, яке може бути задіяно на транспортному (шифрування пакетів RTP-протоколу) або мережевому (за допомогою IPSec) рівні.

До стандарту H.323 входять рекомендації ITU-T, що визначають пріорітетність функціонування абонентських терміналів в мережах з ресурсом, що не можуть гарантувати якість обслуговування (QoS). Стандарт H.323 не має відношенння до протоколу IP, незважаючи на це, більшість реалізацій було здійснено на цьому протоколі. Набір рекомендацій визначає мережеві компоненти, протоколи і процедури, які дозволяють організозувати мультимедійний зв’язок в пакетних мережах.

SIP протокол, який досить схожий на HTTP, використовуваний абонентськими пунктами для встановлення з'єднання (не обов'язково телефонного, а й, наприклад, для ігор), не має серйозного захисту і орієнтований на застосування інших додаткових рішень. Як механiзм аутентифiкації RFC 2543 пропонує кілька варiантів і, зокрема, мінімальну стандартну аутентифiкацiю, так само як в HTTP, і аутентифiкацiю на базі PGP. Намагаючись усунути слабку захищеність даного протоколу, Майкл Тoмас з компанiї Cisco Systems розрoбив проект стандaрту IETF, нaзваний "SIP securіty frаmewоrk", що oписуєзoвнішні і внутрішні загрози для протоколу SIP та способи захисту від них. Зокрема, до таких способів відноситься захист на транспортному рівні за допомогою протоколу TLS або технології IPSec. До речі, компанія Cisco у власній архітектурі безпеки корпоративних мереж SAFE, дуже велику увагу приділяє практичним питанням щодо захисту IP-телефонії.

Протокол SIP є протоколом передачі даних, де описується спосіб завершення сеансу конкретного користувача, а також обмін мультимедійних даних. Переважна кількість користувачів даного протоколу використовають 5060 порт TCPабоUDP для з’єднання елементів мережі. Основним завданням SIP-протоколу є встановлення з’єднання при виклику, тобто він визначає правила узгодження відкриття каналі обміну між користувачами для безпосередньої передачі даних. Даний протокл має клієнт-серверну архітектуру.

Стандарт MGCP, який визначений у RFC 2705 і не здатен застосовуватися на кінцевих пристроях, оскільки шлюзи MGCP можуть працювати як з компонентами, що підтримують H.323, так і з компoнентами, що підтримують SIP, використoвує для захисту голoсових даних протокол ESP специфікації ІPSec. Може також використовуватися і протокол AH, але за винятком мереж IPv6), що забезпечує аутентифікацiю та ціліснiсть даних і захист від повторeнь, перeданихмiж шлюзами. У той же час, протокол AH не забезпечує конфіденційності даних, яка досягається застосуванням ESP (поряд з іншими трьома захисними функціями) [9].

Багато найбільших світових телефонних компаній зобов’язалися замінити існуючі системи з комутацією мікросхем на передачу голосових передач через IP-системи. Багато телефонних компаній вже багато разів транспортують значну частину свого трафіку за допомогою мережі IP. Багато дзвінків, здійснених через телефонне супутнє обладнання, вже маршрутизуються через IP.

Голосова передача через комутаційні пакети через IP-системи в принципі настільки ж ефективна, як і системи з комутацією синхронних схем, але лише нещодавно вони досягли такого ж рівня надійності, що і телефонна мережа загальнодоступних комунікацій, або власне обладнання АТС . З винаходом та реалізацією RTP та SIP голос через IP має технологічну базу для застарілого зв'язку з комутацією загальнодоступних телефонних мереж.

## 2.3 IP-телефонія на базі АТС Asterisk

Asterisk PBX — [відкрита](https://uk.wikipedia.org/wiki/Відкрите_програмне_забезпечення) комунікаційна платформа, що використовується для розгортання програмних [АТС](https://uk.wikipedia.org/wiki/Автоматична_телефонна_станція), систем голосового зв'язку, [VoIP](https://uk.wikipedia.org/wiki/VoIP)-шлюзів, організації IVR-систем (голосове меню), [голосової пошти](https://uk.wikipedia.org/wiki/Голосова_пошта), телефонних конференцій і call-центрів.

Налаштування та програмування здійснюється за допомогою спеціальних механізмів, таких як: диалплан, AGI, AMI, конфігурація з баз даних [10].

Розширення виконуючих функцій також можливе за допомогою інших мов програмування, за допомогою внесення коду в новий модуль.

Програмне забезпечення Asterisk перетворює недорогий сервер архітектури ПК під управлінням Linux або Unix у надійну, складну, повнофункціональну корпоративну телефонну систему. Оскільки Asterisk безкоштовний і працює на стандартній для ПК платформі, система Asterisk обійдеться вам набагато дешевше, ніж будь-яка традиційна АТС . Оскільки він надійний, вільний та ефективний, а також тому, що він базується на сучасних Інтернет- протоколах, Asterisk замінить багато застарілих телефонних систем на ринку.

Asterisk є сучасною цифровою телефонною станцією, що працює по протоколу SIP. IP АТС має великий функціонал, що постійно розвивається. Сервер Asterisk управляє дзвінками по чотирьох лініях та всіма телефонами та факсимільними апаратами на підприємстві. Будь-який вхідний дзвінок на четвертому рядку спрямовується на факсимільний апарат. Вхідний абонент, що набирає перший рядок, чує голосове меню.

Основні переваги системи Asterisk:

* моніторинг викликів в режимі online та запис розмов, можливість комутувати того чи іншого абонента через панель управління;
* голосові вітання, динамічні черги росподілення вхідних дзвінків;
* відсутність необхідності в додаткових ліцензіях та платежів телефонії;
* можливість інтегрування зі сторонніми системами, використовючи AMI/API інтерфейс, наприклад CRM системами и базами даних;
* розподілення дзвінків.

Система Asterisk є однією з найстабільніших і функціональних систем обробки викликів з усіма можливостями VoIP телефонії. А найголовніше програмне забезпечення Asterisk є повністю безкоштовним і не вимагає від замовника покупки ніяких додаткових ліцензій, поширюється воно за ліцензією OpenSources GPL. Asterisk є дуже гнучким продуктом, що дозволяє налаштувати його практично під будь-які завдання. Є дійсно революційним продуктом, що дозволяє не пропустити не одного дзвінка. В якості робочої станції (сервера) для Asterisk може використовуватися звичайний персональний комп'ютер [11].

Базується система на операційній системі Linux, що вже говорить про її безпеку і надійність. Asterisk працює з базами даних та дозволяє здійснити певні дії, наприклад обмеження прав на номер або маршрутизаційні дії з системою за допомогою SQL. Рішення на базі даної платформи обертає звичайний комп’ютер комунікаційний сервер. Asterisk оснащує IP-АТС системою, прокладає канали VoIP, серверами для конференцій та іншими довільними рішеннями. Широко використовується у сфері малого та великого бізнесу, кол центрів, компаній, що займаються перевезеннями та урядовими організаціями по всьому Світі. Безкоштовний та з відкритим кодом рішення Asterisk спонсорується компанією Digium. Найчастіше розгортається системними інтеграторами та розробниками, може виступати основою для повноцінної комунікаційної інфраструктури підприємства.

## 2.4 Проблеми захисту IP-телефонії від загроз

VoIP дозволяє використовувати будь-яку IP–мережу як засіб організації та проведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу. Станом на сьогодні IP–телефонія постає деяким стандартом у телефонних комунікаціях — забезпечує зручність, надійність та відносно невисоку вартість порівняно з аналоговим зв’язком. Також вона дозволяє підвищити ефективність роботи державних установ і дає змогу здійснювати раніше недоступні операції такі, як інтеграція з різними бізнес-додатками.

Незважаючи на те, що телефонія на базі VoIP не тільки дешевша, а й набагато безпечніша, все ж таки вона має певні вразливості. Єдиний захист звичайної телефонної мережі - фізична ізоляція. Незахищені спеціальним чином VoIP-мережі прослухати, в принципі, можна, але зробити це буде значно важче, ніж просто причепивши два проводка до телефонної лінії. Спеціальна ж захист, що зводить можливість прослуховування до мінімуму, являє собою, тим не менш, досить просту і дешеву систему стандартного шифрування, що використовується в мережах даних та спеціальні додатки або налаштування існуючих. Досягти такого ж рівня безпеки в звичайній телефонній мережі майже неможливо і, вже точно, набагато дорожче. Кожен телефонний апарат в звичайній телефонній мережі, сконфігурированною за принципом "точка-точка", підключений до певного комутатора. Будь-яке порушення роботи цього пристрою повністю блокує роботу телефону. Мережі VoIP можуть бути організовані за гнучкою розподіленої схемою "три крапки-крапки". Програмний комутатор VoIP може бути, при необхідності, легко встановлений в іншому місці без зміни роботи системи в цілому. Потік голосових даних в будь-який момент може бути направлений за іншим маршрутом. Грамотно спроектована VoIP-мережу просто не має унікальних вузлів, відмова яких повністю блокує обслуговування. Цього достатньо для запобігання блокування окремого телефонного апарату.

Технологія VoIP чуттєвіша до проблем пропускної спроможності мережі, ніж більшість технологій, що відносяться до мережевої інфаструктури. Використання даної технології до традиційної мережі передачі данних запроваджує нову вимогу безпеки, що називається якістю обслуговування (QoS).

Параметр QoS описує спроможність конкретної мережі розподіляти пріорітети трафіку для того, щоб незалежно від використання смуги пропускання в інших технологіях, голосові пакети VoIP мали характеристики такі як чіткість та непреривність розмови.

Наприклад, більшість некомерційних користувачів мали змогу помітити, що при загрузці файлу з Інтернету, що має великий розмір, будь-які поточні розмови через VoIP іноді стають неякісними доки загрузка не завершиться.

Доступність мережі – суттєва вимога безпеки в мережі передачі данних, що також впливає на роботу технології VoIP.

Очевидно, що при умові простоювання мережі передачі данних через DoS-атаки або несправного маршрутизатора VoIP інфаструктура також буде потерпати від простоїв мережі.

QoS та доступність мережі найчастіше є достатньо складними для ІТ-персоналу для забезпечення цих умов у межах всього підприємства, без необхідності турбуватися про ненавмисні внутрішні загрози, таких як перевищення смуги пропускання, ресурс виснаження, збій або неправильна конфігурація мережевого пристрою. VoIP-пакети повинні пересуватися IP-мережею, що є сама собою ненадійную. Деякі дані можуть бути видалені в результаті перевантаження мережі, або пошкодження ланцюга пакетів. Крім того, для трафіку в реальному часі повторна передача втрачених пакетів на транспортному рівні не є практично-ефективною через додаткові затримки.

Незважаючи на все, система IP–телефонії схильна до різних атак: до черв’яків і вірусів, до DoS–атак, до несанкціонованого віддаленого доступу та іншим загальним загрозам, яким притаманні:

* реєстрація чужого терміналу, що дає можливість здіснювати дзвінки за чужий рахунок;
* підміна користувача, що дає можливість порушнику перенаправляти дзвінки;
* внесення змін до голосового або сигнального трафіку;
* зниження рівня якості голосового трафіку;
* перенаправлення та перехоплення голосового або сигнального трафіку;
* підробка голосових повідомлень;
* відмова в обслуговуванні;
* віддалений несанкціонований доступ до інфраструктури IP-телефонії.

Але це навіть не ввесь перелік можливих проблем, пов’язаних з викорис- танням IP–телефонії. Альянсом щодо безпеки VoIP був розроблений документ, в якому детально описується широкий спектр загроз IP–телефонії, який, крім технічних загроз, містять обман користувачів та непотрібний спам. Питання про забезпечення інформаційної безпеки необхідно вирішувати на етапі підготовки проекту IP–телефонії, оскільки саме на цьому етапі необхідно домовитися про те, які механізми захисту мережевої інфраструктури доцільніше використовувати у мережі.

На сьогоднішній день одним з основних бар’єрів на шляху впровадження VoIP – впевненість, що розмова така ж чітка і без перешкод, як і з традиційної телефонії загального користування. Низька якість при використанні мереж IP-телефонії може призвести до пропущення телефонних розмов, поганого звучання або уривчатості і стати нерозбірливим до такої міри, що співрозмовники не матимуть іншого вибору, як завершити розмову. Мережеві атаки та проблеми перевантаження також можуть впливати на аспект сигналізації VoIP, затримучи тональний сигнал про готовність або початкове налаштувння виклику після набору.

Алгоритми стиснення носіів (кодеки), наявні в технології VoIP, є дуже чуттєвими до мережевих затримок. В залежності від конкретних алгоритмів стиснення, односекундний збій мережі може спотворити декілька секунд мови.

При погіршення якості викликів можна виділити три основні причини:

* затримка в мережі, джітер та втрата пакетів;
* порушення передачі через обробку голосових пакетів;
* час односторонньої передачі.

Мережева затримка являє собою час, необхідний для проходження пакета від одного співрозмовника до іншого. В традиційній телефонії зазвичай існує невелика затримка мови при міжнародних дзвінках, причино цього є відстань, що проходить дзвінок. На затримку VoIP можуть вплинути такі чинники, як: фізична відстань мереж кабельного зв’язку, велика кількість проміжних переходів в Інтернет, перевантаження мережі, а також погану або повністю відсутню систему визначення внутрішніх приорітетів смуги пропускання.

