Хмельницький національний університет
Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів
Назва теми

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

КРМКІ. 015050.19.01.04 ПЗ

Виконав: студент 2 курсу, група КІ1м-19-1 _____ Гулечко М.С.
Підпис

Керівник доц., к. т. н, доцент кафедри КбКСМ _____ Джулій В.М.
Підпис

Нормоконтролер доц., к. т. н, доцент кафедри КбКСМ _____ Муляр І.В.
Підпис

До захисту допускаю:
Зав. кафедри КбКСМ, к.т.н., доц _____ Кльоц Ю.П.
Підпис

4. 12 2020 р.

Хмельницький, 2020

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ МАГІСТРА

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки та
комп'ютерних систем і мереж
к.т.н. доцент Кльоц Ю.П.
"4" 09 2020 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гулечко Михайло Сергійович
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів
Науковий керівник Джулій Володимир Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджена наказом № 118 ректора університету додаток №23 від 01.09.2020
2. Строк подання студентом проекту (роботи) на кафедру 3.12.2020.
3. Вихідні дані до проекту (роботи) Провести дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості. Розробити моделі нелегітимного абонента для оцінки рівня надійності безпечної IP-телефонії. Розробити метод оцінки параметрів IP-протоколів програмного розподілу ключів між кореспондентами IP-телефонії.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз стану та дослідження організації технологій безпечної IP-телефонії.,
Модель нелегітимного абонента забезпечення безпеки IP-телефонії
Імовірнісні алгоритми та методи забезпечення безпеки IP-телефонії
Дослідження ІЧХ протоколів розподілу ключів безпечної IP-телефонії.
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) 1,2.Тема, мета магістерської роботи, об'єкт, предмет, задачі дослідження, наукова новизна, практична цінність, апробація роботи. 3. Принципова схема підключення оператора VoIP. 4. Архітектурна модель підтримки якості IP – телефонії (QoS). 5. Варіанти дій нелегітимного абонента в схемі встановлення з'єднання клієнт – клієнт. 6,7. Модель нелегітимного абонента першого рівня безпечної IP – телефонії. 8. Метод підвищення ефективності IP – протоколу розподілення секретної інформації. 9, 10. Метод підвищення ефективності протоколу розподілення ключів на основі алгоритму Діффі – Хелмана. 11.Висновки.

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Відповідальний за оформлення КРМ	Муляр І.В., доцент, к.т.н		

7. Дата видачі завдання: «_1_» ___лютого_____2020_р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	*Примітка*
1	Грунтовне ознайомлення з предметною галуззю	2.02.2020	Виконано
2	Визначення структури магістерської роботи	2.03. 2020	Виконано
3	Робота над першим розділом магістерської роботи	1.04. 2020	Виконано
4	Робота над першою статтею за результатами обробки літературних джерел	1.05. 2020	Виконано
5	Робота над другим розділом магістерської роботи	1.06. 2020	Виконано
6	Робота над третім розділом магістерської роботи	1.09. 2020	Виконано
7	Робота над четвертим розділом магістерської роботи	1.10. 2020	Виконано
8	Підготовка ілюстративного матеріалу	1.11. 2020	Виконано
9	Оформлення текстової і графічної частини магістерської роботи	11.11. 2020	Виконано
10	Попередній захист магістерської роботи	21.11. 2020	Виконано
11	Захист ДРМ на засіданні ЕК	08.12. 2020	Виконано

Студент _____ Гудечко М.С.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Джулій В.М.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів».

Автор роботи: Гулечко Михайло Сергійович.

Керівник роботи: ктн. доц. Джулій Володимир Миколайович

Загальний обсяг роботи:: 109 сторінок., 40 рисунків., 4 таблиці., 36 посилань, 3 додатки.

МОДЕЛІ, МЕТОДИ, НЕЛЕГІТИМНИЙ АБОНЕНТА, АТАКА, ІНФОРМАЦІЙНА ВЗАЄМОДІЯ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, КАНАЛИ ЗВ'ЯЗКУ.

Мета роботи полягає в криптографічному захисту інформації в сеансах Інтернет-телефонії, що призведе до підвищення рівня безпечності голосового потоку по Internet мережах і на основі використання програмного розподілу ключів змешить час сеансу встановлення безпечного з'єднання.

Дана дипломна робота присвячена розробці методу виявлення нелегітимного абонента на основі алгоритму Діффі-Хелмана. Вирішує наступні задачі: надає можливість виявити активного нелегітимного абонента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності розподіленої секретної ключової інформації між кореспондентами, довіреного центру. Модель нелегітимного абонента може використовуватися при оцінці методів контролю рівня захищенності потоку даних з пакетною комутацією в Інтернет-телефонії, що надасть можливість збезпечення надійності IP-телефонії та підвищення захищенності.

4.12.2020 Дата

Підпис студента

ня прийняв

Прийняв

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

Виконано

С.

М.

ANNOTATION

a master's degree work of Gulechko Mikhail

entitled «A method of increasing the information security of IP-telephony taking into account the characteristics of key distribution protocols».

Mentor: Vladimir Dzhuliy

Total volume of work: 109 pages, 40 figures, 4 tables, 3 appendices, 36 references.

MODELS, METHODS, ILLEGITIMATE SUBSCRIBER, ATTACK, INFORMATION INTERACTION, CRYPTOGRAPHIC PROTECTION, COMMUNICATION CHANNELS.

The purpose of the work is to cryptographically protect information in Internet telephony sessions, which will increase the level of security of voice flow over Internet networks and based on the use of software key distribution will confuse the time of the session to establish a secure connection.

This thesis is devoted to the development of a method for identifying an illegitimate subscriber based on the Diffie-Hellman algorithm. Solves the following tasks: provides an opportunity to identify an active illegitimate subscriber who uses voice synthesis software; identify an active illegitimate IP subscriber - protocols in Internet telephony communication channels in the absence of distributed secret key information between correspondents, a trusted center. The illegitimate subscriber model can be used to evaluate methods of controlling the level of security of a packet-switched data stream in Internet telephony, which will provide an opportunity to ensure the reliability of IP telephony and increase security.

4.12.2020 Date  Signature

ЗМІСТ

стор.

Вступ……..…….. 7

1 Аналіз стану та дослідження організації технологій безпечної IP-телефонії ……..... 12

1.1 Дослідження протоколів криптографічного захисту потоку інформації з пакетною комутацією IP-телефонії …….……...…… 12

1.2 Особливості пакетної комутації в Інтернет мережах голосової передачі інформації.……...……. 22

1.3 Дослідження протоколів програмного розподілу секретної інформації між кореспондентами IP – телефонії …….……... 28

1.4 Протоколи забезпечення якості голосової передачі інформації в IP-телефонії …….……...…… 36

1.5 Постановка задачі ……..……...…….…...……. 42

2 Модель нелегітимного абонента забезпечення безпеки IP-телефонії 44

2.1 Безпека передачі голосової інформації в IP-телефонії ……..…... 44

2.2 Інформаційна безпека захищеної IP-телефонії …….…..... 49

2.3 Узагальнена модель нелегітимного кореспондента безпечної IP – телефонії ……...……...……..……...…….. 54

2.4 Модель нелегітимного абонента першого рівня безпечної IP - телефонії…… 57

2.5 Висновки ……..……..……..……. 64

3 Імовірнісні алгоритми та методи забезпечення безпеки IP-телефонії ….. 65

3.1 Модель нелегітимного абонента другого рівня безпечної IP - телефонії …….. 65

3.2 Оцінка імовірності нелегітимним абонентом успішного завершення атаки ……..……..……..……..… 77

3.3 Метод підвищення ефективності IP - протоколу розподілення

секретної інформації ZRTP ……..…….……..……... 81

3.4 Висновки ……..……..…….. 90

4 Дослідження ймовірнісно-часових характеристик протоколів розподілу ключів безпечної IP-телефонії ……..……. 91

4.1 Метод підвищення ефективності протоколу розподілення ключів на основі алгоритму Діффі – Хелмана …….……..…… 91

4.2 Метод оцінки ймовірнісно-часових характеристик протоколів IP-телефонії …….. 100

4.3 Висновки ……..…….……..……..... 105

Висновки…….……...…….……..…… 106

Перелік джерел посилання 107

Додаток А Код (лістинг) програмного забезпечення обміну ключами Діффі-Хелмана …… 110

Додаток Б Перелік наукових праць……...……..…….. 113

Додаток В Презентація……...…….…….……. 120

ВСТУП

Актуальність роботи. Забезпечення підвищення ефективності всіх галузей на сьогодні є однією з ключових проблем, тому актуальним сьогодення є необхідність в них впровадження і розвитку сучасних інформаційних технологій.

Поширення телефонії через Internet мережі під загрозу поставило прибутки операторів телефонних мереж. Проте, оператори AT&T, British Telecomunications, Deutsche Telecom, починають надавати послуги Internet-телефонії. Deutsche Telecom придбала частину Vocal Tec. Послугами передачі голосу через Internet мережі можна скористатися в багатьох містах і країнах. Аналогічні послуги передачі голосу через Internet мережі надають компанії WorldPort, Lucent, ITXC та інші. Найперспективнішими ринками передачі голосу через IP-мережі для IP-телефонії вважаються Австралія, США та Японія.

IP-телефонія - технологія передачі факсів, мультимедіа зв'язку, цифрування і стиснення голосового потоку по Internet мережах на базі протоколу IPv4(IPv6) з пакетною комутацією.

Поширенню IP-телефонії в Україні перешкоджає кілька факторів: не достатньо надійна інфраструктура Internet мереж каналів зв‘язку; не зацікавлені організації в розвитку IP-телефонії, які забезпечують телефонні мережі послугами зв‘язку. Таким чином, великі корпоративні компанії найбільш інтенсивно використовують IP-телефонію всередині. Лише кілька провайдерів надають послуги IP-телефонії - Infocom, IP Telecom, Sovam Teleport. Перераховані компанії можуть забезпечити якісні послуги Internet-телефонії. Традиційні телефонні мережі, мають якісніший зв'язок в порівнянні з Internet-телефонією, але є дорожчими в експлуатації. Перевагою Internet-телефонії є низька вартість міжміських і міжнародних переговорів, дозволяє зменшити витрати на послуги передачі факсів і мультимедіа зв'язку, за рахунок цифрування і стиснення голосового потоку. Internet-телефонія не використовує на шляху передачі інформації пакетів з голосовим сигналом дороге устаткування. IP-телефонія - високоякісна технологія, не використовує дорогі комутатори-маршрутизатори.

На основі проведеного огляду, можливо зробити висновок проте, що поширення Internet-телефонії послужили: застосуванням недорогих Internet мереж, в порівнянні з телефонними аналоговими мережами, з комутацією IPv4(6)-пакетів, а також мобільність і універсальність, що дозволяє перетворити голосовий потік в зашифровані і стисненні дані в будь-якій точці інфраструктури Internet мережі.

Розвиток нових IP-протоколів Internet мереж, а також передача потоку пакетних даних у вигляді голосових пакетів у відкритому виді через публічні мережі призвели до необхідності стандартизації IP-протоколів Internet мереж, а також криптографічного захисту даних для забезпечення безпечної Internet-телефонії. В результаті проведених заходів IP-протоколи Internet мереж розділені, в відповідності до вирішуваних задач на три групи: протоколи забезпечення захищеності і сигналізації, криптографічний захист пакетного потоку даних (медіа трафіку) і програмний розподіл ключів сучасними криптографічними алгоритмами генерації загальних ключів для медіа трафіку.

На сучасному етапі розвитку Internet-телефонії, телекомунікацій можливо спостерігати зростаючі обсяги трафіку Internet мереж зокрема в корпоративних мережах, а також в мережах Інтернет провайдерів, тут необхідно зазначити методи і технології, набір IPv4(6) - протоколів, методів і технологій, що забезпечують потік даних з комутацією пакетів у вигляді голосового спілкування в середовищі Інтернет мережі.

Стандартизація протоколів, а також масове використання персональних комп'ютерів операторами IP-телефонії в якості терміналів для послуг Інтернет телефонії, стандартизація Інтернет протоколів призвели до розробки спеціалізованого програмного забезпечення для Інтернет -телефонії, а також доступного програмного забезпечення (з відкритим кодом), що дало поштовх розширювати можливості IP-телефонії і використовувати криптографічні алгоритми та алгоритми розподілу ключів для забезпечення надійності в Інтернет -телефонії.