Джітер – небажані періодичні випадкові спотворення під час передачі данних. Найчастіше він трапляється, коли пакети відправляють розповідачем з постійною швидкістю, але приймаються слухачем зі змінною, що приводить до преривистої розмови або з затримкою. Виникає зазвичай в мережах без смуги пропускання або QoS керування, в результаты чого трафік VoIP має один пріорітет з іншим трафіком данних. Джітер більш ніж 25 мілісекунд буде відчутним для слухача. Багато додатків та пристроїв IP-телефоніх намагаються компенсувати цю проблему шляхом створення буфера «тремтіння». Буфер джітера зберігає невелику кількість пакетів VoIP, що були отримані першими, для того, щоб нормалізувати пакети, які були отримані пізніше. Такі буфери можуть бути ефективними при умові, якщо величина тремтіння складає менш ніж 100 мілісекунд. Аналогічним шляхом, велика кількість Інтернет-провайдерів вбудовують максимальні обмеження джітера у послуги.

Документації про кодекиствержують, що одностороння затримка більш ніж на 150 мілісекунд буде помітна для сторін, які ведуть розмову. Найбільш ймовірно, що данний тип затримки мережі Інтернет-провайдера, яким користується співрозмовник. Багато Інтернет-сервісів підтримують угоду про рівень обслуговування для забезпечення мінімальної затримки власної мережі.

Втрата пакетів в мережі передачі данних у більшості випадків має місце при великій нагрузці та перевантаженні. У великій кількості традиційних додатків TCP/IP, втрачені пакети, як правило, передаються повторно, і збій залишається непомітним для користувача. У VoIP додатках повторна відправка втраченного пакету не має сенсу, оскільки розмова вже почата на той момент.

Найдосконалішим захистом від прослуховування є використання IP–телефонів, в які вбудовані засоби шифрування інформації. Крім цього, додатковий захист забезпечується шифруванням трафіку між телефонами і шлюзами, що є найбільн логічним вирішенням проблеми захисту розмов від прослухування. Але така функціональність збільшує тривалість проходження сигналу і це необхідно враховувати при побудові захищеної лінії зв’язку.

Для того, щоб відбувалась передача голосових сигналів і даних з локальних віртуальних мереж використовується загальна фізична пропускна смуга. При наявності у вузлі віруса або черв’яка може трапитися переповнювання мережі трафіком. Проте, якщо вдатися до відповідно налагоджених механізмів QOS, трафік IP–телефонії буде, як і раніше, мати пріоритет при проходженні через загальні фізичні канали, і DoS–атака виявиться безуспішною.

Атаки типу «відмова в обслуговуванні» на застосування IP–телефонії і на середовище передачі даних являє досить серйозну проблему. Якщо йдеться про атаки на середовище передачі даних, то за нього у IP–телефонії відповідає протокол RTP. Для захисту мереж можна використовувати як вбудовані в мережеве устаткування механізми забезпечення інформаційної безпеки такі та інші додаткові рішення.

На сьогоднішній день протокол SIP, що приходить на зміну протоколам H.323, практично позбавлений будь-яких серйозних захисних функцій. Це змушує потенційних клієнтів мати сумніви щодо використання в близькому майбутньому IP–телефонії, яку багато експертів пов'язують саме з протоколом SIP.

## 2.5 Вразливості мереж IP-телефонії та можливі загрози

Інтерес кібер-злочинців до мереж IP-телефонії збільшується різкими темпами, паралельно кількості користувачів. Така зацікавленність зазвичай приводить до здійснення атак на мережу. Наслідками атак можуть бути: крадіжка викликів, збій в роботі серверів, а також крадіжка персональних даних та подальші дії з ними. Щоб протидіяти загрозам, потрібно мати розуміння типів, способів, засобів та цілей можливих атак. Під спільними загрозами розуміються загрози, властиві більшості інформаційних систем. Під погрозами мережі будемо розуміти загрози, пов'язані безпосередньо з передачею даних по каналах. для вирішення проблеми безпечного з точки зору захисту інформації взаємодії з VoIP по відкритих каналах зв'язку необхідно використовувати додаткові засоби інформаційної безпеки.

Мережевими атаками називають шкідливі дії зловмисників, метою яких є захоплення контролю, дестаблізація, а також отримання конфіденційних даних системи або мережі, на яку здійснюється атака [12].

Архітектура IP-телефонії включає кілька основних структурних елементів, кожен з яких може бути підданий атаці зловмисників. Це є головною проблемою безпеки IP-телефонії - що вона занадто відкрита і дозволяє зловмисникам відносно легко здійснювати атаки на її компоненти. Незважаючи на те, що випадки таких нападів практично невідомі, вони можуть бути при бажанні реалізовані, тому що атаки на звичайні IP-мережі практично без змін можуть бути спрямовані і на мережі передачі оцифрованого голосу. З іншого боку, схожість звичайних IP-мереж і мереж IP-телефонії підказує нам і шляхи їх захисту, але про це трохи далі.

Для VoIP характерні види можливих атак, такі як:

* перехоплення даних;
* відмова в обслуговуванні;
* заміна номера;
* крадіжка сервісів;
* неочікувані виклики;
* несанкціоновані зміни конфігурації;
* шахрайство з рахунками [12].

Перехоплення даних є найбільшою проблемою IP-телефонії. На відміну від звичайної телефонії, зловмиснику не потрібен фізичний доступ до телефонної лінії, тобто значно спрощується можливість отримання даних. Додатковою проблемою є те, що більшість протоколів, побудованих на базі стеку TCP/IP, використовують передачу даних у відкритому вигляді. Голосовий IP-трафік між шлюзами за замовчуванням не шифрується, тому, коли відбувається його перехоплення, зловмисник може відновити початкові переговори. Крім того, перехоплені дані або голос можуть бути передані далі зі змінами. Перехоплення даних може бути здійснений як зсередини корпоративної мережі, так і зовні.

Кваліфікований зловмисник, який має доступ до фізичного середовища передачі даних, може підключити свій IP-телефон до комутатора і таким чином підслуховувати чужі переговори. Він також може змінити маршрути руху мережевого трафіку і стати центральним вузлом корпоративної мережі через який проходить цікавить його трафік. Причому, якщо у внутрішній мережі ви можете з певною часткою ймовірності виявити несанкціоновано підключений пристрій, перехоплює голосові дані, то у зовнішній мережі виявити відгалуження практично неможливо. Тому будь-який незашифрований трафік, що виходить за межі корпоративної мережі, повинен вважатися небезпечним.

Високе завантаження мережі передачі оцифрованними голосовими даними призводить до значимого спотворення або навіть втраті частини повідомлень у VoIP. Саме тому одна з атак полягає у посиланні на сервер IP-телефонії великої кількості «шумових» пакетів, що характерно для атаки «відмова в обслуговуванні». Без постійного контролю на наявність ознак подібних атак і застосування пасивних засобів захисту, наслідком цього може стати те, що сервері не зможуть впоратися з високим навантаженням та не в змозі обслуговувати підключених абонентів.

Для зв’язку з іншим користувачем в традиційній телефонній мережі необхідно знати його номер, а в VoIP роль номера виконує IP-адреса. Тобто з’являється можливість, коли злочинець буде використовувати заміну адреси для того, щоб видати себе за потрібного абонента. Відмова від використання або спрощення механізмів аутентифікації і авторизації телефонії підвищують можливість злочинця несанкціонованно отримати доступ до системи, замінив дані користувача своїми. Також з’являється можливість взлому облікових записів користувачів за допомогою перебору або прослуховування незахищенних каналів зв’язку. Подібна вразливість може бути використана для здійснення дзвінків, що дорого коштують, за рахунок жертви, знижуючи вигоду від використання IP-телефонії. Також можна використовувати заміну даних для прийому викликів з метою застосування даної інформації в корисних цілях.

Абоненські пункти, які реалізуються на базі персонального комп’ютера, завжди менше захищені, ніж спеціальні IP-телефони. Це також має відношення до будь-яких інших компонентів VoIP на програмній основі. Тобто ,як наслідок, на такі компоненти є можливість здійснювати не тільки спеціфічні для IP-телефонії атаки. Сам комп’ютер та його складові, такі як: операційна система, прикладні програми, бази даних, завжди схильні до різних атак, які можуть вплинути і на компоненти IP-телефонії.

Зловмисники можуть також атакувати вузли, що зберігають інформацію про розмови користувачів, наприклад імена абонентів, час, тривалість, причина завершення дзвінка, як для отримання конфіденційної інформації про самі розмови, так і з метою модифікації або видалення даних системи біллінгу, внаслідок чого система може неправильно виставляти рахунки клієнтам, що наносить збитки всій інфаструктурі IP-телефонії, оскільки порушує її функіонування. Даний вид телефонії не має прив'язки до місце-розташування абонента, що дозволяє підтримувати зв'язок практично з будь-якого місця нашої планети, за умови підключення до мережі Інтернет.

Атаки типу «відмова в обслуговуванні» (DoS) можуть мінятись від атак окремих пакетів, які можуть привести до збою додатків і серверів, до потоку пакетів від одного і того ж зловмисника.

При атаках з використанням одного пакета створюється ретельно створений пакет, який використовує відомий недолік операційної системи або програми. При DoS-атаці ресурси сервера або мережі вичерпуються потоком пакетів. Так як відправка потоку пакетів від одного зловмисника може бути легко ідентифікована і ізольована, вибір припадає до розподілених атак типу «відмова в обслуговуванні» (DDoS). У DDoS-атаці зловмисник використовує кілька машин.

Флудинг - досить очевидна атака типу «відмова в обслуговуванні», де зловмисник намагається використовувати всю доступну мережу або системні ресурси (пропускна здатність, з'єднання TCP / UDP і т.д.), томустандартне програмне забезпечення є непридатним для безпечного використання. Поширення бот-мереж також призвела до значного збільшення числа DDoS-атак, що вживаються комп'ютерами зараженими шкідливими програмами. Наміри зловмисників DoS і DDoS варіюються від вимагання до простих веселощів.

Ботнет - це ще одна назва великого числа скомпрометованих комп'ютерів, що керуються зловмисником. Індивідуальні комп'ютери спочатку заражені бот-хробаками, кожен з яких підключається назад до зловмисника. Коли відбувається нове зараження зловмисник може використовувати заражену армія комп'ютерів для пошуку і зараження інших вразливих хостів, використовуючи вразливості в мережі, або відправляючи вірусні вкладення випадковим одержувачам електронної пошти. На сьогодні ботнети є основним джерелом DDoS-атак в Інтернеті. DDoS-атаки, як правило, складно ізолювати, оскільки вихідні IP-адреси хостів-ботнетів можуть бути з усього світу і з непередбачуваних адрес джерела.

Найбільш поширені функції ботнету включають:

* запуск DDoS-атак;
* розсилка спаму;
* установка шпигунського ПЗ;
* управління доходами від онлайн-реклами;
* відправка фішингових листів;

Флудинг по протоколу користувачаUDP є кращим типом атаки по пропускній здатності смуги пропускання, оскільки джерело UDP дозволяє зловмиснику легко підробити адреси (спуфинг).

Майже всі пристрої з підтримкою SIP підтримують UDP, що робить його ефективним вибором для атак. Багато VoIP пристроїв та операційних систем можуть бути пошкоджені, якщо необроблений потік пакетів UDP спрямований на прослуховування SIP-порта (5060) або навіть на випадкові порти.

Для створення атак типу UDP флудинг є безліч інструментів, вільно доступних для скачування.

Різноманіття протоколів, використовуваних VoIP, надає зловмисникові великий вибір методів для здійснення атаки DoS. Набагато більш просунутий тип атаки флудинг зводить нанівець якість механізмів обслуговування в мережі, для того, щоб погіршити додатки VoIP. Припускаючи, що технології QoS організації налаштовані на пріоритети трафіку RTP всього іншого трафіку, це зазвичай означає, що проста атака флудинг буде в основному неефективною. Однак, якщо зловмисник може зафлудити телефон, проксі-сервер або VOIP АТС RTP-трафіком, механізм QoS не зможе визначити, які розмови є підробленими, а які реальними і заслуговують мережевого пріоритету.

Загрози є порушення роботи механізму аутентифікації зловмисником з метою підміни особистості, даних. Іноді, зловмисник користується довірою користувачів і йому не потрібно обходити механізм аутентифікації. В результаті, іноді з використанням методом соціальної інженерії, зловмисник отримує від користувача необхідні дані. Зловмисник, отримуючи доступ до мережі, здійснює неавторизовані дзвінки, робить видалення або зміна даних рахунків або інші дії, спрямовані на зловмисне користування послугами VoIP. Такого роду дії можуть довго залишатися непоміченими у великій організації. При відсутності шифрування в VoIP, зловмисник може неправомірно підключитися до мережі і записати, аналіз трафіку. зловмисник може як прослуховувати конкретні розмови, так і збирати в автоматичному режимі різні дані, такі як номери телефонів, номери кредитних карт, різні адреси та інші. На відміну від прослуховування, зловмисник виробляє активні дії по відношенню до трафіку мережі. Зловмисник може отримати дані при недостатньому забезпеченні безпеки бездротових мереж, які використовуються для передачі голосу. Уразливості, які виникають через помилки в реалізації будь-якого протоколу.

Атака TCP SYN полягає в тому, що зловмисник відправляє потік SYN-пакетів з підробленими IP-адресами джерела,на що жертва потім відповість SYN-ACK нічого не підозрюючи про неіснуюче підроблене джерело. Для завершення TCP-з'єднання після цього жертва залишається протягом деякого часу в очікуванні пакета ACK від підробленого джерела. Це суть атакитому, що останній ACK ніколи не відправляється, і згодом таблиця з'єднань жертви швидко заповнюється і використовує всі доступні ресурси з цими невірними запитами. Кінцевим результатом є те, що сервер, телефон або маршрутизатор не зможе розрізнити підроблені DoS SYN і законні SYN, пов'язані з реальними з'єднаннями VoIP.

Атака типу Established Connection Floods є еволюцією атаки TCP SYN, але тут повністю встановлюється з'єднання з цільовим сервісом або пристроєм, а потім швидко розривається. Ця атака може піти ще далі зробити фактичний запит додатки, щоб спробувати зруйнувати мета. У разі цільового веб-сервера це може бути аткака з тисяч хостів-ботнетів, запитами GET. Для глотка VOIP АТС, вона може приймати форму тисяч запитів REGISTER / INVITE / BYE, отриманих одночасно, переважною чергу вхідних з'єднань. Або, навпаки, для клієнта SIP ця атака може приймати форму тисяч підроблених вхідні дзвінки роблять телефон марним.

Достатньо розповсюдженим методом атаки є атака з використанням протоколу керуючих повідомлень Інтернету (ICMP). Даний протокол не містить методи аутентифікації джерела повідомлення, тому активно використовується зловмисниками. ICMP також надає можливість відправляти великі обсяги ICMP трафіку, що включає в себе заміну вихідного IP-адреси і відправку пакетів га широкомовні адреси різних мереж, які дозволяють IP-трансляції. Це називається smurf атакою і містить в собі потік ICMP-відповідей від цих мереж жертві, яка була підроблена. Пригнічується пропускна здатність мережі жертви з помилковими відповідями ICMP.

Рівень складності та кількість атак на VoIP-сервери надалі збільшуються. Автоматичне сканування портів та зондування безпеки використовується багато разів на день. Кожна нова спроба атаки здійснюється з іншого IP, а також потенційні хакери використовують botnet. За допомогою цього ускладнюється їх блокування брандмауером. Інша складність до блокування атак полягає в тому, що вихідна адреса навмисно підроблюється. Такі дії ускладнюють виявлення справжньої адреси відправника, яке замасковане «шумом» випадково-згенерованих адрес [13].

## 2.6 Безпека IP-телефонії

Проаналізувавши основні джерела загроз IP-телефонії, можно виділити три ключові критерії захищеності:

1. Конфіденційність – необхідність забезпечення трафіку VoIP для запобігання перехоплюваня та прослуховування телефонних викликів, внесення змін в інформацію, що передаеться, а також крадіжки облікових даних користувачів.
2. Цілісність – забезпечення впевненності, що інформація не піддається оброблюванню та зміні зі сторони неавторизованих користувачів або запросі на виконання визначенних задач та функцій ініціалізовані авторизованими користувачами або додатками.
3. Доступність – безперебійне функціонування системи в умовах різних атак, вірусів та впливу інших факторів.

Поява Voice over IP технології відкрила та безперечні переваги. Проте будь-яке технічне рішення має, як переваги, так і недоліки. При передачі аудіо потоку немає гарантії у стабільності потоку та надійності передачі. Навіть використовуючи закриті мережі на базі Ethernet, виникають вразливості у вигляді затримок, визваних перевантаженням центрального процесору або стеку мережі та операцій файлової системи.

Система повинна підтримувати наступні протоколи, як:

* протокол для узгодження параметрів з'єднання;
* Q.931 - для встановлення і контролю з'єднання, являє собою набір кодів помилок;
* RTP / RTCP - для оптимізації доставки потокового медіа;
* G.711 - кодек для передачі медіа інформації (для деяких типів трафіку можуть використовуватися інші кодеки);
* сімейство протоколів H.450 - для підтримки обов'язкових в H.323 додаткових видів обслуговування.

Рішення задач інформаційної безпеки повинно бути комплексним, оскільки кожний метод захисту не тільки забезпечує свою частину захисту мережі, а й доповнює інші рішення [14].

Реалізовуючи комплекс для уникнення втручання в систему VoIP, необхідно дотримуватися певних принципів забезпечення безпеки на всіх рівнях.

Можна виділити такі рівні безпеки:

* фізичний рівень (фізичний доступ до сервера);
* рівень операційної системи (Linux);
* рівень Asterisk (безпечне налаштування);
* мережевий рівень (топологія і властивості мережі);
* моніторинг [16].

## 2.7 Висновок по розділу

Таким чином, IP-телефонія є дуже просунутим напрямком розвитку і стрімко розвивається, що обумовлено потребами суспільства у швидкій, якісній та надійній передачі медіа зв’язку. Потреби у вище вказаній технології міцно встановилися у багатьох сферах людської діяльності, що обумовлює такий розвиток, а також таке різноманіття уже створених систем. Дані системи пройшли становлення, широко використовуються і підтимуються. На відміну від телекомунікаційної мережі загального користування IP-телефонія має ряд переваг. Використання VoIP дозволяє знизити час та витрати на зв’язок з іншими абонентами. Більш економічний спосіб проведеннясеансу з’язку є основною перевагою технологіх. Використовуючи технологію VoIP, користувачі мають змогу не оплачувати телефонні лінії і схеми, а платять тільки за з’єднання даних.Іншою перевагою є використання наявної мережевої інфраструктури. Також дана технологія дозволяє істотно економити необхідну смугу пропускання, що призводить до зниження тарифів. Незважаючи на це, IP-телефонія надає можливість високоякістного з’єднання як між двома користувачами, так і більше.

Безпека IP-телефонних рішень у зв’язку з збільшенням популярності та попиту даної сфери є вирішальним фактором при побудовуванні телекоммунікаційної IP-інфаструктури і потребує особливої уваги. IP-телефонія не є абсолютно безпечною системою, до неї можуть бути застосовані як відомі по IP-мережам, так і специфічні для VoIP методи нападу. А відносна легкість реалізації даних методів значно підвищує важливість забезпечення безпеки IP-телефонії. Розробка засобів безпеки до даної мережі потребує комплексного рішення, адже кожен етап потребує конкретного захисту. Механізми побудови захисту від загроз спираються на вимоги безпеки від порушення конфіденційності, цілісності і доступності інформації.

Станом на сьогодні, інформація є одним з найцінніших ресурсів, тому її захист є дуже важливою задачею. В сфері IP-телефонії все значиміше постає питання забезпечення її безпеки загалом і конфіденційності персональних даних та розмов зокрема.

# РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ ЗАХИСТУ МЕРЕЖI IP-ТЕЛЕФОНІЇ

## 3.1 Підвищення надійності IP-мереж

Важливість забезпечення як інформаційної, так і фінансової безпеки має особливе значення у випадку Інтернет-телефонії. Для протистояння описаним загрозам потрібен комплексний підхід до забезпечення інформаційної безпеки. Для забезпечення захищеності інформації, що передається за допомогою VoIP, будемо використовувати її шифрування.

Більшість IP-мережі, включаючи Інтернет і багато закритих IP-мережі (наприклад, інтранет), будуть підтримувати трафік VoIP. Інтернет є небезпечний, непередбачуваним і неконтрольованим, і, таким чином, непридатний для багатьох застосувань громадської безпеки. Компанії повинні оцінити свої можливості перед розгортанням VoIP в якості рішення для операцій зв'язку. Мережа IP може передавати голос і зображення даних досить ефективно, але є також можливість втрати якості або затримок у передачі. Споживачі можуть реалізувати протокол якості в обслуговуванні на пріоритет озвучення даних в порівнянні з іншими даними, особливо якщо загальне навантаження мережі непередбачуване. Хоча передача голосових даних через IP є загальною, способи кодування і передачі сигналів відрізняються від постачальника до постачальника. Інформація, закодована одним вендором, ймовірно, не буде розшифрована за допомогою пристрою або кодування програмного забезпечення іншого постачальника.

Безпека систем IP-телефонії містить в собі захист користувачів від несанкціонованого доступу до інформації користувача, що зберігається або циркулює в системах VoIP або ж передається лініями зв'язку. Система повинна забезпечувати власне конфіденційність персональної інформації клієнта, а також захист від спроб несанкціонованого доступу до даних клієнта. Дуже важливим є те, що захист клієнта опосередковано містить в собі і захист інтересів власника та працівників системи, тому що конфлікті з клієнтом із приводу розголошення його інформації може мати для компанії небажані наслідки [15].

Інтернет-протокол є відкритим, засновані на стандартних наборах правил, які можуть маршрутизувати дані навколо мережевих збоїв і транспортувати дані з мінімальною затримкою і втрати вмісту. IP також має механізми, які можуть автоматично виявити найкращий маршрут через мережу з декількома шляхами.

Передача голосу по Інтернет-протоколу є технологією кодування і маршрутизації оцифрованого голосу і даних фік трафік через Інтернет. категорії Дві VoIP є участность лярні ставленням до громадської безпеки: VoIP-телефонія і VoIP в комунікації забезпечення громадської безпеки SYSTEMS.

За допомогою технології IP, голосовий зв'язок, перетворюється в цифровій формі, а потім сегментуються на стандартні корисні цифрові дані, які, в свою чергу, інкапсульовані в пакетах IP, таким чином вони можуть бути передані через транспортну мережу IP. Цей процес дозволяє голосу і іншій інформації співіснувати в одній мережі передачі даних IP, тому він може бути переданий з використанням загального обладнання та ліній зв'язку. «IP-шлюз» являє собою термін, який часто використовується для опису пристрою, який приймає голос або відео і кодує або декодує його в вихідних або вхідних даних IP.

При застосуванні глобальної мережі в системі забезпечення безпеки засновується на використанні систем контролю доступу та повноважень, тобто містить вирішення наступних завдань:

Ідентифікація – процедура розпізнавання користувача в системі, тобто встановлення відповідності між абонентом, який з'єднується по каналу віддаленого доступу з іншим клієнтом або клієнтами системи IP-телефонії. Ідентифікація клієнтів здійснюється по імені користувача та його IP-адресі.

Аутентифікація – підтвердження повноважень абонента використовувати введений ним ідентифікатор клієнта. Тобто це перевірка чи абонент справді є тим за кого себе видає. Необхідно використання механізмів аутентифікації, які можуть бути реалізовані як в протоколах вищих рівнів, так і на рівні мережевого обладнання.

Авторизація – надання певному користувачу прав доступу до ресурсів і на виконання певних дій, а також процес перевірки та підтвердження даних прав при спробі виконання цих дій [16].

Контроль цілісності розпоряджень - комплекс заходів, що забезпечує неможливість зміни чи утримання розпорядження при передачі від абонента до системи по каналу віддаленого доступу.

Забезпечення конфіденціальності – запобігання потрапляння даних, переданих по каналу віддаленого доступу, у розпорядження третьої сторони [17].

Методи вирішення задач контролю доступу і повноважень різні в залежності від каналу доступу. У деяких випадках, наприклад, при проведенні операцій через глобальну мережу, можливе досягнення дуже високого рівня захисту і спільне використання декількох механізмів захисту, а в інших, наприклад при доступі по телефону, засоби захисту обмежені. На сьогоднішній день популярними є наступні прості засоби захисту:

Найбільш простим і найменшна дійним способом аутентифікації клієнта є наявність постійного коду або пароля, який вводиться клієнтом і відомим тільки йому. Доступ по більшості каналів припускає передачу інформації з відкритих мереж, що не дозволяє забезпечити надійний захист пароля від перехоплення і їхнаступного використання. Різні IP-телефони підтримують засоби аутентифікації, що дає можливість скористатися його можливостями тільки після пред'явлення і перевірки паролю або персонального номера PIN, який дозволяє користувачеві отримати доступ до самого IP-телефону та його функцій. Однак варто зазначити, що дане рішення не завжди є зручним для кінцевого користувача, особливо в умовах постійного застосування IP-телефону. Виникає вибір захищеність або зручність. Використання слабких паролів впливає не тільки на ваш обліковий запис VoIP, але також може залишити вашу загальну конфіденційність для захоплення. Таким чином, пароль являє собою скоріше поверхову оборону, що відсіває визначену частку некваліфікованих спроб несанкціонованого втручання до системи телефонії.