Таким чином, дипломна робота, присвячена дослідженню алгоритмів криптографічного захисту потоку даних з комутацією пакетів, а також алгоритмів

програмної генерації та розподілу ключів, для забезпечення та підвищення інформаційної безпеки Інтернет-телефонії, а також удосконалення IPv4(6) протоколів для забезпечення ефективного і безпечного функціонування при роботі в Internet мережі по каналах зв'язку. Тема дипломної роботи є актуальною і відповідає вимогам сьогодення в IP-телефонії.

Проведений аналіз наукових досліджень технологій IP-телефонії в областях криптографічного захисту передачі інформації, забезпечення якості потоку даних з пакетною комутацією (передача голосових і медіа- файлів), надання якісних послуг IP-телефонії, архівація відео і голосової інформації, показав що на сьогодні питання безпечної Інтернет -телефонії є відкритим для сценарію точка-точка, у випадку не вироблення зазделегіть загального секретного ключа для операторів. Також залишаються відкритими питання як впливають IPv4(6)- протоколи на виконання норм встановлених під час експлуатації безпечної IP-телефонії, в роботах мало уваги приділено імовірнісно-часовим характеристикам (ІЧХ) Інтернет протоколів забезпечення безпечної технології IP-телефонії. До загального недоліку розглянутих робіт слід віднести що в них, не описується така поширена атака на протоколи програмного розподілу ключів, як "зустріч посередині", тому виникає необхідність в розробці моделі нелегітимного абонента, яка буде враховувати атаку "зустріч посередині".

Об'єктом дослідження є технологія Інтернет-телефонії - безпечної передачі голосового потоку по Internet мережах на базі протоколу IP з пакетною комутацією потоку даних.

Предметом дослідження є застосування моделей, методів і IP – протоколів забезпечення криптографічного захисту та стиснення потоку даних при застосуванні технології Інтернет - телефонії. ІЧХ IP – протоколів.

Мета дипломної роботи і завдання дослідження. Мета роботи полягає в криптографічному захисту інформації в сеансах Інтернет-телефонії, що призведе до підвищення рівня безпечності голосового потоку по Internet мережах і на основі використання програмного розподілу ключів зменшити час сеансу встановлення безпечного з'єднання.

Відповідно до поставленої мети в дипломній роботі поставлені, і вирішені наступні задачі:

- дослідження існуючих криптографічних протоколів захисту інформації, а також протоколів програмного розподілення секретної інформації між кореспондентами зв’язку, для підвищення надійності IP-телефонії і впливу IP протоколів на параметри якості;

- розробка моделі нелегітимного абонента для оцінки рівня надійності безпечної IP-телефонії;

- розробка методу оцінки параметрів IP-протоколів програмного розподілу ключів між кореспондентами IP-телефонії;

- розробка методу, на основі алгоритму Діффі-Хелмана, виявлення нелегітимного абонента, IP - протоколів розподілу ключів між кореспондентами IP-телефонії.

Наукова новизна

1. Розроблена модель нелегітимного абонента. Модель нелегітимного абонента враховує атаку "зустріч посередині" на IP – протоколи, що надають можливість підвищення захищеності Інтернет-телефонії.

2. Метод виявлення нелегітимного абонента на основі алгоритму Діффі-Хелмана. Вирішує наступні задачі: виявити активного нелегітимного абонента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності розподіленої секретної ключової інформації між кореспондентами, довіреного центру.

Методи дослідження. Для вирішення поставлених задач в дипломній роботі використовувалися методи системного аналізу, імовірнісних графів, випадкових процесів і математичної статистики, теорії ймовірності, методів чисельного аналізу, комбінаторики.

Основні результати, отримані в дипломній роботі та виносяться на захист:

1. Модель нелегітимного абонента. Модель нелегітимного абонента враховує атаку "зустріч посередині" на IP – протоколи, що наддасть можливість підвищення захищеності Інтернет-телефонії.

2. Метод виявлення нелегітимного абонента на основі алгоритму Діффі-Хелмана. Вирішує наступні задачі: виявити зловмисника, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності розподіленої секретної ключової інформації між кореспондентами, довіреного центру.

Практична цінність результатів дипломної роботи. Модель нелегітимного абонента може використовуватися при оцінці методів контролю рівня захищеності потоку даних з пакетною комутацією в Інтернет-телефонії, що надають можливість забезпечення надійності IP-телефонії та підвищення захищеності.

Достовірність наукових положень, висновків отриманих в дипломній роботі результатів підтверджується коректною постановкою задач, результатами моделювання та апробацією результатів отриманих на конференціях, коректністю використовуваного математичного апарату. Отримані в ході виконання дисертаційного дослідження результати не суперечать раніше отриманим даним, описаним в літературі іншими авторами.

Особистий внесок. Всі дослідження, викладені в дипломній роботі, проведені автором в процесі наукової діяльності. Результати, які виносяться на захист, отримані автором особисто, запозичений матеріал позначений в роботі посиланнями.

Апробація роботи. За темою дипломної роботи ОКР «Магістр» опубліковано 1 теза та 1 стаття.

Структура і обсяг роботи. Дипломна робота ОКР «Магістр» складається зі вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел. Загальний обсяг роботи - 109 сторінок. Робота містить 40 рисунків та 4 таблиці. Список використаної літератури включає 36 бібліографічних джерела.

1 АНАЛІЗ СТАНУ ТА ДОСЛІДЖЕННЯ ОРГАНІЗАЦІЇ ТЕХНОЛОГІЙ БЕЗПЕЧНОЇ IP-ТЕЛЕФОНІЇ

1.1 Дослідження протоколів криптографічного захисту потоку інформації з пакетною комутацією IP-телефонії

Засоби мережної безпеки забезпечують: запобігання порушень безпеки, які виникають при передачі інформації з мереж; міри, що дозволяють визначати, що такі порушення безпеки мали місце.

Характерні проблеми, пов'язані з безпекою, які виникають при використанні комп'ютерних мереж: при пересиланні із загальнодоступної Internet мережі конфіденційної інформації необхідно бути впевненим, що ніхто не зможе підглянути, змінити цю інформацію; при керуванні віддаленим комп'ютером, необхідно бути впевненим, що ніхто не зможе перехопити керуюче повідомлення, змінити його вміст і відправити повідомлення на даний комп'ютер; отримання несанкціонованого доступу (НСД) до віддаленого комп'ютера із правами законного користувача, або, маючи право доступу до комп'ютера, одержати доступ з набагато більшими правами; при відкритті фірмою сайта в Internet. У якийсь момент вміст сайту заміняється новим, або виникає такий потік і такий спосіб звертань до сайту, що сервер не справляється з обробкою запитів. У результаті звичайні відвідувачі сайту або бачать інформацію, що не має до фірми ніякого відношення, або просто не можуть потрапити на сайт фірми; при відкритті Internet-магазину, що приймає оплату в електронному виді, продавець повинен бути впевнений, що він відпускає товар, що дійсно оплачений, а покупець повинен мати гарантії, що він, по-перше, одержить оплачений товар, а по-друге, номер його кредитної картки не стане нікому відомий.

Розглянемо основні поняття, що відносяться до інформаційної безпеки, і їхній взаємозв'язок. Власник визначає множину інформаційних цінностей, які повинні бути захищені від різного роду атак. Атаки здійснюються супротивниками або

опонентами, які використовують різні вразливості в цінностях що захищаються. Основними порушеннями безпеки є розкриття інформаційних цінностей (втрата конфіденційності), їхня неавторизована модифікація (втрата цілісності) або неавторизована втрата доступу до цих цінностей (втрата доступності). Власники інформаційних цінностей аналізують вразливості ресурсів, що захищаються, і можливі атаки, які можуть мати місце в конкретному оточенні. У результаті такого аналізу визначаються ризики для даного набору інформаційних цінностей. Цей аналіз визначає вибір контрзаходів, що задається політикою безпеки й забезпечується за допомогою механізмів і сервісів безпеки. Необхідно враховувати, що окремі вразливості можуть зберегтися й після застосування механізмів і сервісів безпеки. Політика безпеки визначає погоджену сукупність механізмів і сервісів безпеки, адекватну цінностям що захищаються, і оточенню, у якому вони використовуються. На рис. 1.1 показаний взаємозв'язок розглянутих понять інформаційної безпеки.

Приведемо наступні визначення: вразливість — слабке місце в системі, з використанням якого може бути здійснена атака. Ризик — імовірність того, що конкретна атака буде здійснена з використанням конкретної вразливості. Кожна організація повинна прийняти рішення щодо припустимого для неї рівня ризику. Це рішення повинне знайти відображення в політиці безпеки, прийнятої в організації. Політика безпеки — правила, директиви й практичні навички, які визначають то, як інформаційні цінності обробляються, захищаються й поширюються в організації та між інформаційними системами; набір критеріїв для надання сервісів безпеки. Атака — будь-яка дія, що порушує безпеку інформаційної системи (дія або послідовність зв'язаних між собою дій, що використовують вразливості даної інформаційної системи і приводять до порушення політики безпеки. Механізм безпеки — програмне і/або апаратний засіб, що визначає і/або запобігає атаці. Сервіс безпеки — забезпечує безпеку систем і/або переданих даних, або визначає здійснення атаки, що задаються політикою. Сервіс використовує один або більше механізмів безпеки.

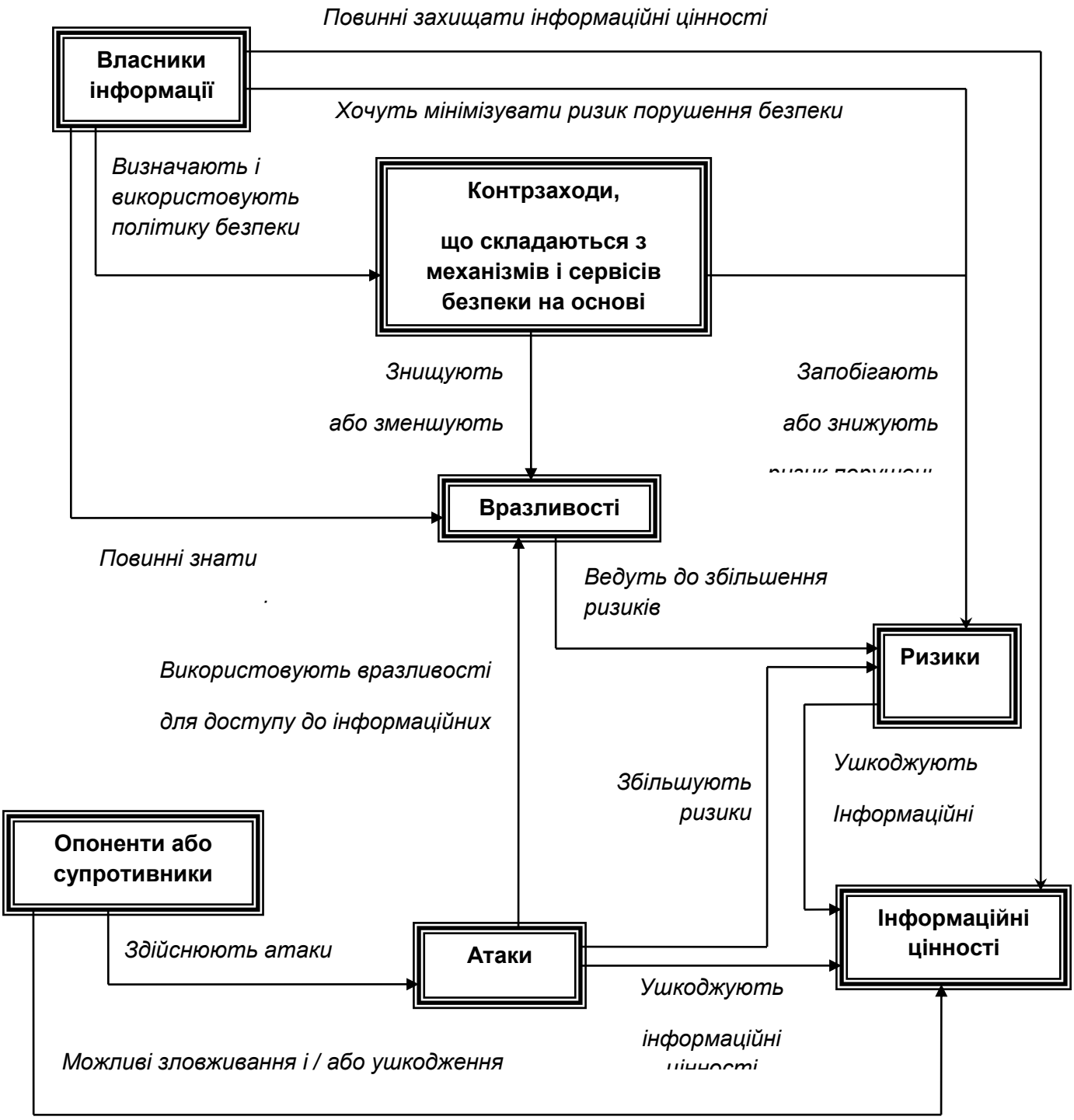


Рисунок 1.1 - Взаємозв'язок основних понять безпеки інформаційних систем

Класифікація мережних атак. У загальному випадку існує інформаційний потік від відправника (файл, користувач, комп'ютер) до одержувача (файл, користувач, комп'ютер (рис.1.2):

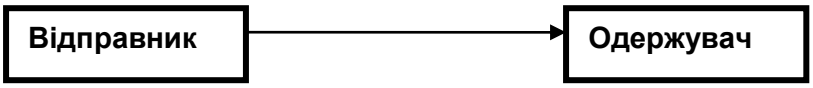


Рисунок 1.2 - Інформаційний потік

Всі атаки можна поділити на два класи: пасивні й активні.