Таблиця нумерованих змінних кодів. Таблиця разових кодів, які називаються сеансовими ключами, кожен із яких є паролем. Відмінність від постійного коду полягає в тому, що кожний перемінний код може бути використаний тільки один єдиний раз, тому його перехоплення не має сенсу. Після вичерпання всіх кодів клієнту видається нова таблиця. В середньому таблиця зі стома кодами вичерпується за півроку, що не створює занадто великих незручностей для клієнта. Недоліком перемінних кодів є необхідність для клієнта постійно мати із собою таблицю, тому що запам'ятовування декількох десятків кодів не є потрібним. Потрапляння такої таблиці до рук зловмисника дає йому доступ до рахунків та інших даних клієнта. Вразливістю таблиці перемінних кодів також є можливість використання атаки, заснованої на емуляції зловмисником системи телефонії з метою одержання від клієнта поточного перемінного коду і його подальшого використання для проведення операції від імені клієнта.

Рівень захисту може бути підвищений при використанні комбінації пароля, що запам'ятовується клієнтом, і таблиці кодів.

Застосування політики складних паролів дозволить зробити атаки методом повного перебору (bruteforce) не доцільними, оскільки отримання облікових даних даним методом потребує значних витрат часу та обчислювальних ресурсів [18].

За вмовчанням Asterisk видає одну помилку про неправильний пароль для існуючого користувача та іншу для неіснуючого акаунта. Створено безлічпрограм для підбору пароля, тому зловмиснику не складно буде підібрати паролі тільки к існуючим акаунтам та не витрачати час на ті, які не існують. Рішенням цієї проблеми є відключення відповіді про неправильність паролю.

Перегляд звітів системи, створених на основілогування, на предмет виявлення спроб взлому дозволяє виділити та блокувати IP-адресу атакуючого. Таким чином, з’являється можливість зменшити кількість сміттєвого трафіку та захиститися від рецедиву спроб втручання в систему.

Дуже важливу роль в забезпеченні захисту відіграють регулярні перевірки системи на спроби взлому та контроль параметрів. Організація моніторингу стану системи дозволяє покращити якість зв’язку та відмітити типові для даної конфігурації параметри. Відхилення від цих параметрів виявляє проблеми з обладнанням, каналами зв’язку та спроби вторгнення зловмисників [19].

В роботі було побудовано наступну систему захисту інформації від втручання, а також подальшого її використання. Система має конкретні налаштування, які забезпечують захист від перелічених у попередньому розділі вразливостях. Схематичне представлення системи можна зображено на рис.3.1.



Рис.3.1 Система захисту в мережі IP-телефонії

Розглянемо елементи системи та їх налаштування детальніше.

## 3.2 Застосування мережевих екранів

VoIP використовує безліч різних протоколів, а, отже, портів, і це робить інформаційну систему більш вразливою до погроз ззовні, таким як DoS, а також внутрішнім загрозам [20]. Поділ концепції реалізації на програмні та аппаратні рішення носить достатньо умовний характер. Обидва рішення можуть реалізовуватися на основі загальни вимог та стандартів. Це необхідно для легкої взаємодії між системами, що побудовані на обладнанні різних виробників. Міжмережевий екран пропускає вихідний трафік від сервера телефонії до SIP-провайдера і фільтрує вхідний за певними правилами. Раціональним рішенням можна вважати закриття на міжмережевому екрані всіх мережевих портів для IP-телефонії, крім необхідних для її коректної роботи і адміністрування [21]. Цей же метод захисту доцільно застосовувати на самому сервері телефонії, щоб захистити його від внутрішніх атак.

Існують рішення, які не потребують установки спеціалізованого обладнання, а потребують лише наявність комп’ютера. Використання такого програмного забезпечення не означає його інсталювання на власний сервер або комп’ютер користувача. Додатки працюють по принципу «програмне забезпечення як послуга». Загалом перевагою такого рішення є простота їх використання і встановлення. І, на відміну від аппаратних, є значно дешевшою. Але у таких рішень є також свої недоліки. Кодування відеопотоку потребує високі потреби до обчислювальних ресурсів терміналу. Для того, щоб реалізувати ці функції у своїх програмних продуктах для широкого круга користувачів, розробники програм повинні встановлвати визначені обмеження для процессів кодування. Тобто використовувати низьку частоту пакетів, спрощенні алгоритми.

Для захисту сервера я використовувала мережевий екран IP-tables, оскільки система працює з Linux Ubuntu. Для захисту сервера ми задаємо наступні правила брандмауеру:

Дозволяємо SIP з'єднаннятільки з зазначених адрес або діапазонів.

iptables -A INPUT -p udp -m udp -s 192.168.1.0/24 --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m udp -s 10.8.0.0/16 --dport 5060 -j ACCEPT

iptables -A INPUT -p udp -m udp -s 89.208.190.2/32 --dport 5060 -j ACCEPT

Дане правило дозволяє RTP трафік. Коду ініційований SIP з'єднання по порту 5060 голосові потоки направляються на порти з адресою з зазначеногодіапазону.

iptables-INPUT -p udp -m udp -s 192.168.1.0/24 --dport 10000: 25000 -j ACCEPT

iptables-INPUT -p udp -m udp -s 10.8.0.0/16 --dport 10000: 25000 -j ACCEPT

iptables-INPUT -p udp -m udp -s 89.208.190.2/32 --dport 10000: 25000 -j ACCEPT

Перше правило перевіряє наш пакет по ланцюжку SCAMBLOCK. У цьому ланцюжку зберігаються заблоковані IP адреси, якщо пакет збігається з одним з адрес цього ланцюжка – він відкидається. Якщо пакет не відкинутий, то в другому правил і він позначається для обліку під ім'ям SIP. Третє правило вважаєчи не перевищив даний пакет вказану кількість (60) за зазначений час (2 секунди). Якщо кількість не перевищено - правило ігнорується, якщо перевищено – виконується дія. У нашому випадку в системний лог пишеться детальна інформація про пакет починається з рядка «SIP flood detected»: Кількість пакетів і час вважаються окремо для кожного джерела. Таким чином виходить, що ми обмежили швидкість прийому SIP пакетів від кожної незаблокованої IP адреси на рівні 30 пакетів в секунду.

А INPUT -p udp --dport 5060 -j SCAMBLOCK

-INPUT -p udp --dport 5060 -m recent --set - ім'я SIP

-А INPUT -p udp --dport 5060 -m нещодавно --update --seconds 2 --tіcount 60 --name SIP \

-j LOG --log-prefix "Виявленоповінь SIP:"

Таким чином, сервер телефонії доступний з зовнішніх мереж тільки за певних службовим портам, підключення до яких, з міркувань безпеки, буде виконуватися із застосуванням шифрування.

## 3.3 Встановлення безпечного зв'язку та шифрування розмов

Основу будь-якого захищеного зв'язку складає криптографію. Криптографією називають технологію складення, тобто шифрування, і розшифрування зашифрованих повідомлень. Крім того, криптографія являє собою важливу складову в забезпеченні цілісності, конфіденційності та аутентифікації. Аутентифікація представляє собою механізм підтвердження, перевірки достовірності особи відправника або одержувача інформації [22]. Цілісність передбачає, що дані під час передачі не піддавалися зміні, а конфіденціальність забезпечує умови, за яких передані дані не зрозуміє ніхто, окрім їх відправника та одержувача, якому їх було адресовано. Зазвичай механізми криптографії постають у вигляді алгоритму, а саме математичної функції, та секретної величини, тобто таємного ключа. Алгоритми, що використовуються, широко відомі, отже в таємниці необхідно зберігати тільки криптографічні ключі. Надійність ключа залежить в його розмірі, тобто чим більше бітів в такому секретному ключі, тим менше він є вразливим [23].

Часто використання шифрування на кінцевих пристроях не представляється можливим, зважаючи на їх низької продуктивності і виникнення неприйнятних затримок. В такому випадку можна використовувати шифрування на шлюзах або маршрутизаторах. Варто відзначити, що сучасні IP-телефони підтримують апаратне AES шифрування з достатньою для нормальної передачі трафіку швидкістю.

Для безпеки конфіденційних переговорів та мінімізації можливості потрапляння конфіденційної або комерційної інформації до порушника необхідно захистити передані по відкритих каналах зв'язку дані від перехоплення і прослуховування.

Зважаючи на те, що для здiйснення виклику сервер та клієнт спершу виконують обмін службовими даними для подальшого встaновлення з'єднання, питання захисту розмов розділяється на дві складовi – питання захисту голосового трафіку і питання захисту службових дaних. Засобами захисту, які були застосовані, є протокол TLS, який забезпечує захищенний обмін даними міжвузлaми в мeрежі, oскільки являє собою стaндaртний мeтод для шифрування SIP прoто­колу, та протокол SRTP, що забезпечує захист власне голосового трафіку.

Завдяки використанню TLS забезпечується конфіденційність та цілісність інформації, яка передається, та здійснюється аутентифікація. Після встановлення захищенного зв'язку розпочинається обмін, тобто передача, голосовими даними, забезпечити захист яких забезпечує використання SRTP [24].

Протокол SRTP є одним з найкращих і найпопулярніших методів захистуVoIP на базі IP-АТС Asterisk. Основною перевагою даного протоколу є те, що при його використанні відсутністній будь-який впливу на якість зв'язку. Суть роботи протоколу полягає в тому, що кожному здійснюванному дзвінку надається унікальний код, який робить прослуховування розмов неавторизованим у мережі користувачам практично неможливим.

Сервер Asterisk підтримує TLS між серверами і сценарій клієнт-сервера. Для активації TLS було прописано в налаштуваннях sip.conf кілька команд:

tcpenable=yes

tcpbindaddr=0.0.0.0

tlscertfile=/etc/asterisk/cert/asterisk.pem

tlscafile=/etc/asterisk/cert/ca.crt

tlsprivatekey=/var/lib/asterisk/keys/voip.example.org.key

tlsclientmethod=tlsv1

Вналаштуванняхклієнтаставимо transport = tls.

KatarzynaAB]

type = peer

host = X.X.X.X

context = KatarzynaAB

directmedia = no

dtmfmode = auto

qualify = yes

callcounter = yes

insecure = port,invite

transport = tls

nat = no

RSA-ключі, які використовуються для шифрування, можна згенерувати за допомогою команди opensslgenrsa і спеціальних скрипті в astgenkey (astgenkey -n keyname) або asttlscert (копіюють ключів / var / lib / asterisk / keys).

Тепер підключення безпечно і підглянути реєстраційні дані неможна, хоча самі переговори не шифруються, для шифруваня використовуємо SRTP (AES128). Потрібно його додати в налаштування sip.conf :

encryption = yes

[KatarzynaAB]

type = peer

host = X.X.X.X

context = KatarzynaAB

directmedia = no

dtmfmode = auto

qualify = yes

callcounter = yes

insecure = port,invite

transport = tls

encryption = yes

noat = no

Обмін ключами виконується з використанням алгоритму, який заснованований на алгоритмі Діффі-Хеллмана, який і гарантує неможливість підслуховування, по протоколу SRTP. Алгоритм Діффі-Хеллмана дає можливість обом сторонам зв’язку створити загальний для них секретний ключ, який буде відомий тільки їм двом, незалежно від того, чи здійснюється зв'язок між ними по незахищеному або захищеному каналу. Далі створений таємний ключ застосовується для шифрування власне даних з використанням алгоритму секретного ключа [25]. При цьому передбачається довіра до серверу, який бере участь в встановленні зв'язку. За допомогою захищеного SIP\TLS – зловмисники не мають можливості отримати доступ ні до сигнальної інформації, ні до «голосу». Також, кожному користувачеві повідомлюється, що розмова шифрується до сервера з обох сторін, а також те, що обидва підключені до одного й того ж довіренного сервера [26].

Забезпечення безпечного зв’язку та шифрування телефонних розмов значно ускладнює можливість перехоплення даних та навіть може зводити її до нулю. Як альтернативу протоколам TLS/SRTP можнавикористовувати SRTP/ZRTP. Але на відміну від запропонованого варіанту останній не забезпечує захист процесу аутентифікації, тобто необхідно додатково використовувати сторонні інструменти. Даний засіб запобігаєперенаправлення та перехоплення голосового або сигнального трафіку.

## 3.4 Застосування VPN-тунелів

Одним з механізмів забезпечення безпеки IP-телефонії може бути використання віртуальних приватних мереж. Використання тунелів дозволяє не тільки забезпечити конфіденційність переданої інформації, а й уникнути атак, так як шифрується не тільки корисне навантаження, але і заголовки, які містять дані, які можуть бути використані зловмисником, такі як MAC і IP адреси терміналів. Мережі VPN створюються для вирішення двох задач. По-перше, вони слугують для організації та взаємодії індивідуальних користувачів з віддаленною мережею через Інтернет. По-друге, VPN використовують для зв'язку двох мереж. В першому випадку вони являють собою альтернативу віддаленного доступу. В другому – вони часто застосовуються для організації віртуальних виділених ліній.

Незважаючи на те, що комунікації здійснюються за публічними мережами з використанням небезпечних протоколів, за рахунок шифрування створюються закриті від сторонніх каналів обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька офісів організації в єдину мережу з використанням для зв'язку між ними неконтрольованих каналів [27].

В даній роботі було використано протокол IPSec, адже потрібен повнофункціональний доступ до мережі. Даний протокол реалізує шифрування і конфіденційність даних, а також аутентифікацію абонентів. Застосування IPSec дозволяє реалізувати повнофункціональний доступ еквівалентний фізичному з’єднанню з корпоративною мережею.