Пасивна атака - атака, при якій супротивник не має можливості модифікувати передані повідомлення й вставляти в інформаційний канал між відправником і одержувачем свої повідомлення. Метою пасивної атаки може бути тільки прослуховування переданих повідомлень і аналіз трафіка (рис. 1.3).

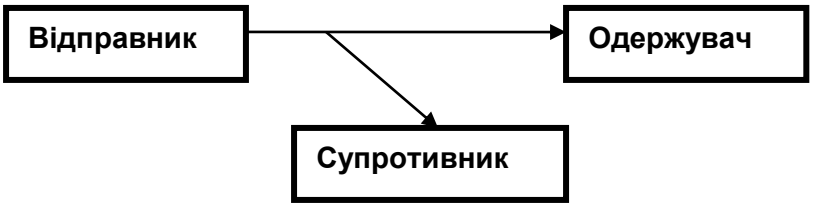


Рисунок 1.3 - Пасивна атака

Активна атака - атака, при якій супротивник має можливість модифікувати передані повідомлення й вставляти свої повідомлення. Розрізняють наступні типи активних атак:

1. Відмова в обслуговуванні — DoS-атака (Denial of Service) DoS-атака порушує нормальне функціонування мережних сервісів. Супротивник може перехоплювати всі повідомлення, що направляються певному адресатові. Іншим прикладом подібної атаки є створення значного трафика, у результаті чого мережний сервіс не зможе обробляти запити законних клієнтів. Класичним прикладом такої атаки в мережах TCP/IP є SYN-атака, при якій порушник посилає пакети, що ініціюють встановлення TCP – з’єднання, але не посилає пакети, що завершують встановлення цього з’єднання. В результаті може відбутися переповнення пам'яті на сервері, і серверу не вдасться встановити з'єднання із законними користувачами.

2. Модифікація потоку даних — атака «man in the middle» Модифікація потоку даних означає зміна порядку повідомлень або зміну вмісту повідомлення (рис.1.4). Поширена атака при використанні технології IP – телефонії.

Рисунок 1.4 - Атака «man in the middle»

3. Створення помилкового потоку (фальсифікація**)**

Фальсифікація (порушення аутентичності) означає спробу одного суб'єкта видати себе за іншого (рис. 1.5).

Рисунок 1.5 - Створення помилкового потоку

4. Повторне використання

Повторне використання означає пасивний захват даних з наступним їхнім пересиланням для одержання несанкціонованого доступу - replay-атака. Replay-атака є одним з варіантів фальсифікації, але в силу того, що це один з найпоширеніших варіантів атаки для одержання несанкціонованого доступу, його часто розглядають як окремий тип атаки (рис. 1.6).

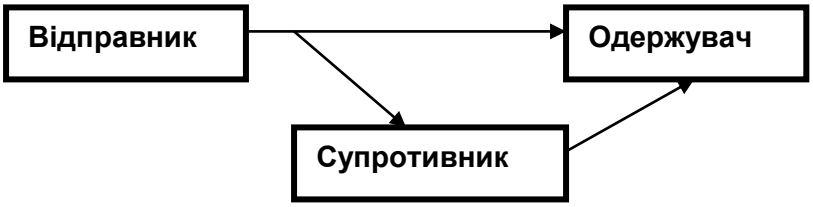


Рисунок 1.6 - Replay-атака

Наведена класифікація атак може існувати в будь-яких типах мереж і на будь-якому рівні моделі OSI, а не тільки в мережах, що використають як транспорт протоколи TCP/IP. В мережах, побудованих на основі протоколів TCP/IP, атаки зустрічаються найчастіше, тому що, Internet став найпоширенішою мережею. При розробці протоколів TCP/IP вимоги безпеки ніяк не враховувалися.

Дану особливість необхідно враховувати для забезпечення захищеності при використанні технології IP – телефонії.

Для криптографічного захисту потоку інформації з пакетною комутацією в Інтернет мережах голосової передачі даних виникає необхідність використання симетричних алгоритмів шифрування інформації. До переваг симетричних алгоритмів шифрування інформації слід віднести швидкість шифрування потоку даних та відносно невелика довжина ключа. Суттєвим недоліком симетричних алгоритмів шифрування інформації є програмний розподіл секретної інформації – ключа шифрування. Дану задачу вирішують алгоритми асиметричного шифрування інформації, більш детально розглянемо їх в розділі 1.3.

Модель безпечної Інтернет - мережної взаємодії при використанні симетричних алгоритмів шифрування потоку даних в загальному виді представлена на рис. 1.7.

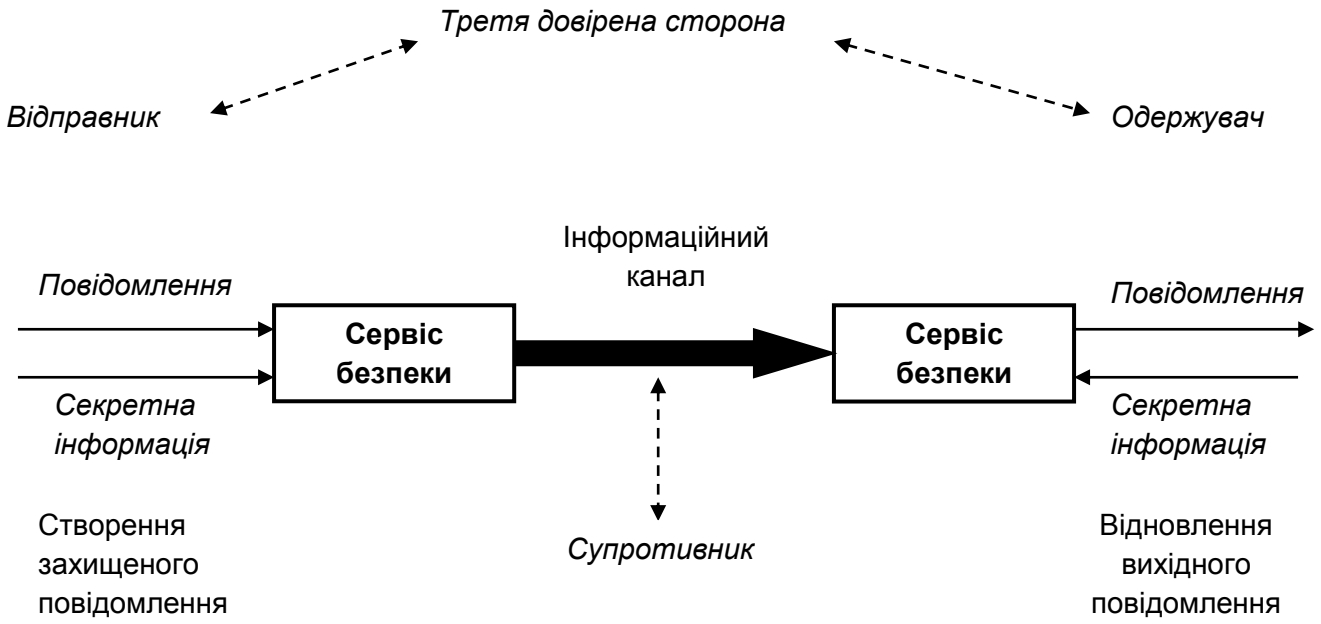


Рисунок 1.7 - Модель безпечної Інтернет - мережної взаємодії

Інформація, яка передається в Інтернет мережі від одного кореспондента іншому, проходить через різні типи мереж. Під час передачі потоку даних в Інтернет мережі встановлюється логічний інформаційний канал, з використанням комунікаційних IP - протоколів (наприклад, сокетні протоколи, TCP/IP). При

цьому необхідно задіяти засоби безпеки, для підвищення надійності передачі потоку даних, для захисту переданої інформації від нелегітимного абонента, що може мати загрозу аутентифікації, цілісності та конфіденційності.

Технології підвищення безпечної Інтернет - мережної взаємодії в своєму активі використовують дві компоненти:

1. Відносно захищена передача потоку інформації з комутацією пакетів. Засобом безпечної передачі даних є шифрування, інформація видозмінюється таким чином, що нечитається нелегітимним абонентом, доповнюється хеш кодом, отриманого з інформації, який використовується для аутентифікації оператора й забезпечення цілісності інформації.

2. Секретна інформація, яка розподіляється між абонентами і закрита для нелегітимного абонента (ключ шифрування). Для забезпечення надійності передачі інформації, в деяких випадках, використовується третя довірена сторона (third trusted party - TTP), яка може бути відповідальна за розподіл секретної інформації між абонентами Інтернет – телефонії.

Таким чином модель безпечної Інтернет - мережної взаємодії показує необхідність розв’язання три задачі, для розробки сервісу безпеки:

1. Для виконання надійної передачі потоку даних необхідно розробити алгоритм шифрування/дешифрування. Алгоритм повинен забезпечити неможливість дешифрування інформації нелегітимним абонентом, без секретної інформації.

2. Забезпечити секретною інформацією алгоритм шифрування/дешифрування.

3. Розробити IP-протокол обміну інформацією в Інтернет мережі для розподілу секретної інформації між абонентами IP – телефонії таким чином, щоб не стала доступною нелегітимному абоненту.

Проведемо огляд симетричних алгоритмів шифрування інформації при використанні IP – телефонії.

Симетричні алгоритмів шифрування при закритті інформації використовують криптографічні методи, класифікація яких представлена на рис. 1.8.

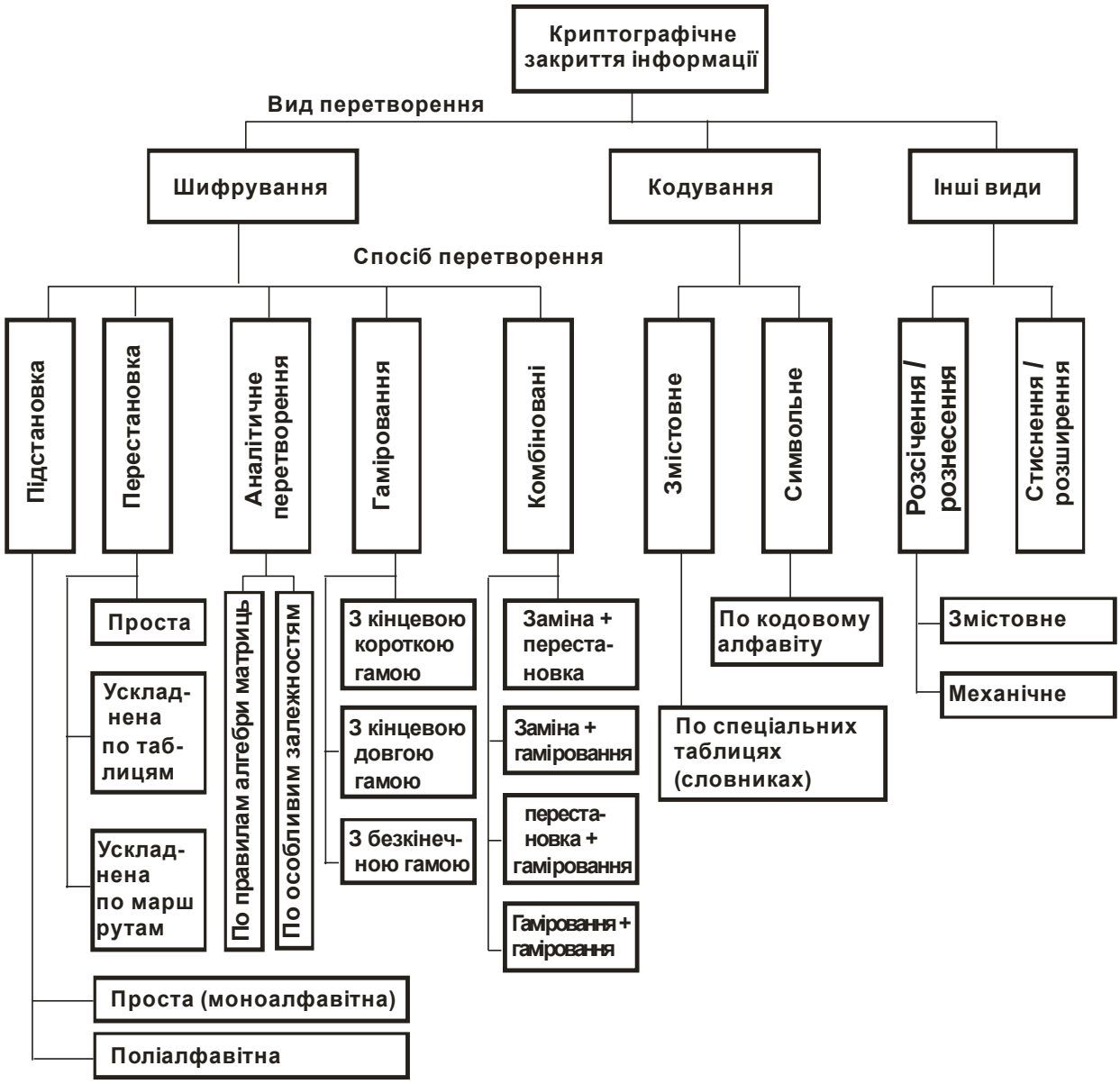


Рисунок 1.8 - Криптографічні методи закриття інформації

На рис. 1.9 представлена схема симетричних алгоритмів шифрування (традиційна криптографія).

Рисунок 1.9 - Симетрична криптографія

В процесі закриття інформації (шифрування потоку даних) використовується симетричний алгоритм шифрування, вхідна інформація - незашифроване повідомлення (plaintext), і секретна інформація (ключ). Вихідна інформація симетричного алгоритму - зашифроване повідомлення (ciphertext). Секретна інформація (ключ) значення, яке не залежить від повідомлення. Зміна секретної інформації призводить до видозміни зашифрованого повідомлення.

Розглянемо класичний алгоритм симетричного шифрування DES (Data Encryption Standard). Алгоритм DES представлений двома гілками класичною мережею Фейштеля. Інформація, яку необхідно шифрувати розбивається на 64 – бітні блоки, при цьому використовується 56-бітний ключ. Алгоритм DES шифрує інформацію за 16 раундів. Процес шифрування потоку даних виконується в чотири етапи. На першому - виконується забілювання (початкова перестановка IP) 64-бітного блоку, біти переупорядковуються у відповідності зі стандартною таблицею. Другий етап виконує функцію операції зсуву й підстановки в 16-и раундах. На наступному етапі блоки виходу останньої (16-й) ітерації міняються місцями. На четвертому етапі виконується IP^{-1} перестановка результату.

На рис. 1.10 представлена загальна схема виконання алгоритму DES, а також генерація підключа раунда.

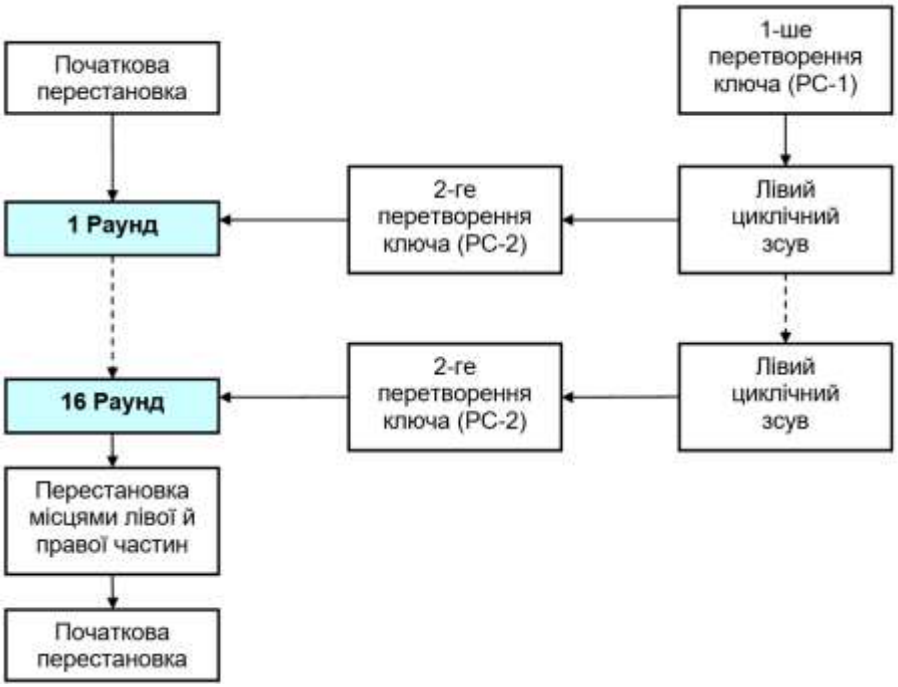


Рисунок 1.10 - Схема виконання алгоритму DES, генерація підключа раунда

На рис. 1.11 показано і-й раунд виконання алгоритму DES.

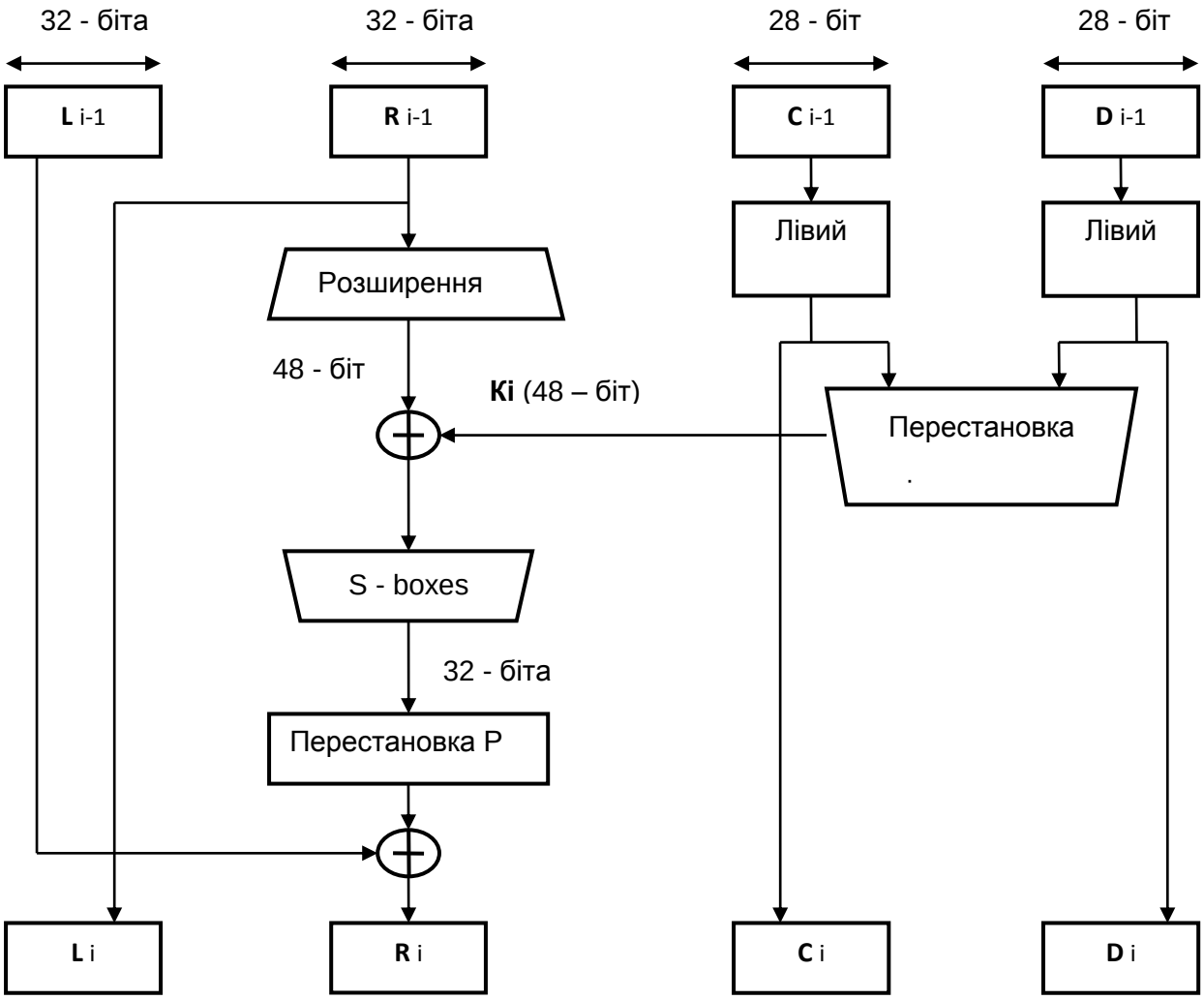


Рисунок 1.11- і-й раунд виконання алгоритму DES

Недоліком DES є недостатня довжина ключа, існує 2^{56} можливих ключів, що є недостатнім для захисту від застосування лобових атак.

Альтернативою DES на сучасному етапі є використання потрійного DES – довжина ключа 112 біт, алгоритм IDEA - для шифрування даних використовує 128-бітовий ключ. Недоліки IDEA: значно повільніший за Rijndael (майже в два рази); IDEA запатентований, що перешкоджає його вільному поширенню; не передбачається збільшення довжини ключа. Роботи по криптоаналізу IDEA не всі опубліковані, цілком можливо, що алгоритм IDEA зламаний, або буде зламаний найближчим часом. Алгоритм Rijndael **(**Advanced Encryption Standard**)**, прийнятий

на сьогоднішній день, як новий стандарт на алгоритми симетричного шифрування. Алгоритм Rijndael - симетричний алгоритм шифрування потоку даних (розмір блоку 128 біт, секретна інформація (ключ) 128/192/256 біт), прийнятий урядом США в якості стандарту шифрування/дешифрування інформації за результатами конкурсу AES. Алгоритм Rijndael проаналізований криптоаналітиками і широко використовується, в якості альтернативи DES.

Таким чином, на проведеного аналізу алгоритмів симетричного шифрування рекомендується для криптографічного захисту потоку даних при використанні в IP -телефонії використовувати алгоритм Rijndael **(**Advanced Encryption Standard (AES)**)**, прийнятий як новий стандарт на алгоритми симетричного шифрування

1.2 Особливості пакетної комутації в Інтернет мережах голосової передачі інформації

Протоколи Інтернет-телефонії - протоколи, які працюють в мережі, використовуються для організації голосової передачі інформації (телефонних розмов) та для мультимедійної взаємодії поверх IP-мережі.

На сьогоднішній день не існує чіткого стандарту, який визначає роботу в Інтернет мережі протоколів IP-телефонії. Протоколи IP-телефонії можна умовно розділити на дві групи: протоколи управління встановленням з'єднання (сигнальні протоколи) і протоколи передачі потоку даних по пакетним мережам [7]. Розглянемо найбільш поширені з них з практичної точки зору.

Перша група протоколів - сигнальні протоколи (протоколи управління встановленням з'єднання) - призначені для координації взаємодії кореспондентів IP - телефонії, узгодження параметрів сеансу зв'язку, для установки і завершення встановлення з'єднання (дзвінків), та вирішення інших задач, не переносять інформації в IP - мережі, передають дану задачу іншим протоколам IP-телефонії [8]. До протоколів управління встановленням з'єднання (сигнальних) можна

віднести: H.323; SIP (Session Initiation Protocol); MGCP (Media Gateway Control Protocol) [9]; Skinny (SCCP); UNIStim [8].