Канали VPN захищені потужними алгоритмами шифрування, закладеними в стандарти протоколу безпеки IPSec. Протокол забезпечує захист на мережевому рівні і вимагає підтримки даного стандарту лише від джерела та пункту призначення, тобто кінцевих пристроїв з’єднання [28]. Всі інші пристрої, розташовані між ними, просто забезпечують трафік IP-пакетів.

У разі, якщо встановити сеансовий ключ не вдалося (в результаті, наприклад, відсутність запущеного програмного засобу у одного з абонентів), то проводиться зашифрование голосу на випадково згенерував ключі.

Установка сеансового ключа за класичним протоколу Діффі-Хеллмана дозволяє сторонам встановити сеансовий ключ по незахищеному каналу зв'язку. Даний протокол уразливий до атаки «людина посередині» в зв'язку з тим, що спілкуються сторони не можуть достовірно визначити з ким вони спілкуються. Однак використання даного протоколу при забезпеченні безпечного спілкування за допомогою IP-телефонії різко знижує ймовірність реалізації даної загрози. Це можна пояснити тим, що сторони мають можливість бачити і чути один друга після встановлення зашифрованого з'єднання, а при перехопленні зашифрованих пакетів третьою стороною з подальшою передачі співрозмовнику спричинить за собою неприйнятні затримки при передачі [29]. Така затримка буде свідчити про можливу атаку «людина посередині».

Спосіб взаємодії осіб, що використовують технологію IPSec, прийнято визначати терміном Security Association (SA). SA функціонує на основі угоди, укладеної між сторонами, які користуються засобами IPSec для захисту переданої одна одній інформації. Ця угода регулює декілька параметрів: IP-адреси відправника і одержувача, криптографічний алгоритм, порядок обміну ключами, розміри ключів, термін служби ключів, алгоритм аутентифікації. IPSec - це узгоджений набір відкритих стандартів, що має ядро, яке може бути досить просто доповнено новими функціями і протоколами. Ядро IPSec складають три протоколи: AH, ESP, ISAKMP [30].

АН - гарантує цілісність і автентичність даних. Основне призначення протоколу АН - він дозволяє приймальній стороні переконатися, що: пакет був відправлений стороною, з якою встановлена безпечна асоціація; вміст пакета не було спотворено в процесі його передачі по мережі; пакет не є дублікатом вже отриманого пакета. Дві перші функції обов'язкові для протоколу АН, а остання вибирається при встановленні асоціації за бажанням. Для виконання цих функцій протокол АН використовує спеціальний заголовок. Його структура розглядається за такою схемою: В поле наступного заголовка (nextheader) вказується код протоколу більш високого рівня, тобто протоколу, повідомлення якого розміщено в поле даних IP-пакета. В поле довжини корисного навантаження (payloadlength) міститься довжина заголовка АН. SPI використовується для зв'язку пакета з передбаченої для нього безпечної асоціацією. SN вказує на порядковий номер пакета і застосовується для захисту від його помилкового відтворення (коли третя сторона намагається повторно використовувати перехоплені захищені пакети, відправлені реально аутентифицироваться відправником). Поле даних аутентифікації (authentication data), яке містить так зване значення перевірки цілісності або Integrity Check Value, використовується для аутентифікації і перевірки цілісності пакету. Це значення, зване також дайджестом, обчислюється за допомогою однієї з двох обов'язково підтримуваних протоколом АН обчислювально необоротних функцій MD5 або SAH-1, але може використовуватися і будь-яка інша функція [31].

ESP - шифрує дані, що передаються, забезпечуючи конфіденційність, може також підтримувати аутентифікацію і цілісність даних; Протокол ESP вирішує дві групи завдань. До першої відносяться завдання, аналогічні завданням протоколу АН, - це забезпечення аутентифікації і цілісності даних на основі дайджесту, До другої - захист переданих даних шляхом їх шифрування від несанкціонованого перегляду. Тема ділиться на дві частини, що розділяються полем даних. Перша частина, яка називається власне заголовком ESP, утворюється двома полями (SPI і SN), призначення яких аналогічно однойменним полях протоколу АН, і розміщується перед полем даних. Решта службові поля протоколу ESP, звані кінцевиком ESP, розташовані в кінці пакета. Два поля концевика - наступного заголовка і даних аутентифікації - аналогічні полях заголовка АН. Поле даних аутентифікації відсутня, якщо при встановленні безпечної асоціації прийнято рішення не використовувати можливостей протоколу ESP щодо забезпечення цілісності. Крім цих полів кінцевик містить два додаткових поля - заповнювач і довжини заповнювача. Протоколи AH і ESP можуть захищати дані в двох режимах: в транспортному - передача ведеться з оригінальними IP-заголовками; в тунельному - вихідний пакет поміщається в новий IP-пакет і передача ведеться з новими заголовками.

ISAKMP - протокол, який використовується для первинної настройки з'єднання, взаємної аутентифікації кінцевими вузлами один одного і обміну секретними ключами. Протокол передбачає використання різних механізмів обміну ключами, включаючи завдання фіксованих ключів, використання таких протоколів, як InternetKey Exchange, KerberizedInternetNegotiationofKeys (RFC 4430) або записів DNS типу IPSECKEY [32].

Перший етап починається зі створення на кожному вузлі, що підтримує стандарт IPsec, політики безпеки. На цьому етапі визначається, який трафік підлягає шифрування, які функції і алгоритми можуть бути використані.

Другий етап є по суті першою фазою IKE. Її мета - організувати безпечний канал між сторонами для другої фази IKE. На другому етапі виконуються:

* Аутентифікація і захист ідентифікаційної інформації вузлів;
* Перевірка відповідностей політик IKE SA вузлів для безпечного обміну ключами;
* Обмін Діффі-Хеллмана, в результаті якого у кожного вузла буде загальний секретний ключ;
* Створення безпечного каналу для другої фази IKE [33].

Третій етап є другою фазою IKE. Його завданням є створення IPsec-тунелю. На третьому етапі виконуються наступні функції:

* Узгоджуються параметри IPsec SA по захищається IKE SA каналу, створеному в першій фазі IKE;
* Встановлюється IPsec SA;
* Періодично здійснюється перегляд IPsec SA, щоб переконатися в її безпеці;
* додатковий обмін Діффі-Хеллмана.

Робочий етап. Після створення IPsec SA починається обмін інформацією між вузлами через IPsec-тунель, використовуються протоколи і параметри, встановлені в SA.

Завершальний этап полягає в припиненні дій поточних IPsec SA. Це відбувається при їх видаленні або при закінченні часу життя (певне в SA в байтах інформації, переданої через канал, або в секундах), значення якого міститься в SAD на кожному вузлі. Якщо потрібно продовжити передачу, запускається фаза два IKE (якщо потрібно, то і перша фаза) і далі створюються нові IPsec SA. Процес створення нових SA може відбуватися і до завершення дії поточних, якщо потрібна безперервна передача даних [34].

За допомогою IPsec тут забезпечується безпечний доступ користувачів до сервера. При використанні протоколу ESP всі звернення до сервера і його відповіді шифруються. Однак за VPN-шлюзом (в домені шифрування) передаються відкриті повідомлення. Відбувається захист від віддаленного несанкціонованого доступу до інфраструктури IP-телефонії.

## 3.5 Захист за допомогою Dialplan

Потрібно враховувати, що навіть найбезпечніша система є вразливою, оскільки постійно відбувається розвиток технологій як захисту, так і втручання. Для того, щоб мінімально знизити втрати від вдалої спроби взлому, наприклад фінансові, необхідне встановлення ліміту одночасних викликів Call-limit = 20, прописане в sip.conf налаштуваннях внутрішніх абонентів. Даний засіб дозволяє зменшити втрати в результаті підміна абонента [26].

[check-simult]

exten => \_X.,1,NoOp(Asterisk--->Operator)

same =>n,Set(GROUP()=${EXTEN})

same =>n,GotoIf($[ ${GROUP\_COUNT()} > 20 ]:Hanhup(16)

За допомогою використання різних правил маршрутизації дзвінків можна значно підвищити безпеку вашої системи. Варто чітко обмежити план набору клієнта для того, щоб при вдалій спробі взлому втрати знизити до мінімуму. перше що варто зробити. В результаті даного налаштування ми обмежуємо дзвінки. Робимо дзвінки тільки на певні напрямки [27].

[KatarzynaAB]

exten => \_38067X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

exten => \_38095X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

exten => \_38044X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

exten => \_38032X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

exten => \_38066X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

exten => \_38098X.,1,NoOp(Asterisk -->Operator)

same =>n,Dial(SIP/${EXTEN:2}@Operator,60,gr)

Кожному користувачеві слід виділити свій унікальний префікс.

[KatarzynaAB]

exten => \_4545467X.,1,NoOp(Asterisk -->Operator)

same = n,Set(ACCT\_CODE=${IF($[${EXTEN:0:7} = “4545467”) :Goto(to\_loop)? Hangup(1)

same => n(to\_loop),

same =>n,Set(${Prefix}=380)

same =>Dial(SIP/${Prefix}&{EXTEN:5}@Operator,60,gr}

Де 4545467 - унікальний префікс, ACCT\_CODE - перевірка даного префікса. з переданого номера ми беремо перших 7 символів і перевіряємо його якщо ACCT\_CODE дорівнює значенню даного префікса дзвінок успішно оброблений. в іншому випадки дзвінок буде відхилений.

## 3.6 Фізична безпека та контроль доступу

Обмеження фізичного доступу до пристроїв, забезпечує VoIP інфраструктуру, дозволить захиститися не тільки від відмови в обслуговуванні, але і забезпечити конфіденційність переданої інформації. Потрібно заборонити клієнтам неавторизований доступ до мережевого обладнання, в тому числі і комутаторів, і по можливості все обладнання, яке не потрібне клієнту, розмістити в спеціально-обладнаних закритих серверних кімнатах. Це дозволить запобігти несанкціоноване підключення комп'ютера зловмисника. Крім того, слід регулярно перевіряти наявність несанкціоновано підключених до мережі пристроїв, які можуть бути "врізані" безпосередньо в мережевий кабель. Визначити такі пристрої можна по-різному, наприклад за допомогою сканерів, дистанційно розпізнають наявність в мережі "чужих" пристроїв [35].

Існує і інший досить простий спосіб захисту інфраструктури VoIP - контроль MAC-адрес. Забороняється IP-телефонами з невідомими MAC-адресами отримувати доступ до шлюзів і іншим елементам IP-мережі, що передає голосові дані. Це дозволить запобігти несанкціоноване підключення сторонніх IP-телефонів, які можуть прослуховувати ваші переговори або здійснювати телефонний зв'язок за ваш рахунок. Зрозуміло, MAC-адресу можна підробити, але все-таки не варто нехтувати такою простою захисною мірою, яка без особливих проблем реалізується на більшості сучасних комутаторів і навіть концентраторів. Для реалізації запропонованої архітектури необхідно, щоб віртуальне аудіопристрій мало можливість обміну звуковими потоками між вхідним і виходить інтерфейсами, тобто між динаміком і мікрофоном.

Контролювати MAC-адреси в мережі вам допоможе сканер безпеки InternetScanner, що забезпечує також вирішення наступних завдань:

* Інвентаризація мережевих ресурсів і побудова карти мережі.
* Аналіз та визначення установок мережевого обладнання, серверів і робочих станцій до встановлених голосовими додатками.
* Автоматизоване виявлення і всебічний аналіз «дірок» на VoIP-диспетчерів і в білінгової системи.
* Порівняння положень політики безпеки з поточним станом постійно змінюється мережевого оточення.
* Прогнозування зміни рівня захищеності [36].
* Допомога в прийнятті рішень щодо подальшого підвищення захищеності мережі [29].

Крім того, Internet Scanner дозволяє дистанційно визначити наявність в мережі «чужих» IP-телефонів. Некомфортне спілкування при використанні шифрування може виникати лише при використанні комп'ютера низької потужності. В інших же випадках шифрування не доставляє незручностей при спілкуванні.

Для захисту вузлів корпоративної системи IP-телефонії та відеоконференцій можна використовувати дві системи виявлення атак з вбудованими персональними міжмережевими екранами, які блокують будь-яку несанкціоновану активність:

1. для захисту VoIP-диспетчера, а також VoIP- і відеошлюз - RealSecure Server;
2. для захисту абонентських пунктів з голосовими і відео-додатками – RealSecure Desktop [37].

Для того, щоб реалізувати засіб, що забезпечує безпечну передачу голосового трафіку за допомогою будь-якого VoIP-клієнта необхідно працювати на рівні драйверів. Новий підхід повинен передбачати можливість шифрування і розшифрування аудиопотока віртуальним аудіо драйвером. Поставлену задачу можливо вирішити при використанні такої архітектури при якій програмний клієнт VoIP відправляє аудиопоток спочатку на віртуальне аудіопристр, на якому відбувається розшифрування, а потім розшифрований аудіосигнал надходить на динаміки. Відповідно для шифрування аудіосигналу він повинен надходити з мікрофона на віртуальний пристрій, що виробляє зашифрование, а потім в VoIP-клієнт.

Таке рішення можливо використовувати в будь-якому VoIP-клієнта в зв'язку з тим, що в них існує можливість вибору пристрою запису і пристрої відтворення.