Для передачі потоку даних по пакетним мережам використовуються протоколи: RTP (Real-time Transport Protocol); SRTP. Протокол IAX поєднує можливості протоколу для передачі потоку даних по пакетним мережам і протоколу управління встановленням з'єднання (сигнального протоколу).

Також існує декілька допоміжних протоколів, які використовуються в IP - телефонії, і не належать до перерахованих груп, але також використовуються при передачі потоку інформації в IP-мережах, це протокол RSVP.

Протокол RTP працює поверх UDP (User Datagram Protocol) протоколу. Таким чином протоколи UDP/RTP/IP забезпечують транспортний механізм для голосової передачі інформації IP - телефонії. Розглянемо протоколи забезпечення взаємодії при обслуговуванні сенсу зв’язку між абонентами. Протоколи сигналізації можуть працювати як поверх транспортного протоколу TCP так і поверх транспорту UDP. Таким чином, на основі протоколів IP/((UDP/TCP)/SIP/H.323/ MGCP) формується сигнальний механізм IP -телефонії для голосової передачі інформації і медіа трафіку в Інтернет мережі.

Більш детально розглянемо протоколи управління встановленням з'єднання (сигнальні). Протокол H.323 - протокол на рівні моделі OSI - містить стандарти для голосової передачі інформації і передачі мультимедіа в Інтернет мережах з пакетною передачею. Протокол H.323, представлений Міжнародним союзом електрозв'язку. Документ описує сукупність протоколів, які забезпечують роботу протоколів для голосової передачі інформації і передачі мультимедіа в Інтернет мережах з негарантованою якістю обслуговування. Протокол H.323 розроблявся для інтеграції телефонної мережі загального користування з Інтернет мережами передачі потоку даних, тому має досить складну структуру.

Протокол MGCP – керує VoIP-шлюзами. Управління встановленням з'єднання, координацію взаємодії кореспондентів IP - телефонії може бути реалізовано використанням протоколу MGCP. Архітектура протоколу MGCP

становить: шлюз - Media Gateway, виконує функції перетворення голосової інформації з телефонної мережі загального користування в Інтернет мережу з комутацією пакетів IP - телефонії; контролер шлюзів - Call Agent, забезпечує роботу та керування шлюзами; шлюз сигналізації - Signaling Gateway, забезпечує передачу інформаційного потоку (сигналізації), яка надходить з телефонної мережі загального користування, до Call Agent (контролера шлюзів) і в зворотному напрямку. Протокол MGCP надає забезпечення зосередження інтелекту розподіленого шлюзу в контролері і можливість розподілення функцій Call Agent (контролера шлюзів) між обчислювальними платформами.

SIP протокол - протокол, який відповідає за встановлення зв'язку між абонентами IP – телефонії всередині IP-мережі, для обміну голосовою інформацією, текстовою та відео - інформацією. SIP протокол забезпечує встановлення і завершення сеансу зв'язку. SIP протокол дозволяє здійснювати управління викликами в IP - телефонії [10]. SIP протокол працює поверх протокола, більш простий в порівнянні з протоколами H.323 і MGCP. Задача протоколу SIP - реалізувати абонентські пристрої і шлюзи більш інтелектуальними, для підтримки додаткових послуг для абонентів забезпечити розширюваність протоколу. Таким чином побудова мереж IP-телефонії на базі SIP протоколу простіша, ніж побудова мереж IP-телефонії на базі протоколів H.323 і MGCP.

На основі проведеного дослідження додатково можливо виділити декілька підсистем IP-телефонії, призначення яких надання послуг VoIP [2]: підсистема забезпечення захищеності IP-телефонії; підсистема забезпечення якості IP-телефонії; підсистема білінгу IP- телефонії і менеджменту IP- телефонії; підсистема додаткових послуг IP- телефонії; підсистема забезпечення управлінням викликами і адресацією IP- телефонії.

Розглянемо виділені підсистеми. Підсистема управління викликами і адресацією IP- телефонії бере на себе відповідальність за виконання базових

послуг VoIP: передача голосового трафіку в Інтернет мережі; організація викликів; і маршрутизацію викликів IP - телефонії.

Підсистема додаткових послуг IP - телефонії бере на себе відповідальність за надання додаткових сервісів абонентам Інтернет мережі IP-телефонії: забезпечення роумінгу, мобільності; надання додаткових сервісів (відео виклики, інформаційні сервіси і т.д). В основі підсистеми задіяні протоколи для надання додаткових послуг.

Підсистема забезпечення якості IP - телефонії бере на себе відповідальність за підтримку якості телефонного зв'язку, для досягнення цієї мети використовує відповідні протоколи, алгоритми і механізми підвищення якості IP - телефонії.

Підсистема забезпечення безпеки (захищеності) IP-телефонії бере на себе відповідальність за нерозголошення (закритість) переданої інформації, конфіденційність телефонних переговорів абонентів. Підсистема забезпечення безпеки (захищеності) IP-телефонії для досягнення поставленої задачі використовує відповідні протоколи, механізми, алгоритми для гарантування безпеки в Інтернет мережі IP-телефонії.

Підсистема білінгу IP- телефонії і менеджменту IP- телефонії бере на себе відповідальність за ведення обліку викликів абонентів, відслідкування тарифікації дзвінків і своєчасне та достовірне ведення взаєморозрахунків між абонентами та оператором, який надає відповідні послуги.

Для проведення відповідного аналізу та дослідження системи IP-телефонії необхідно визначити всі можливі сеанси зв’язку (сценарії) взаємодії кореспондентів. Сценарій можна визначити як сукупність активних елементів (протоколів, алгоритмів, механізмів), які приймають при обробці дзвінка, для досягнення кінцевої мети.

Розглянемо сценарій взаємодії кореспондентів, при якому в якості протоколу сигналізації на Інтернет мережі IP-телефонії використовується SIP протокол. А також було враховано при складанні схеми взаємодії, що згідно із законом про зв'язок, заборонено приєднання операторів з використанням VoIP. Таким чином

з'єднання різних VoIP операторів дозволяється тільки через телефонну мережу загального користування [11].

На рис. 1.13 представлена "Принципова схема встановлення з'єднання кореспондента VoIP". На прикладі принципової схеми встановлення з'єднання кореспондента VoIP (рис.1.13) розглянуті в Інтернет мережі IP-телефонії можливі варіанти сценаріїв обробки викликів: абонентами, IP-телефонними станціями (IP АТС, SoftSwitch), шлюзами Е1. На рис. 1.13 - показано два постачальника послуг IP-телефонії, оператор традиційної телефонії. Таким чином оператор 1 надає VoIP сервіси підключеним на мережі 1 абонентам. Оператор 1 використовує декілька IP АТС (SSx, де х - порядковий номер IP АТС). Імовірність виклику від абонента А1 абонента Інтернет мережі (Б1 або В1) вкрай мала для невеликих компаній. Таким чином будемо вважати найбільш поширені дзвінки абонентам, які підключені до інших операторів.

Можливі сценарії з'єднання: А1-SS1-GWl-ТМЗК-GW2-SS2-В2 (VoIP абонент однієї компанії через ТМЗК телефонує VoIP абоненту іншого оператора); Al-SSl-GWl-ТМЗК-Г (VoIP абонент однієї компанії через ТМЗК телефонує абоненту мережі ТМЗК іншого оператора); А1-SS1-SS2-В1 (VoIP абонент одного оператора телефонує абоненту цього ж оператора, підключеному до додаткової IP АТС оператора); Al-SSl-Б1 (VoIP абонент одного оператора телефонує абоненту цього ж оператора, при цьому абоненти підключені до однієї IP АТС); А2-Б2 (VoIP абонент одного оператора телефонує другому абоненту, при цьому виклик здійснюється між кореспондентами, минаючи IP АТС). Наведений приклад з'єднання А2-Б2? використовується, в разі необхідності організувати передачу абонентської лінії традиційної телефонії по мережах IP. З'єднатися без АТС може використовуватися для організації внутрішнього (службового) зв'язку в корпоративних мережах. З'єднатися без АТС також може бути між окремими абонентами глобальної Інтернет мережі, які мають потребу в захищеному режимі проведення сеансів телефонного зв'язку.

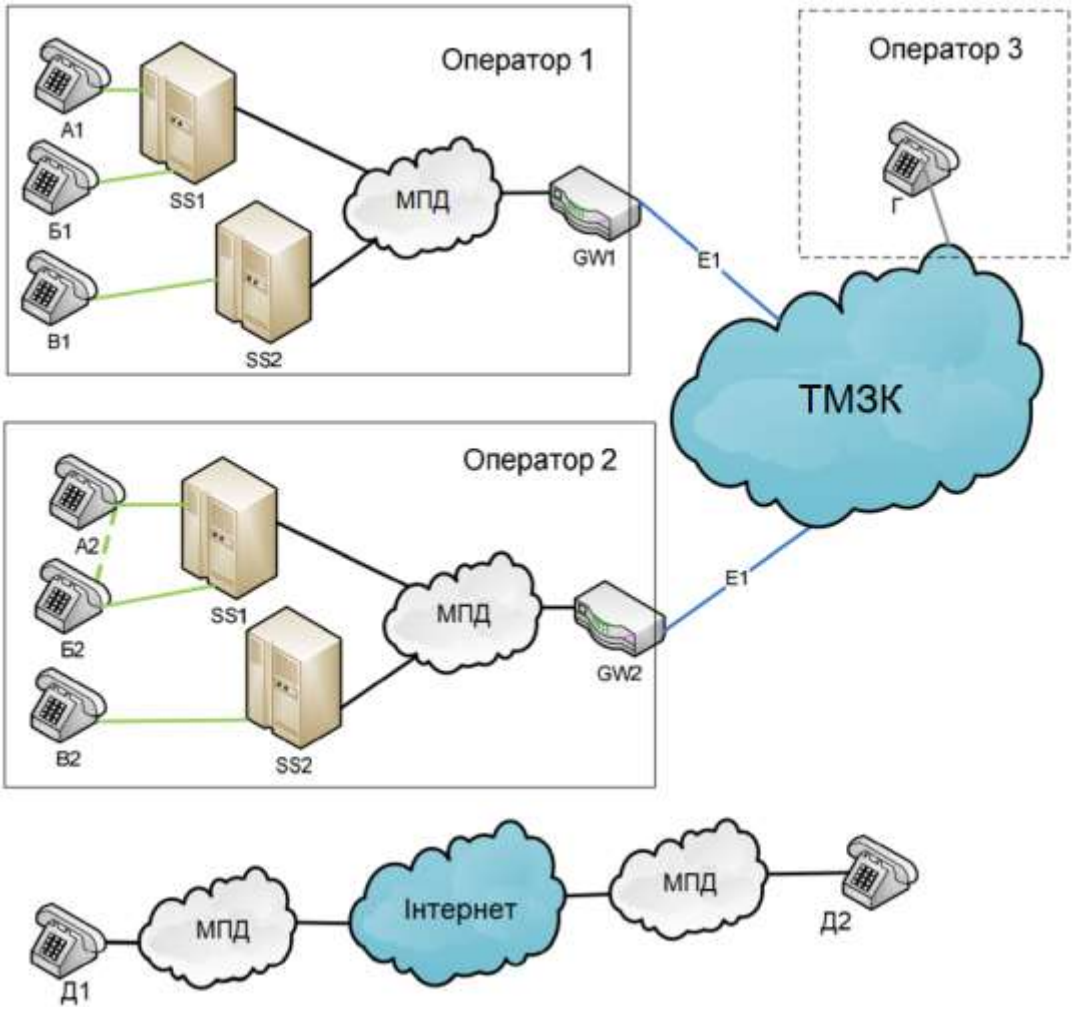


Рисунок 1.13 - Принципова схема встановлення з'єднання кореспондента VoIP

Описані вище сценарії встановлення з'єднання наведені на рис. 1.14

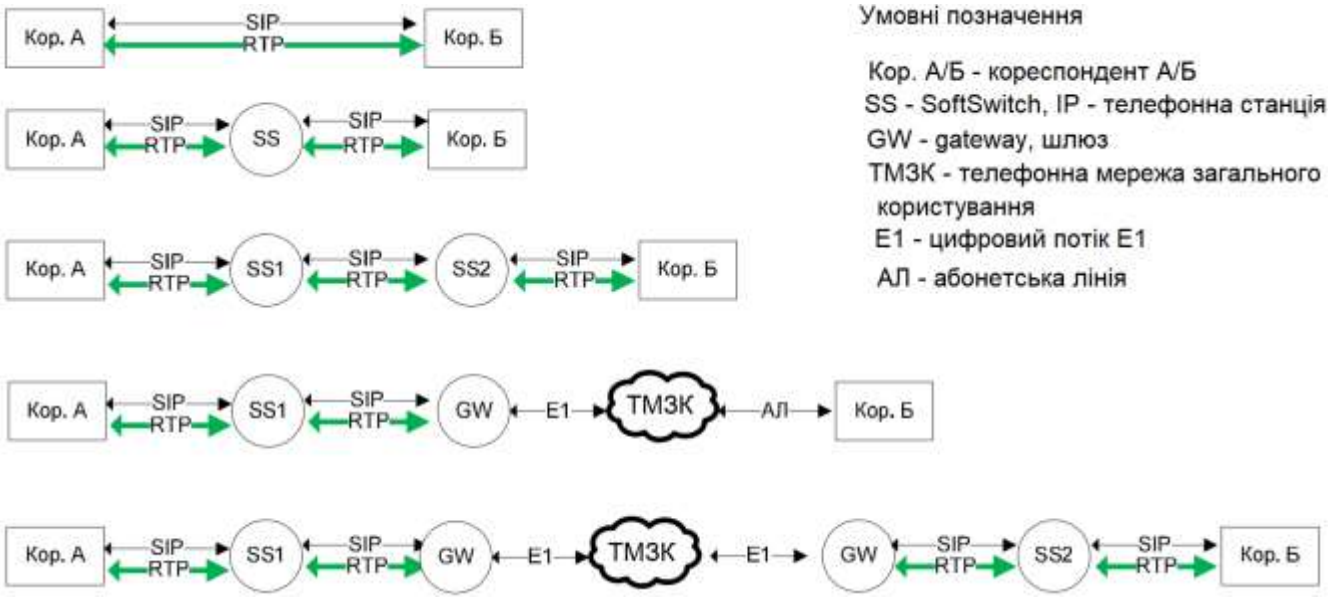


Рисунок 1.14 - Сценарії підключення оператора VoIP

В розглянутих сценаріях можуть використовуватися різні протоколи передачі та захисту потоку даних, алгоритми забезпечення безпечної IP – телефонії, також при обробці викликів необхідне виконання норм, визначених для телефонного зв'язку. Також в розглянутих сценаріях можливе використання протоколів, алгоритмів, механізмів підтримки якості при встановленні з'єднання між абонентами різних операторів. Таким чином, підсистемам забезпечення якості IP-телефонії та забезпечення безпеки IP-телефонії [12] необхідно приділити більш уваги для їх детального вивчення.

1.3 Дослідження протоколів програмного розподілу секретної інформації між кореспондентами IP – телефонії

Для розподілу секретної інформації між кореспондентами IP – телефонії на даному етапі використовуються алгоритми асиметричного шифрування. До переваг використання алгоритмів асиметричного шифрування можна віднести розподіл секретної інформації між кореспондентами IP – телефонії. Недоліком є те що вони досить повільні, мають відносно довгу величину ключа, не є придатними для шифрування великих об’ємів інформації. Область їх застосування - розподіл секретної інформації між кореспондентами IP – телефонії, формування цифрового підпису. Розглянемо деякі з них, що є актуальними на сьогоднішній день.

Запропонований У. Діффі і М. Хеллманом принципово новий підхід організації секретного зв'язку, шифрування з відкритим ключем, без попереднього обміну ключами. Для шифрування і дешифрування потоку даних використовуються різні ключі, при цьому доступ до одного ключа не надає практичної гарантії обчислити інший. Таким чином ключ шифрування в даній схемі може бути відкритим, при цьому без втрати стійкості зашифрованого повідомлення (шифру), ключ дешифрування одержувачем повинен триматися в секреті. Такі криптосистеми з відкритим ключем ще називають асиметричними (несиметричними) криптосистемами.

Стійкість асиметричних алгоритмів обумовлена розв’язанням двох трудобчислювальних математичних проблем: факторизація великих чисел; дискретне логарифмування в кінцевих полях. Ці математичні проблеми, для розв’язання яких не існує ефективних алгоритмів, або вимагає задіювання часових витрат і великих обчислювальних ресурсів, знайшли широке застосування в вирішенні завдань побудови асиметричних алгоритмів.

Розглянемо модель криптосистеми з несекретний ключем (асиметричної криптосистемами). Асиметричні криптосистеми припускають використання двох ключів: несекретного (відкритого), призначеного для шифрування потоку даних (повідомлення), і секретного (закритого), використання якого дозволяє одержувач дешифрувати прийняту зашифровану інформацію.

Несекретний ключ розподіляється між абонентами IP – телефонії по відкритих каналах зв’язку. Знання несекретного ключа не дає надії нелегітимному абоненту отримати доступ до інформації, яка знаходиться в зашифрованому повідомленні. На рис. 1.15 приведена модель криптосистеми з несекретний ключем (відкритим ключем). В залежності від заданих початкових умов (ПУ), заданих одержувачем повідомлення, генератор ключової пари, по заданому алгоритму генерує пару ключів ($К_1$, $К_2$). Секретний ключ (відкритий) $К_1$ передається джерелу по Інтернет мережам по незахищеним каналам зв'язку. Відправник шифрує інформацію (М), при цьому використовує відкритий ключ $К_1$. Зашифроване повідомлення (шифротекст) С передається по Інтернет мережам по незахищеним каналам зв'язку одержувачу.

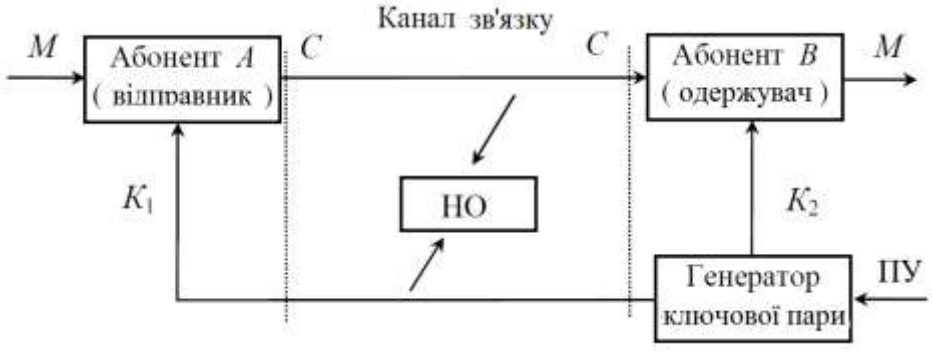


Рисунок 1.15 - Модель криптосистеми з несекретний ключем

Одержувач дешифрує зашифроване повідомлення (криптограму) відновлюючи вихідну інформацію, при цьому використовує закритий (секретний) ключ $К_2$. Нелегітимний абонент (несанкціоноване особа (НО)) має доступ до незахищених каналів Інтернет мереж, таким чином може перехопити зашифроване повідомлення (криптограму) С і несекретний (відкритий) ключ $К_1$, також, несанкціоноване особа може використати алгоритм шифрування. Єдине, до чого нелегітимний абонент немає доступу – до закритого ключа $К_2$.

Розглянемо найбільш використовуванні на сучасному етапі асиметричні криптосистеми з відкритим ключем: асиметрична криптосистема RSA; асиметрична криптосистема Діффі-Хеллмана; асиметрична криптосистема, побудована на використанні особливостей параметрів еліптичних кривих.

Криптосистема запропонована Аді Шаміром (A. Shamir) забезпечує обмін секретною інформацією по Інтернет мережам по відкритій лінії зв'язку для абонентів, які використовують не захищені канали зв'язку і не володіють секретними ключами. На рис. 1.16 представлена криптосистема запропонована Аді Шаміром.

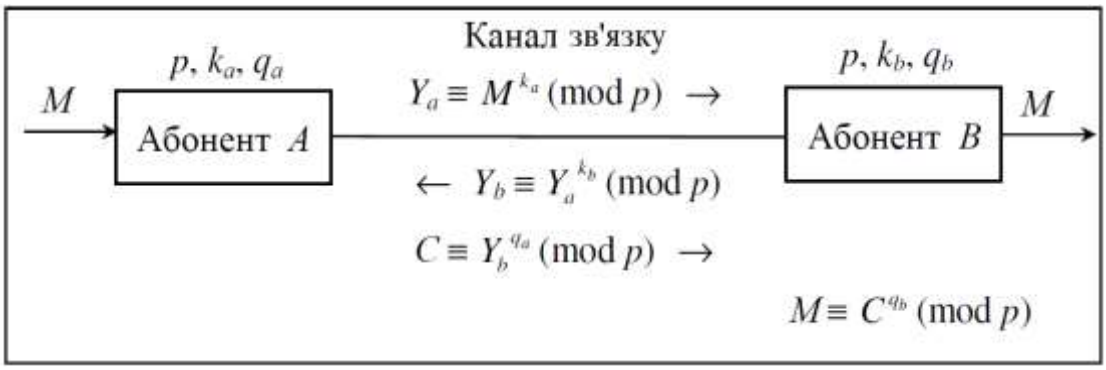


Рисунок 1.16 – Модель криптосистеми А.Шаміра

Для обміну інформацією між абонентами по незахищеним каналам зв’язку необхідно відправнику (абонент *A*) вибрати велике випадкове просте число ***p*** і передає його абоненту *B*. Абонент *A* вибирає два числа - k_a і q_a, які повинні задовільнити вимогу, і тримаються в секреті:

$$k_a\, q_a \equiv 1 \bmod (p-1).$$

Абонент *B* також вибирає два числа - $k_в$ і $q_в$, які повинні задовільнити вимогу, і також є секретними:

$$k_b\, q_b \equiv 1 \bmod (p-1).$$

На сучасному етапі криптосистема А.Шаміра використовується переважно для передачі секретних ключів.

Розглянемо алгоритм роботи криптосистеми А.Шаміра при передачі інформації по незахищеним каналам зв'язку.

Алгоритм 1.1- Криптосистеми А.Шаміра

1 Джерело *A* обчислює Y_a і по Інтернет мережі по незахищеним лініям зв'язку передає абоненту *B*

$$Y_a \equiv M^{k_a} \pmod p.$$

2 Одержувач *B*, після отримання Y_a, обчислює Y_b і по Інтернет мережі по незахищеним лініям зв'язку передає абоненту *A*

$$Y_b \equiv Y_a^{k_b} \pmod p.$$

3 Абонент *A* обчислює *C* і пересилає його по незахищеним каналам зв'язку абоненту *B*:

$$C \equiv Y_b^{q_a} \pmod p.$$

4 Абонент *B*, після отримання *C*, дешифрує його і отримує вхідне повідомлення *M*:

$$M \equiv C^{q_b} \pmod p.$$

$$M \equiv C^{q_b} \pmod p \equiv \left(Y_b^{q_a}\right)^{q_b} \bmod p \equiv \left(Y_a^{k_b}\right)^{q_a q_b} \bmod p \equiv \left(M^{k_a}\right)^{k_b q_a q_b} \bmod p \equiv$$
$$\equiv M^{k_a k_b q_a q_b} \pmod p \equiv M^{(k_a q_a k_b q_b) \bmod (p-1)} \pmod p \equiv M.$$

Криптосистема А.Шаміра в повному обсязі вирішує задачу передачі потоку даних по незахищеним каналам зв'язку. Недоліком криптосистеми А.Шаміра є те що інформація яка передається по незахищеним каналам зв'язку пересилається тричі між абонентами.

Криптосистема асиметричного шифрування RSA. Криптосистема RSA є повноцінним алгоритмом несиметричного шифрування з відкритим ключем, його

можна використовувати як для створення цифрових підписів так і для шифрування. Стійкість криптосистема RSA визначається складністю обчислення факторизації цілих великих чисел. На даний момент не існує ефективних алгоритмів обчислення факторизації цілих великих чисел, тому на даному етапі криптосистема RSA вважається стійкою. Не секретний (відкритий) і секретний (закритий) ключі є функціями від двох простих чисел розрядністю 100 ... 200 цифр і більше. Результати криптоаналізу проведеного криптоаналітиками не доводить, і не спростовує стійкість криптосистема RSA, тим самим залишаючи ступінь довіри до алгоритму RSA.