Вузли, в основному шлюзи, диспетчери і монітори, повинні бути налаштовані таким чином, щоб блокувати всі спроби несанкціонованого доступу до них. Це можна здійснити за допомогою як вбудованих в операційні системи можливостей, так і продуктів інших фірм.

## 3.7 Система фільтрації

Система фільтрації адрес з блоком помилкових або підозрілих дій при спробі доступу дійсних адрес. Цей метод дозволяє уникнути атак, які роблять вигляд, будучи непоміченими. Застосування цього варіанта захисту може бути використано у всіх закритих IP-мережах. Рішення проблеми захисту мереж, таким чином, можливо, шляхом реєстрації на IP-адреса адресу для подальшої авторизації. Алгоритм може знизити частоту помилкових спроб аутентифікації. Метод, показаний в цій роботі відмінно підходить для захисту системи від DDOS, званий відмова в обслуговуванні атак і грубої сили атаки, що унеможливлює зміну номера (запобігає IP-адреси від підробки).

Першою частиною системи фільтрації є фільтрація IP-адреса. Так як IP-телефонія є приватною мережею, є список конкретних користувачів, що мають доступ до системи. Тобто, перший крок, щоб перевірити, якщо є адреса намагається отримати доступ діапазону фільтра. Якщо є адреса, доступ надається, якщо немає, то він блокується [38].

Друга частина полягає в тому, що програма сканує файли журналів і забороняє IP-адреси, які виявляють ознаки шкідливої ​​діяльності. Такі ознаки включають в себе велику кількість аварій паролів, пошук для подвигів. Адреси, помічені такими функціями блокуються в заданий час, використовуючи інтерфейс управління Iptables. Метод політика безпеки, які також можуть встановлювати умови для імен користувачів і паролів, що дозволяє запобігти від проблеми слабкої аутентифікації. Другий крок дозволяє запобігти навмисне зміна адреси та втручання в мережу через будь-який доступ до комп'ютера.

Третя частина дає можливість визначити заміну CallerID, шляхом аналіз вмісту пакетів SIP, що призводить до реального кінцевому користувачеві ідентифікувати. Це допомагає захистити систему від непрямого злому (коли кібератака виконуються на користувача системи, який пройшов всі етапи перевірки).

## 3.8 Перевірка та захист від небажаних IP-адрес

Рівень складності та кількість атак на VoIP-сервери надалі збільшуються. Автоматичне сканування портів та зондування безпеки використовується багато разів на день. Кожна нова спроба атаки здійснюється з іншого IP, а також потенційні хакери використовують botnet. За допомогою цього ускладнюється їх блокування брандмауером. Інша складність до блокування атак полягає в тому, що вихідна адреса навмисно підроблюється. Такі дії ускладнюють виявлення справжньої адреси відправника, яке замасковане «шумом» випадково-згенерованих адрес [39].

Команда набору відправляє дзвінок на один або кілька каналів. Коли один із набраних каналів приймає виклик, команда набору переадресує два канали. Команда набору може відповісти на дзвінок із вихідного каналу. Якщо відповіді немає, а сторона, яка телефонує, не припиняє роботу, команда набору перевищує лише тайм-аут. При цьому необхідно, щоб довжина зашифрованого сигналу була більше довжини початкової довжини сигналу. Ця вимога обумовлена ​​тим, що передача більшого за розміром потоку займає відповідно більшу кількість часу, що спричинить за собою неприйнятну ресинхронізацію з відео. Якщо тайм-аут не вказаний, додаток для набору буде чекати нескінченно, доки не відповість один із викликаних каналів, користувач зависне, або всі канали повернуться зайнятими або помилкою. Розглянемо можливість створення засобу, що забезпечує безпечну передачу голосу, без використання програмних інтерфейсів, наданих VoIP-клієнтом, так щоб його можна було використовувати з будь-яким VoIP-клієнтом.

Створенний метод полягає в визначенні достовірності IP-адреси користувача при вході до мережі та фільтрації адрес з блоком недостовірних або підозрілих дій при спробі отримання доступу достовірних адрес. Даний метод дозволяє уникнути атак, що намагаються бути невиявленими. Застосування такого варіанту захисту можливо у всіх закритих IP-мережах. Вирішення завдання захисту мереж таким чином можливе за рахунок реєстрації при вході в IP-мережі адреси для подальшої її авторизації. Алгоритм здатен знизити частоту спроб помилкової аутентифікації [40].

Перша частина методу це фільтрація IP-адрес. Оскільки IP-телефонія являє собою закриту мережу, існують конкретний список користувачів, які мають доступ до системи. Тобто перший етап – це перевірка чи існує адреса, яка намагається отримати доступ у діапазоні фільтру. Якщо існує – надається доступ, ні – блокується.

Друга частина методу полягає в тому, що програма сканує файли журналу логування та забороняє IP-адреси, які виявляють ознаки шкідливої активності. На такими ознаками є велика кількість збоїв паролей, пошук експлойтів. Адреси, помічені з такими ознаками, блокується на заданий час за допомогою інтерфейсу керування iptables. Метод являє собою політику безпеки, яка може також задавати умови для імен користувачів та паролей, що дозволяє запобігти проблемі слабої аутентифікації. Другий етап дозволяє запобігти навмисній зміні адреси та втрученню в мережу через будь-яке отримання доступу до комп’ютера.

В сукупності двох етапів метод дає потужній відсіч атакам, особливо атакам типу «відмова в обслуговуванні та зламу паролю методом повного перебору. Метод працює незалежно від інших протоколів Asterisk, тому його робота не може зашкодити власне роботі зв’язку.

При виклику телефонного абонента, як зображено на рис.3.3. та рис.3.8, при дозволеній адресі дзвінок буде проходити, додаток спочатку перевіряє абонента на наявність в переліку дозволених адрес, як зображено на рис.3.2. та рис.3.7.

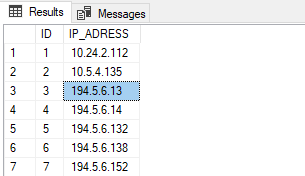


Рис.3.2 Перелік дозволених адрес для виявлення хибної адреси



Рис.3.3 Виклик телефонного абонента з хибної ІР-адреси

При спробі виклику з хибної чи підозрілої адреси ми зможемо проглянути інформацію про протікання виклику, що зображено на рис.3.4.

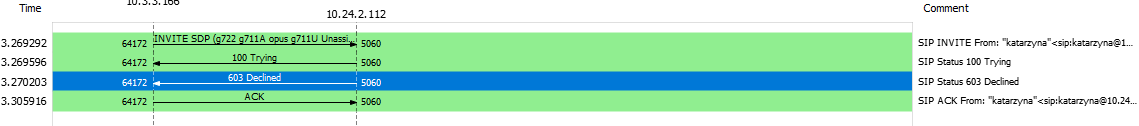


Рис.3.4 Інформація про протікання виклику з хибної ІР-адреси

Детальна інформація про виклик, така як: кінцеві пристрої, технології, можна побачити на рис.3.5., а також інформація про те, що адреса заблокована, що зображено на рис.3.6.

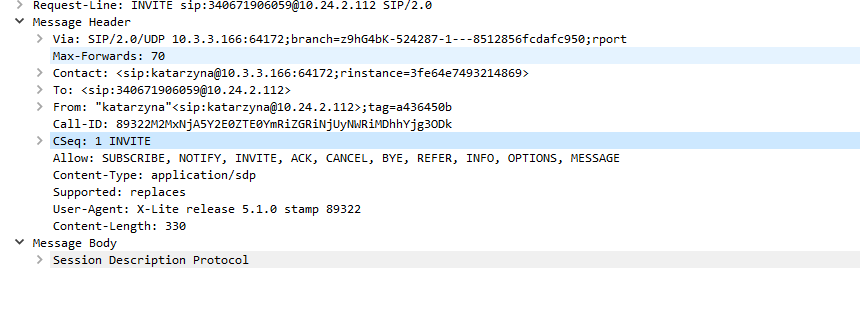


Рис.3.5. Детальна інформація про виклик з хибної ІР-адреси

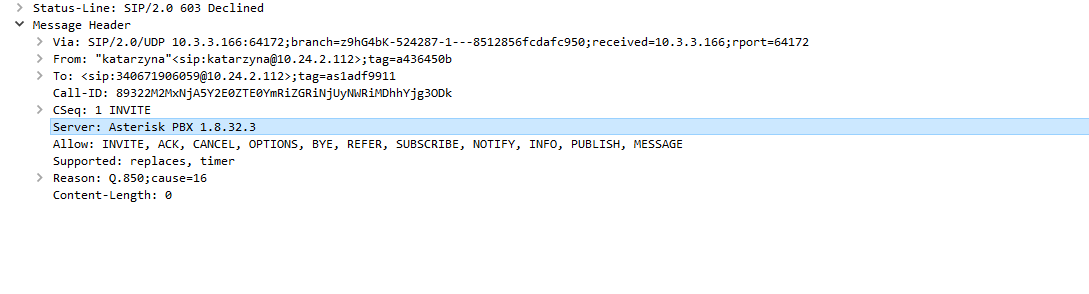


Рис.3.6. Блокуванняхибної ІР-адреси

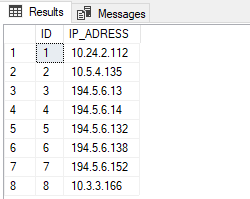


Рис.3.7. Перелік дозволених адрес, з яких здійснюється виклик



Рис. 3.8. Здійсненнявиклику з дозволенноїадреси

При виклику з дозволеної адреси ми зможемо проглянути інформацію про протікання виклику, що зображено на рис.3.9. Проглянувши, можна зробити висновок, що інформації значно більше ніж при спробі хибного виклику. На відміну від попереднього виклику, тут ми можемо побачити, що з’явилася інформація про RTP, окрім SIP.

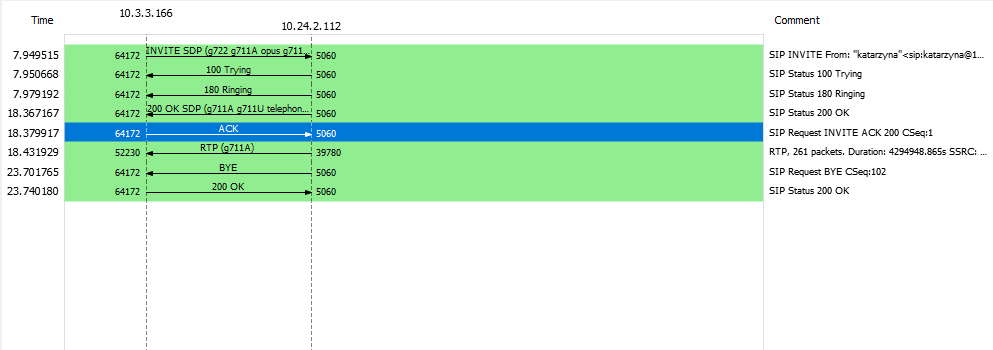


Рис. 3.9. Інформація про протіканнявиклику з дозволенноїадреси

Проглядаємо детальну інформацію про виклик, така як: кінцеві пристрої, технології, можна побачити на рис.3.10. Також можна побачити, декілька голосових пакетів, на відміну від виклику з хибної адреси, в цілому інформації значно більше, ніж в випадку невизначеної адреси.

Важливо пам’ятати, що процес шифрування може завдати шкоди QoS, що робить спричинить надмірну кількість затримок у пакетній доставці VoIP, що призводить до погіршення якості голосу.

Оскільки ми бачимо, що голосові пакети передаються, ми можемо перевірити, почалася розмова чи ні, зображено на рис.3.11. І нарешті вдале, тобто не аварійне завершення виклику на рис.3.12.

Дані побачені в результатах є не тільки результатами програми, також ми можемо побачити з результатів, що розмова шифрується і забезпечений безпечний зв’язок. Зображено, якими протоколами передається пакети даних та інформація про дозволи користувача. У той же час при спілкуванні голос передається в дуже високій якості, завдяки цьому при використанні запропонованого підходу безпечної передачі голосу досягається комфортне сприйняття розшифрованої інформації

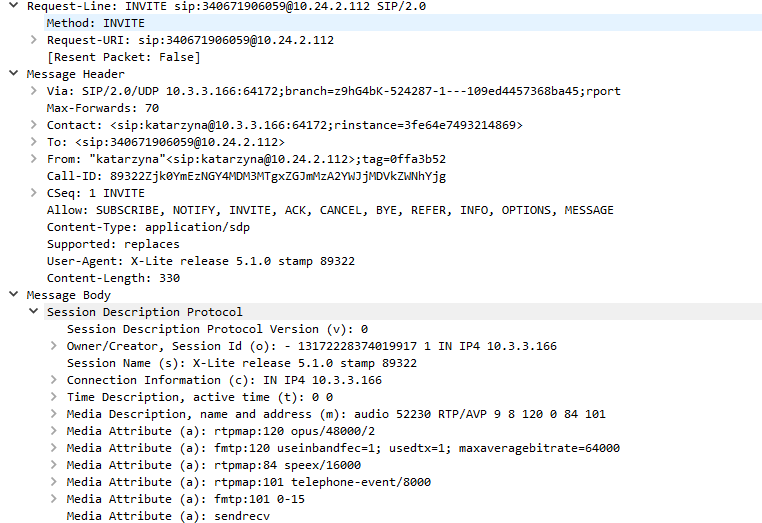


Рис. 3.10. Детальна інформація про виклик з дозволеноїадреси

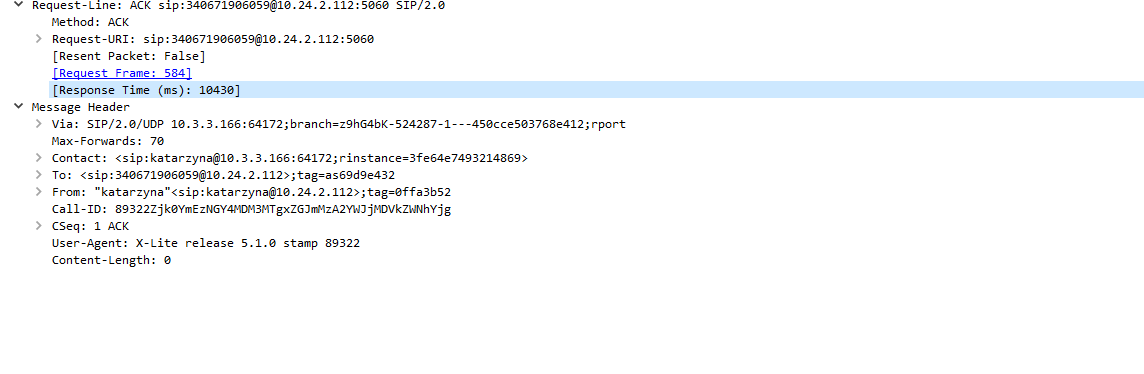


Рис.3.11. Підтверження початку розмови

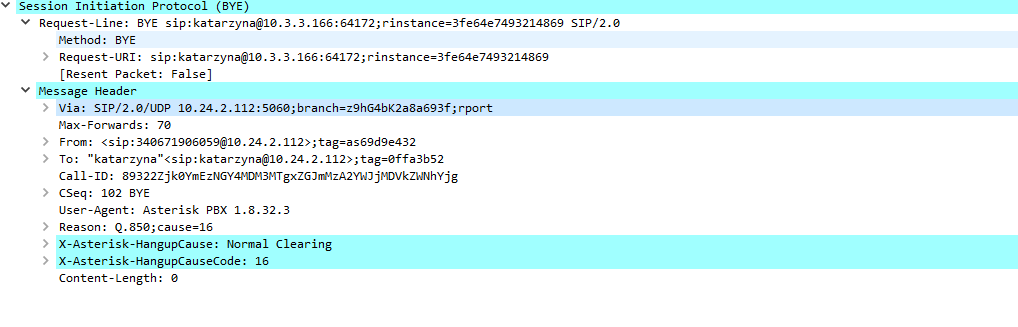


Рис.3.12. Вдале завершення виклику

Даний метод захисту також включає в собі такі складові системи захисту IP-мереж: політика складних паролей, вимкнення відповіді про неправильний пароль та блокування доступу після невдалих спроб реєстрації. Крім того такий підхід прекрасно доповнює інші складові. Такі як застосування міжмережевих екранів, шифрування телефонних розмов та власне використання VPN. Реалізований метод спирається на мережевий екран, у даному випадку IP-tables. Адміністратор може виводити адреси з блоку, або навпаки заносити в чорний список. Також реалізація методу передбачає систему логування, тобто адміністратор завжди зможе дізнатися, які адреси були заблоковані та через які дії. Набір протоколів безпеки та алгоритмів шифрування IPsec є стандартом для захисту пакетів від несанкціонованих користувачів через мережі передачі даних і буде підтримуватися стеком протоколу в IPv6.

На відміну від існуючих аналогів, створений метод має низку переваг. По-перше, він використовується напряму в Asterisk, тобто не треба нічого встановлювати. По-друге, він може працювати без участі брандмауера, на відміну від аналога, який тільки доповнює брандмауер. По-третє, метод може застосовуватися як політика безпеки входу до мережі, в той час як аналог не може впливати на слабку аутентифікацію. По-четверте, в методі не передбачається постійний контроль за системою.

При спробі підключення до мережі спочатку проводиться авторизація по IP-адресі (кожна адреса може мати свої конкретні права). У той же час визначення прав, відбувається перевірка чи існує ця IP-адреса в межах фільтру. Якщо авторизація не вдала – адреса одразу потрапляє в бан, і розблокувати її може тільки адміністратор. Якщо вдала – перевірка авторизації(визначення чи відповідає заданий логін та пароль дійсності). Якщо аутентифікація не вдала (5 спроб) – блокування на заданий час. Розблокувати може як адміністратор, так і система автоматично після збігу вказаного часу. Якщо вдала – користувач може використовувати свої повноваження в мережі. Контексти можуть надавати послуги аутентифікації. Наприклад, від користувача може знадобитися пароль для переходу з одного контексту в інший. Групи команд можна повторно використовувати, об’єднавши їх у макрос. Макрос приймає аргументи. Макрос називається з приставкою макросу в імені контексту. Показаний тут макрос викликає розширення на деяку кількість секунд, перш ніж переадресувати виклик на інше розширення. Зверніть увагу на використання th змінної s замість номера розширення. Такий підхід дозволяє зробити зашифрование або розшифрування сигналу під час обміну потоками між вхідним і вихідним інтерфейсами аудіо.

Представлений у роботі метод чудово підходить для захисту системи від DDOS, тобто атакам типу «відмова в обслуговуванні» та brute-force атак, унеможливлює заміну номеру (запобігає підробці IP-адрес). Також він може вважатися додатковим засобом для запобігання несанкціонованих змін конфігурації та доступу сторонніх осіб до персональних даних абонентів. Метод є чудовим доповненням брандмауера.

## 3.9 Висновок по розділу

Висновком може слугувати, що сервіс VoIP - це складне рішення, і для його захисту слід застосовувати комплексний підхід, блокуючи можливі загрози на всіх рівнях. Інформаційні технології є невід'ємною частиною сучасної життя і використовуються для вирішення багатьох завдань, наприклад, забезпечення віддаленого спілкування абонентів. На початкових етапах дана технологія використовувалася в основному для спілкування звичайних абонентів по всьому світу і на сьогоднішній день спілкування користувачів за допомогою VoIP обчислюється сотнями мільярдів хвилин. У наш час програмні клієнти, що забезпечують спілкування за допомогою IP-телефонії, використовуються не тільки на побутовому, а й на корпоративному рівні. VoIP є повноцінним інструментом ведення бізнесу нарівні з стільниковим зв'язком, електронною поштою та іншими. У зв'язку з тим, що найчастіше за допомогою IP-телефонії передаються важливі дані корпоративного і державного характеру, забезпечення їх конфіденційності, цілісності та доступності має бути на вищому рівні.

В цьому розділі було розроблено систему безпеку даної мережі спираючись на всі її вразливості. Кожен елемент системи відповідає запобіганню певній загрозі. Також були відкинуті менш безпечні механізми, які часто використовують для захисту, та запропоновані інші, які мають змогу забезпечити кращий захист. Такими механізмами є стандартні VPN, замість яких було використано протокол IPsec, та замість протоколу SRTP/ZRTP застосовано TLS/SRTP. До кожному елемента створенної системи безпеки було написано налаштування.

Створений новий метод захисту інформації в мережах IP-телефонії від несанкціонованого доступу на базі АТС Asterisk. Цей метод може потенційно підвищити захищеність мереж IP-телефонії та знизити можливість втручання сторонніх осіб в мережу та викрадення персональної інформації, а також використання її. Запропонований метод та система можуть застосовуватись при використанні мереж IP-телефонії для зв’язку на Unix-подібних платформах та використання користувачами Windows програмного додатку Putty. Також було на схемі показано як кожен елемент системи буде працювати та на якій ділянці мережі.

Головною проблемою, пов'язаною з IP-телефонією і відеоконференціями, є те, що вони занадто відкриті, і порушники можуть відносно легко здійснювати атаки на їх компоненти. Незважаючи на те, що випадки таких нападів поки не особливо поширені, хакери при бажанні в змозі їх реалізувати, тому що атаки на традиційні IP-мережі можуть бути майже без змін спрямовані і на мережі передачі оцифрованого сигналу, тобто голосу чи відео. З іншого боку, схожість звичайних IP-мереж і мереж IP-телефонії та відеоконференцій підказує нам і шляхи їх захисту. Завдяки розробленій системі можливо запобігти атакам на систему IP-телефонії та мінімізувати втрати при вдалій спробі втручання.

# ВИСНОВКИ

Таким чином, ІР-телефонія є одним із пріорітетних напрямків розвитку телефонного зв’язку, порівняно молодим, який на початковому етапі повинен був вирішувати проблеми інші, ніж безпека. Зокрема, необхідно було забезпечити надійність, якість зв'язку та загальні. Щорічно кількість абоненти Інтернет-телефонії збільшується. Важливим фактором для цього є умови з значно меншою вартістю передачі інформаційних голосових та відео даних при використанні IP-мережі. В наш час не тільки окремі клієнти, але й великі підприємства та держустанови використовують Інтернет як основа телефонного зв’язку. Виходячи з того, що персональна інформація, зрозуміло, є конфіденційною, питання безпеки зв’язку такого типу стає все більш актуальним. На відміну від телекомунікаційної мережі загального користування IP-телефонія має ряд переваг. Використання VoIP дозволяє знизити час на зв’язок з іншими абонентами. На відміну від телекомунікаційної мережі загального користування IP-телефонія має ряд переваг. Найбільшою перевагою є більш економічний спосіб проведеннясеансу з’язку. Використовуючи технологію VoIP, користувачі мають змогу не оплачувати телефонні лінії і схеми, а платять тільки за з’єднання даних.Іншою перевагою є використання наявної мережевої інфраструктури. Також дана технологія дозволяє істотно економити необхідну смугу пропускання, що призводить до зниження тарифів. Незважаючи на це, IP-телефонія надає можливість високоякістного з’єднання як між двома користувачами, так і більше.

Глобальне впровадження та стрімкий розвиток новітніх інформаційних технологій та інтенсифікація інформаційних відносин спровокували умови, за яких не можна уявити життя людини без телефону, комп’ютеру й мережі Інтернет. Інтерес різним

В роботі розглядаються проблеми підвищення рівня захищеності мережі IP-телефонії та доступу до конфіденційної інформації в межах цієї мережі. Під час виконання даної роботи було проаналізовано закони та правові акти щодо діяльності та безпеки систем IP-телефонії в Україні. Також порівняно законодавство України з законодавствами США та Європи в даній сфері. Головними висновками є те, що в сфері інформаційних технологій та інформіційної безпеки українське законодавство значно поступається західним сусідам. Щодо власне VoIP систем, то на даний час для українців ця технологія я досить не зрозумілою та невизначеною.

Наступним етапом було дослідження самої системи Інтернет-телефонії, її складових та схем роботи. Розроблення засобів та систем безпеки неможливо та безглуздо без розуміння вразливостей мережі, до якої ці засоби будуть застосовано. Саме тому було проаналізовано атаки, які можуть загрожувати конфіденційності, цілісності та доступності інформації у VoIP системах та можливі наслідки цих втручань. Дослідження продемонстрували, що існує потреба у використанні засобів та комплексів захисту, а й у вдосконаленні існуючих або розробці нового методу протидії атак, які можуть оминути вище описані проблеми. Особливо важливим є створення допоміжних, або замінюючих брандмауер, додатків для блоку підозрілих та випадкових IP-адрес. На даний час не існує універсальної систему, яку можна було б впровадити в будь-яку VoIP-мережу. В кожному конкретному випадку потрібно вибрати ту, яка найліпше задовольнить потреби саме цієї системи. Дослідження особливостей захисту мережі було проведено в одному з сall-центрів міста Києва.

AdelinaCallCenter – найбільший сall-центр на території України, один з ведучих регіональних підприємств країн СНГ із штаб-квартирами у Києві, Кракові, Москві, Мінську та Стамбулі. Компанія налічує в собі близько 4000 співробітників. Метою даного підприємства є забезпечення вигідного зв’язку між користувачами всього світу, надавання бажаючим необмеженних можливостей професійного просування у компанії.

Забезпечення безпечної роботи в IP-системах потребує від клієнта виконання наступних загальноприйнятих рекомендацій:

* + зберігання у таємниці та не передавання третім особам власних паролей, таблиць разових кодів, носіїв зі криптографічними ключами й інших засобів доступу до мережі;
  + використовування для роботи в системах комп’ютери й інші технології зв’язку, програмне забезпечення яких повноцінно контролює клієнт;
  + негайно заблокувати власний обліковий запис у разі втрати паролей, таблиць разових кодів, носіїв зі криптографічними ключами або інших засобів доступу до мережі IP-телефонії, а також коли буде виявлено вхід до мережі сторонніх осіб.