Розглянемо стійкість криптосистеми RSA. Стійкість криптосистеми RSA залежить від трудомісткості розкладання на множники великих чисел. На сьогодні відомі декілька атак на криптосистему RSA, результатом яких є доступ до секретної інформації.

Атака на криптосистему RSA при використанні абонентами мережі загального модуля. Можлива ситуація при використанні криптосистеми RSA, в якій абонентам Інтернет мережі розіслали однаковий модуль m. Таким чином можлива ситуація коли повідомлення шифрується різними ключами при використовується однаковий модуль, в даній ситуації вхідне повідомлення може бути дешифроване при відсутності відомостей ключів дешифрування. Наведемо приклад здійснення атака даного типу: M - повідомлення, e_1 і e_2 – відкриті ключі шифрування, m - модуль. Маємо: $C_1 \equiv M^{e_1} \pmod{m}$; $C_2 \equiv M^{e_2} \pmod{m}$.

Криптоаналітик має доступ до n, e_1, e_2, C_1 і C_2 .

Криптоаналітик використовуючи розширений алгоритм Евкліда визначає r і s, для яких виконується рівняння $re_1 + se_2 = 1$. Далі обчислює вхідне повідомлення

$$\left(C_2^{-1}\right)^{-s} C_1^r \equiv M \pmod{n}$$

Наступна можлива атака на криптосистему RSA використання методу без ключового читання криптосистеми RSA. При використання даної атаки криптоаналітику відомі несекретний (відкритий ключ) (e, n) і закрите

повідомлення (шифротекст) *C*. Криптоаналітик підбирає *i*, таким чином для якого виконується співвідношення:

$$C^{e^i} \pmod{n} \equiv C.$$

При виконанні даної рівності криптоаналітик проводить *i* раз дешифрування шифротексту на несекретному ключі: $(((C^e)^e)^e\ldots)^e \bmod n \equiv C^{e^i} \pmod{n}$. Далі криптоаналітик обчислює $C^{e^{i-1}}$ - це значення і є вхідним текстом *M*.

Таким чином на проведеного дослідження, розглянутих атак, для протоколу RSA необхідно ввести наступні обмеження: знання пари секретного(закритого) / несекретного (відкритого) ключів для заданого модуля дозволить криптоаналітику розкласти успішно модуль на множники; знання пари секретного(закритого) / несекретного (відкритого) ключів для даного модуля дозволить криптоаналітику обчислити успішно інші пари ключів; в протоколах Інтернет мереж при використанні незахищених каналів зв'язку, які використовують криптосистему RSA, не потрібно використовувати модуль загальний для всіх абонентів; виявляється недостатнім використання стійкого криптографічного алгоритму, також необхідно що б вся криптосистема була безпечною і також криптографічний протокол.

Асиметрична криптосистема обміну ключами Діффі-Хеллмана. Криптосистема обміну ключами Діффі-Хеллмана, як і криптосистема Ель-Гамаля, використовує для підвищення стійкості алгоритму, розв’язання труднообчислювальної математичної проблеми дискретне логарифмування в кінцевих полях. Асиметрична криптосистема обміну ключами Діффі-Хеллмана використовується в Інтернет мережах для генерації загального секретного ключа (розподілу ключів), дозволяє абонентам обмінюватися ключами по незахищених каналах зв'язку, алгоритм не можна задіяти для шифрування інформаційного повідомлення.

Криптосистема запропонована У. Діффі і М. Хелманом забезпечує обмін секретною інформацією по Інтернет мережам по відкритим лініям зв'язку для абонентів, які використовують не захищені канали (рис.1.17).

Абоненти інформаційного процесу *A* і *B* сумісно виробляють значення великого простого числа *p,* а також значення дискретного кореня цього простого числа *a* (рис. 1.17).

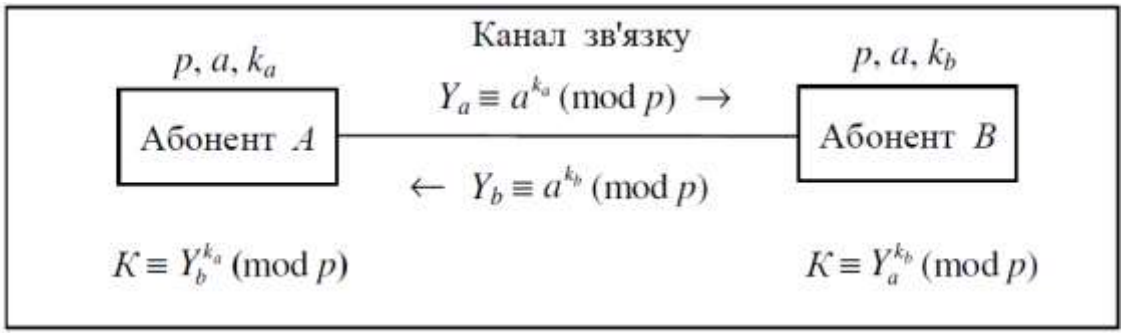


Рисунок 1.17 – Модель криптосистеми обміну ключами Діффі-Хеллмана

Кореспонденти сеансу зв’язку вибирають секретні випадкові числа, відповідно k_a, і k_b такі щоб виконувалася умова $1 < k_a < p - 1$ і $1 < k_b < p - 1$.

Кореспонденти сеансу зв’язку *A* і *B* формують кожен свій відкритий ключ за правилом відповідно $Y_a \equiv a^{ka} \pmod p$ і $Y_b \equiv a^{kb} \pmod p$.

Після обміну несекретними відкритими ключами Y_a і Y_b кореспонденти виробляють загальний секретний ключ *K*:

$$K \equiv Y_a^{kb} \pmod p \equiv a^{kakb} \pmod p; \quad K \equiv Y_b^{ka}\, Y^{ka} \pmod p \equiv a^{kbka} \pmod p.$$

Отриманий загальний секретний ключ *K* для несанкціонованої особи є недоступний (секретний), так як розв’язання рівнянь Y_a і Y_b для зловмисника є труднообчислювальною математичною проблемою дискретного логарифмування в кінцевих полях.

Необхідно зауважити, що криптосистеми обміну ключами Діффі-Хеллмана вразлива для атак типу «man-in-the-middle». У випадку, якщо зловмисник здійснить активну атаку, може перехопити несекретні відкриті ключі кореспондентів Y_a і Y_b і таким чином створити свою пару несекретного відкритого

й секретного закритого ключа (Y_c , k_c) і відправити кореспондентам свій несекретний відкритий ключ. Після цього кореспонденти обчислять загальні секретні ключі, які будуть загальними для із зловмисником, а не між кореспондентами. Якщо відсутній контроль цілісності, кореспонденти не виявити підміну.

Інтернет протоколи керування криптоключами SKIP і IKE, в основі використовують криптосистему обміну ключами Діффі-Хеллмана. Дані протоколи функціонують на мережному рівні при побудові захищених віртуальних мереж VPN.

Асиметрична криптосистема на еліптичних кривих. Криптосистема відноситься до класу асиметричних криптосистем з відкритим ключем. Безпека криптосистеми на еліптичних кривих основана на розв'язанні труднообчислювальної математичної проблеми - дискретне логарифмування в кінцевих полях. Однією суттєвою перевагою криптосистем даного класу є достатньо висока швидкість обробки секретної інформації.

Криптосистеми на еліптичних кривих, забезпечують еквівалентний захист потоку інформації, в порівнянні з іншими асиметричними криптосистемами, при цьому використовуєтьсяі менша довжина секретного ключа. В Україні прийнятий стандарт цифрового підпису, заснований на асиметричній криптосистемі на еліптичних кривих ДСТУ 4145-2002. Проведенні дослідження показали, що асиметричні криптосистеми на основі еліптичних кривих перевершують сучасні асиметричні криптосистеми з відкритим ключем по важливим параметрам: ступені захищеності в розрахунку на кожен біт секретного ключа і швидкодії при програмно-апаратній реалізації. Таким чином, задачу, яку необхідно розв'язати криптоаналітику при криптоаналізі криптосистеми на базі еліптичних рівнянь - задача дискретного логарифмування на еліптичній кривій. Дана задача сформулюється так: задана еліптична крива порядку n, де n - число точок на еліптичній кривій. Задані точки P і Q на еліптичній кривій. Необхідно підібрати єдину точку x, таку, що виконується умова $P = xQ$.

Розглянемо використання еліптичних кривих в криптографії для обміну ключами за схемою Діффі-Хеллмана.

Алгоритм 1.2 - Обмін ключами з використанням еліптичних кривих

1. Задаємо просте число p і параметри для еліптичної кривої a і b.

2. Задаємо генеруючу точку $G = (x, y)$. Параметри $E_p(a, b)$ і G– асиметричної криптосистеми, доступні всім учасникам.

3. Абонент A генерує секретний особистий ключ k_a, менший n.

4. Абонент A генерує відкритий ключ $Y_a = k_a G$. Відкритий ключ – точка заданої еліптичної кривої ($E_p(a, b)$)

5. Абонент B генерує секретний особистий ключ $k_в$, менший n.

6. Абонент B генерує відкритий ключ $Y_в = k_в G$.

7.Кореспонденти сеансу зв’язку генерують загальний секретний ключ

$$k_a Y_b = k_a (k_b G) = k_b (k_a G) = k_b Y_a.$$

Таким чином отриманий загальний секретний ключ представляє собою пару чисел. Необхідно звернути увагу, що загальний секретний ключ представляє собою пару чисел.

1.4 Протоколи забезпечення якості голосової передачі інформації в IP-телефонії

Згідно наведеної інформації Міжнародним союзом електрозв'язку якість послуг, визначається як сумарний ефект від послуг що надаються IP – телефонією показників якості послуг. Сумарний ефект визначається як ступінь задоволеності абонента IP – телефонії [14].

Для оцінки показників якості IP-телефонії використовується вербальна оцінка показників якості послуг. Як приклад можна привести оцінку MOS (Mean Opinion Schore). Оцінка якості надання послуг IP-телефонією визначається за п'ятибальною шкалою. Оцінка якості визначається як середнє арифметичне значення, від обробки отриманих результатів від великою групи експертів [14].

Якість надання послуг IP-телефонією можливо визначити на основі використання двох складових - якістю голосової передачі інформації в Інтернет мережі і якістю управління встановленням з'єднання – координації взаємодії кореспондентів IP - телефонії, узгодження параметрів сеансу зв'язку, установки і завершення встановлення з'єднання (сигналізації) [11]. Якість голосової передачі інформації в Інтернет мережі, яку забезпечує IP - телефонії можна виразити наступними параметрами: якість діалогового спілкування кореспондентів - зв'язуватися і вести діалог в повнодуплексному режимі в реальному часі; луна(ехо) рівень чутності власного голосу; немаловажний показник розбірливість – наскільки чистий і тональний рівень голосового спілкування; також необхідно враховувати рівень гучності голосового спілкування при використанні IP - телефонії.

Таким чином показник якості управління встановленням з'єднання – координації взаємодії кореспондентів IP - телефонії, узгодження параметрів сеансу зв'язку, установки і завершення встановлення з'єднання (сигналізації) включає наступні параметри: час затримки необхідний для встановлення виклику - швидкість успішного доступу до наданих сервісів IP – телефонією, час необхідний для встановлення з'єднання; час необхідний для завершення виклику – відбій, швидкість роз'єднання сеансу зв’язку.

В процесі використання в Інтернет мережі безпечної IP- телефонії можливо визначити також додаткові показники якості, а саме: час необхідний для встановлення з'єднання - час необхідний для того щоб встановити захищений голосовий канал між абонентами IP- телефонії, що використовують протоколи генерації розподілу секретних ключів; ймовірність завершеної атаки нелегітимного кореспондента на IP-телефонію в Інтернет мережі, яка використовує на даний момент захищений режим; час і ймовірність безвідказної та успішної роботи завершення IP - протоколів забезпечення безпеки IP- телефонії.