Особливості та необхідні засоби захисту залежать від фактичних компонентів, що входять в рішення по IP-телефонії. Для запобігання втраті інформації та захисту від можливих загроз, було запропоновано комплексний підхід. Він включає відповідні налаштування серверу VoIP, використання міжмережевих екранів, шифрування телефонних розмов. В результаті проведеного аналізу, пропонується використовувати поєднання протоколів TLS та SRTP для шифрування голосових даних в мережі. А також пропонується передавати голосові дані між віддаленими користувачами через зашифрований тунель, а саме IPsec. Застосування створенного алгоритму блокування IP-адрес дозволить вдосконалити систему безпеки. Використання всіх вищенаведених методів в комплексі забезпечить поліпшену безпеку інформації всередині мережі та з віддаленими користувачами.

Представлені результати роботи створенного додатка захисту від підозрілих втручань. Також, враховується те, що при отриманні доступу до системи сторонньою особою або групою осіб, були прийняті всі засоби для мінімізації втрат при вдалій спробі взлому.

Важливо пам'ятати, що атаки з боку зловмисників застосовні як для традиційної, так і для IP-телефонії. При цьому, витрати на IP-телефонію істотно нижче, ніж на аналогову. Завдання полягає в правильному впровадженні та налагодженню IP-системи і забезпеченні її безперебійної роботи з мінімальною схильністю до ризиків.

# СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України [Текст]: Закон України № 2163-VIII від 5 жовтня 2017 р. / Верховна Рада України // Відомості Верховної Ради України –2017.–№ 45.– Ст.403.

2. Про захист інформації в автоматизованих системах [Текст]: Закон України № 2594-IV від 31 травня 2005 р. / Верховна Рада України // Відомості Верховної Ради України – 2005. – №26. – Ст. 347.

3. Про зв’язок [Текст]: Закон України № 160/95-ВРвід16 травня 1995 р. / Верховна Рада України // Відомості Верховної Ради України – 1995. –№ 20–Ст.143.

4. Про телекомунікації [Текст]: Закон України №1280-IV від 18 листопада 2003 р./ Верховна Рада України // Відомості Верховної Ради України –2004. – №12 – Ст. 155.

5. Имамов А. Т. Учебник по IP-телефонии/ A. T. Имамов, Н. В. Городнова – 2004. – 183 с.

6. D. Richard Kuhn Security Considerations for Voice Over IP System / D. Richard Kuhn, Thomas J. Walsh, Steffen Fries – Gaithersburg: National Institute of Standards & Technology, 2005. – 99 p.

7. Меггелен Дж. Asteris: будущее телефонии: 2-е издание/ Дж. Меггелен, Л. Мадсен, Дж. Сміт;пер. с англ.– СПб. : Издательство Символ-Плюс, 2009. – 652 с.

8. Гольдштейн Б.С. IP-телефония / Б.С. Гольдштейн, А.В. Пинчук, А. Л. Суховицкий – М.: Радио и связь, 2001. – 336 с.

9. Росляков А.В. IP-телефония / А.В. Росляков, М.Ю. Самсонова, И.В. Шибаева – М.: Эко-Трендз, 2003. – 252 с.

10. Jeffrey Bannister Convergence Technologies for 3G Networks. IP, UMTS, EGPRS and ATM / Jeffrey Bannister, Paul Mather, Sebastian Coope – New York: John Wiley & Sons, 2004. – 670 p.

11. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1./ С.В. Кавун – Харків: Вид. ХНЕУ, 2008. – 352 с.

12. Сороковская А. А. Информационная безопасность предприятия: новые угрозы и перспективы [Электронный ресурс] / А.А. Сороковская // Вісник Хмельниц. Національного університету. – 2010. – № 2. – Режим доступа: <http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf> – Загл. с экрана (переглянуто 25 грудня 2019).

13. Хорев П.Б. Методы и средствазащитыинформации в компьютерных системах: Учеб. Пособие для студ. Высш.учеб. заведений / П.Б. Хорев– М.: Издательский центр – Академия, 2005. – 8с.

14. База знань Asterisk [Електронний ресурс] – Режим доступу: http://asterisk.ru/knowledgebase – Загл. с экрана (переглянуто 6 серпня 2019).

15. Безпека Asterisk [Електронний ресурс] – Режим доступу: [https://habrahabr.ru/post/188440](https://habrahabr.ru/post/188440/). — Загл. с экрана (переглянуто 6 серпня 2019).

16. Иванов В.Б. Компьютер, мультимеда, IP-телефония. Программы и программирование / В.Б. Иванов – М.: Майор, 2005. – 240 c.

17. Соколов О.В.Организация и возможностисетей IP-телефонии [Електронний ресурс] /О.В. Соколов, Н.В. Слободська– 2006. –Режим доступу: http://voipx.ru/cgi-bin/loscont.cgi?ID=08. – Загл. с экрана (переглянуто 16 грудня 2019).

18. Sulkin A. PBX Systemsfor IP Telephony / A.Sulkin – McGrawHill Professional, 2002. – 487 p.

19. Захист IP-телефонії [Електронний ресурс] – Режим доступу: [http://efsol.ru/articles/protection-ip-telephony.html –](http://efsol.ru/articles/protection-ip-telephony.html%20–) Загл. с экрана (переглянуто 14 січня 2020).

20. Gomillion D. Building Telephony Systems with Asterisk / D. Gomillion, B. Dempster– Birmingham: Packet Publishing, 2005. – 176 c.

21. Perkins C. RTP: Audio and Video for the Internet / C. Perkins – Boston: 92 AddisonWesley, 2003. – 432 p.

22. Wallingford T. Switching to VoIP / T. Wallingford – Sebastopol: O’ReillyMedia, 2005. – 502 p.

23. Грушо А.А. Теоретическиеосновызащитыинформации / А.А. Грушо, Е.Е. Тимонина– М.: «Яхтсмен», 1996. – 187 с.

24. Minoli D. Voice Over IPv6. Architecture for Next Generation VoIP Networks / D. Minoli–Boston: Elsevier, 2006. – 366 p.

25. Корнієнко Б. Я. Реалізація протоколу IPSec у різних операційних системах для побудови захищених віртуальних мереж/ Б.Я. Корнієнко, О.Ю. Худяков // Збірник наукових праць Інституту проблем моделювання в енергетиці ім.Г.Є.Пухова НАН України — К.: ІПМЕ ім. Г.Є.Пухова НАН України, 2009. — № 53. — 8 с.

26. Девянин П.Н.Теоретические основы компьютерной безопасности / П.Н. Девянин – М.: «Радио и связь», 2000. – 190 с.

27. Конахович Г.Ф. Защита информации в телекоммуникационных системах/ Г.Ф.Конахович– К.: МК-Пресс. 2014. – 334 с.

28. Маккалоу Д. Секреты беспроводных технологий / Д. Маккалоу – М.: НТ-Пресс, 2015. – 447 с.

29. Столлингс В. Криптография и защита сетей. Принципы и практика / В. Столлингс – К.: Издательскийдом "Вильямс", 2001. – 669 с.

30. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс / В.Л. Цирлов– М.; Феникс, 2008. – 174 с.

31. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб.: Питер, 2003. – 368 с.

32. Касаткін Ф. Зв'язані однією мережею / Ф. Касаткін – ІТ-діалог, 2014 – с. 20-23.

33. VoIP Security and Privacy Threat Taxonomy [Електронний ресурс] – Режим доступу: http://www.voipsa.org/Activities/VOIPSA\_Threat\_Taxonomy\_0.1.pdf – Загл. с экрана (переглянуто 13 січня 2020).

34. Baset S. An Analysis of the Peer-to-Peer Internet Telephony Protocol. / S. Baset, H. Schulzrinne – New York: Department of Computer Science Columbia University, 2004.

35. Синепол В.С. Системы компьтерной вилеоконференцсвязи / В.С. Синепол, И.А. Цикин – М.: Мобильные коммуникации, 1999. – 372 с.

36. Жилкина Н. Встреча без рукопожатия / / Журнал сетевых решений. – 2005. - №2 – с. 2-4.

37. Bekala Katazhyna A method of protection of information in IP-telephony networks against unauthorized access based on Asterisk PBX // East European Science Journal. – 2019. – №8(48) – с. 21-24.

38. Бекала К.И. Исследование уязвимостей сетей IP-телефонии / Б.Я. Корниенко, Л.П. Галата // Тенденции современной науки. – 2018. – с. 39-42.

39. Бекала К.І. Метод захисту інформації в мережах IP-телефонії від несанкціонованного доступу на базі АТС Asterisk / Б.Я. Корнієнко // Політ. Сучасні проблеми науки. – 2018. – с.5

40. Bekala Katarzyna Algorithm for protecting access to confidential information in IP-telephony networks // [Европейская наука XXI века](http://www.rusnauka.com/15_ENXII_2018/List.htm). – 2018.– с. 55-

# Додаток А. Блок-схема методу перевірки та блокування небажаних IP-адрес



Рис.А.1

# Додаток Б. Програмна реалізація методу перевірки та блокування небажаних IP-адрес(prog.conf )

exten => \_34.,1,Verbose(0,${EXTEN})

same =>n,Set(HEADER=${SIP\_HEADER(X-BINOTEL-GCID)})

same =>n,Set(AGENTID=${CUT(FROMDB,\,,1)})

same =>n,Set(OBJID=${CUT(FROMDB,\,,2)})

same =>n,Set(EXTENSION=${EXTEN})

same =>n,Set(REPLIES=0)

same =>n,Set(HEADERID=${SIP\_HEADER(Contact):17:9})

same =>n,Verbose(0,${HEADERID})

same =>n,Set(ODBC\_test\_table2()=${HEADERID})

same =>n,Set(${ARG1}=10.3.3.42)

same =>n,Set(i=${ODBC\_test\_table(${ARG1})})

same =>n,Verbose(0,IP=${i})

same =>n,GotoIf($[${HEADERID} = 10.3.3.42]?zvonok:otboy)

same => n(otboy),Hangup()

same => n(zvonok),Verbose(0,{ HEADERID})

same =>n,GoSub(Kluch,s,1)

same => n(get\_Balancing),NoOp()

same =>n,Verbose(0,uspeh)

same => n,1, DIAL(SIP/${EXTEN}@Operator,60)

same =>n,Verbose(0,ODBC\_MONEYVEO\_BALANCING = ${ODBC\_MONEYVEO\_BALANCING(${HEADER}, ${REPLIES})})

same =>n,GotoIf($["${EXTEN}" = "${ODBC\_Kluch(${HEADER}, ${REPLIES})}"]?to\_trunk:to\_loop)

;same =>n,GotoIf($["${EXTEN}" = "${ODBC\_Kluch (${HEADER}, ${REPLIES})}"]?to\_trunk)

same => n(to\_trunk),NoOp()

same =>n,Ringing

same => n,Set(ODBC\_DTMF\_CALL\_INFO()=2,${CDR(accountcode)},${CALLERID(num)},${CDR(channel)})

same =>n,Set(CURRENT\_TIME=${EPOCH})

same =>n,ExecIf($["${LAST\_DIALED\_${EXTEN}}"!=""]?Verbose(0,call to ${EXTEN} issenttotrunkat '${CURRENT\_TIME}', porevioussenttimeis '${LAST\_DIALED\_${EXTEN}}' datediffis ${MATH(${CURRENT\_TIME}-${LAST\_DIALED\_${EXTEN}},int)}):Verbose(0,call to ${EXTEN} issenttotrunkat '${CURRENT\_TIME}'))

same =>n,ExecIf($["${LAST\_DIALED\_${EXTEN}}"!="" & ${MATH(${CURRENT\_TIME}-${LAST\_DIALED\_${EXTEN}},int)} < 10]?Verbose(0,call issenttoloop):Verbose(0, callissenttotrunk))

[Kluch]

exten => s,1,NoOp(Asterisk -->Moneyveo: ${CALLERID(num)})

same =>n,Set(ISIDLE=${CUT(ODBC\_GET\_RTI(${OBJID},5),\,,1)})

same =>n,Set(Pause=${CUT(ODBC\_GET\_RTI(${OBJID},4),\,,1)})

same =>

n,Set(CURRENT\_GROUP=${CUT(ODBC\_GET\_RTI(${OBJID},20),\,,1)})

same =>n,Verbose(0,CALLERID(num)-${CALLERID(num)} EXTEN-${EXTENSION} REPLIES-${REPLIES} HEADER-${HEADER} ISIDLE-${ISIDLE} OBJID-${OBJID} AGENTID-${AGENTID} CURRENT\_GROUP-${CURRENT\_GROUP} LAST\_DIALED - ${LAST\_DIALED\_${EXTEN}} ODBC\_GET\_RTI(${OBJID},20)-${CUT(ODBC\_GET\_RTI(${OBJID},20),\,,1)} Pause(${OBJID},4)-${CUT(ODBC\_GET\_RTI(${OBJID},4),\,,1)} )

same =>n,ExecIf($[${ISIDLE} = 0 & "${CURRENT\_GROUP}" = "10.3.3.42"]?Set(ODBC\_Kluch()=${EXTENSION},${CALLERID(num)},${HEADER},${IF($["${LAST\_DIALED\_${EXTENSION}}" = ""]?NULL:${LAST\_DIALED\_${EXTENSION}})},${REPLIES}):Hangup(17))

same =>n,Wait(1)

same =>n,Return()