На сьогоднішній день IP-телефонія стає поширеним явищем, масово використовується як великими корпораціями так і середніми і малими. Таким

чином на IP-телефонію в Інтернет мережі додатково накладаються норми традиційної телефонії. До них можливо віднести наступні додаткові показники для IP – телефонії: показник втрати переданих пакетів по Інтернет мережі визначається як відношення прийнятих коректно пакетів до загального числа переданих пакетів по IP - мережі. Показник затримки інформації при проходженні через мережі інтернет – визначається як час, який необхідний для проходження пакета від точки відправки до точки призначення. Наступний показник пропускна здатність каналів передачі інформації визначається як доступна для кореспондентів для передачі захищеної інформації смуга пропускання. Наступний показник який розглянемо відхилення затримки визначається як різниця між затримками передачі різних пакетів по Інтернет мережам.

В Українському законодавстві слід виділити наказ “Про захист інформації в інформаційно-телекомунікаційних системах”: Закон України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: http://zakon5.rada.gov.ua/laws/show/80/94-вр (дата звернення: 02.09.2020).

В документі вказані та описані кількісні значення, які визначають показники якості, як для місцевих так і для міжнародних і також для міжміських сеансів IP - телефонії. У наведеному документі також наведені норми показників та їх визначення. До цих показників можна віднести: процент збійних викликів, виклики які не відбулися; час від моменту заняття лінії до отримання відповіді на право передачі інформації від станції IP - телефонії.

Для досягнення надання якісних послуг IP – телефонії для досягнення високих показників якості використовують декомпозицію Інтернет мереж на декілька блоків і для більш детального визначення показників використовують додаткові засоби і алгоритми в кожному конструктивному блоці.

Таким чином для прикладу можна розглянути рекомендації ITU-T Y.1291 [18]. В рекомендаціях пропонується виділення декілька конструктивних блоків, які в свою чергу розподілені в даному випадку по трьом площинах (рис. 1.18).

1. В наведених рекомендація перша площина – управління. Перша площина містить механізми для управління трактами в Інтернет мережі, через які проходить трафік по каналу з'єднання кореспондента. Сукупність механізмів забезпечують резервування ресурсів; управління допуском кореспондентів IP – телефонії а також маршрутизація для QoS.

2. Друга площина – площина даних, містить механізми, які забезпечують безпосередньо безвідказну роботу з трафіком кореспондента. Сукупність цих механізмів забезпечують управління буферами, ведення контролю за перевантаження, ведення та відслідкування маркування пакетів, диспетчеризація та відслідкування, ведення та організація черг, організація дій по класифікації трафіку, а також дотримання правил його обробки та виконання моделювання.

3. Третя площина - площина адміністративного управління. Дана площина в своєму розпорядженні містить механізми, які забезпечують відповідний рівень експлуатації, адміністрування Інтернет мереж IP – телефонії, адміністративного управління Інтернет мережею. Перераховані механізми включають в себе: рівень обслуговування (SLA) Інтернет мереж IP – телефонії, відновлення при необхідності трафіку, а також дотримання заданих правил доставки потоку даних з пакетною комутацією.

Технологія IP – телефонії для підвищення якості наданих послуг виконуються маркування та класифікація пакетів у другій площині даних, також технологією виконується планування до пакетів, а для обробки пакетів використовуються додаткові спеціальні протоколи та алгоритми обробки пакетів.

Класифікація пакетів для підвищення якості надання послуг виконується в залежності від значення декількох параметрів: CoS, MPLS-EXP; номера порту по якому йде підключення абонента до мережевого обладнання Інтернет мереж, або при цьому використання MAC адреси кореспондента, типу пакета і т.д. Головною задачею яку необхідно вирішити класифікацією пакетів це розподіл пакетів на групи для проведення їх подальшого маркування а також для визначення параметрів пакету наприклад: MPLS-EXP - три біта в MPLS для маркування QoS.

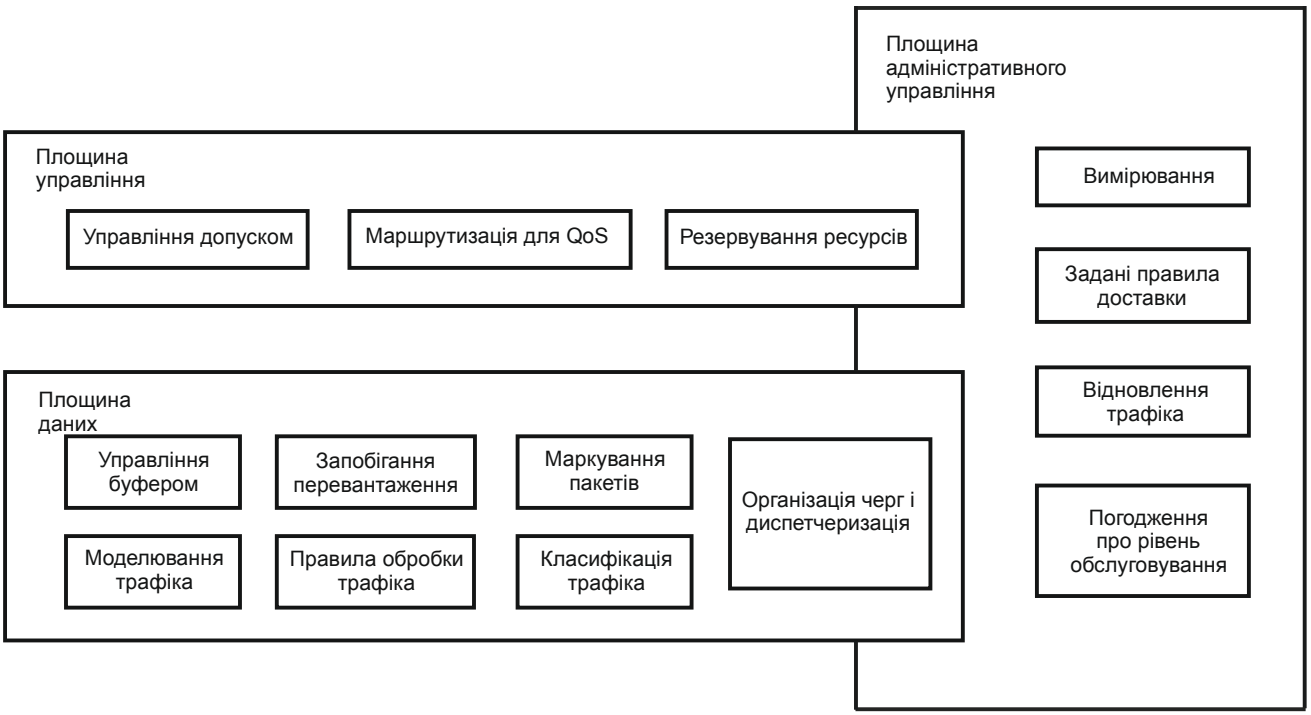


Рисунок 1.18 - Архітектурна модель підтримки QoS

Інструмент планування другої площини в задачі якого виконання наступних дій: ведення контролю за перевантаження, диспетчеризація та відслідкування, ведення та організація черг, одна із задач яку вирішує даний інструмент - визначає який пакет з інтерфейсу буде першим виходити з мережевого вузла. Дана задача вирішується алгоритмами управління чергою, а також механізмів ведення контролю за перевантаження черг. Серед алгоритмів управління чергою можна виділити: SP, WRR, MDRR, LLQ, WRED.

Для забезпечення якості наданих послуг IP – телефонією можуть також застосовуватися додаткові механізми обмеження швидкості - policing чи shaping. Механізм Policing – використовується для обмеження швидкості при передачі потоку даних без буфера. Механізм Shaping - використовується для обмеження швидкості передачі потоку даних з використанням проміжного буфера. Також додатково можливо застосування в Інтернет мережах управління потоком даних Ethernet - механізм, забезпечує вбудованими засобами можливість попередження абонента про необхідність призупинити передачу даних на заданому інтервалі часу, що приймаючий порт на даний момент не в стані виконати обробку.

Для забезпечення якості наданих послуг технологія IP – телефонія надає для низькошвидкісних каналів додаткові механізми, такі як: виконання фрагментація і забезпечення чергування пакетів; механізми компресії дозволяє стискати голосових пакетів заголовок IP/UDP/RTP з 40 до 2-5 байт. Використання даного механізму можливо в межах одного фізичного каналу зв'язку.

Для підтримки якості наданих послуг технологіє IP – телефонії до механізмів площини управління моделі додатково можливе застосування RSVP (резервування ресурсів) в Інтернет мережі, а також використання протоколів маршрутизації з урахуванням якості наданих послуг. Як вхідні даних IP - протоколи використовують поля в маркованих пакетах також таблицю маршрутизації, що враховує різні параметри якості наданих послуг для інтерфейсів обладнання і для різних маршрутів. Частина функціоналу підтримується IP – протоколом Інтернет мережі маршрутизації OSPF.

Також до площині (третя площина) адміністративного управління можна також віднести механізми налаштування параметрів для IP – телефонії трафіку, які використовуються на відповідних для користувача терміналах, IP- станціях, а також на інших елементах Інтернет мережі IP – телефонії, наприклад RTP-проксі-сервери і контролери сесій (Session Border Controller) .

Забезпечення надання достатнього рівня якості наданих послуг IP – телефонії приділяється увага в університетах Центральної Флориди, Карленгтонском університеті Канади. Питання забезпечення достатнього рівня якості наданих послуг IP – телефонії виносяться на розгляд такими організаціями як MCE, IEEE, ETSI, IETF, 3GPP. Для забезпечення якості IP-телефонії прийняті ряд стандартів і моделей, але до теперішнього часу для визначення рівня якості QoS IP-телефонії не існує єдиного стандарту.

1.5 Постановка задачі

На основі проведеного огляду, можливо зробити висновок проте, що поширення Internet-телефонії послужили: застосуванням недорогих Internet мереж, в порівнянні з телефонними аналоговими мережами, з комутацією IPv4(6)-пакетів, а також мобільність і універсальність, що дозволяє перетворити голосовий потік в зашифровані і стисненні дані в будь-якій точці інфраструктури Internet мережі.

На сучасному етапі розвитку Internet-телефонії, телекомунікацій можливо спостерігати зростаючі обсяги трафіку Internet мереж зокрема в корпоративних мережах, а також в мережах Інтернет провайдерів, тут необхідно зазначити методи і технології, набір IPv4(6) - протоколів, методів і технологій, що забезпечують потік даних з комутацією пакетів у вигляді голосового спілкування в середовищі Інтернет мережі.

Стандартизація протоколів, а також масове використання персональних комп'ютерів операторами IP-телефонії в якості терміналів для послуг Інтернет телефонії, стандартизація Інтернет протоколів призвели до розробки спеціалізованого програмного забезпечення для Інтернет -телефонії, а також доступного програмного забезпечення (відкритим кодом), що дало поштовх розширювати можливості IP-телефонії і використовувати криптографічні алгоритми та алгоритми розподілу ключів для забезпечення надійності в Інтернет -телефонії.

Проведений аналіз наукових досліджень технологій IP-телефонії в областях криптографічного захисту передачі інформації, забезпечення якості потоку даних з пакетною комутацією (передача голосових і медіа- файлів), надання якісних послуг IP-телефонії, архівація відео і голосової інформації, показав що на сьогодні питання безпечної Інтернет -телефонії є відкритим для сценарію точка-точка, у випадку не вироблення зазделегіть загального секретного ключа для операторів. Також залишаються відкритими питання як впливають IPv4(6)- протоколи на виконання норм встановлених під час експлуатації безпечної IP-телефонії, в

роботах мало уваги приділено імовірнісно-часовим характеристикам (ІЧХ) Інтернет протоколів забезпечення безпечної технології IP-телефонії. До загального недоліку розглянутих робіт слід віднести що в них, не описується така поширена атака на протоколи програмного розподілу ключів, як "зустріч посередині", тому виникає необхідність в розробці моделі нелегітимного абонента, яка буде враховувати атаку "зустріч посередині".

Відповідно до поставленої мети в дипломній роботі необхідно вирішити наступні задачі:

- дослідження існуючих криптографічних протоколів захисту інформації, а також протоколів програмного розподілення секретної інформації між кореспондентами зв’язку, для підвищення надійності IP-телефонії і впливу IP протоколів на параметри якості;

- розробка моделі нелегітимного абонента для оцінки рівня надійності безпечної IP-телефонії;

- розробка методу оцінки параметрів IP-протоколів програмного розподілу ключів між кореспондентами IP-телефонії;

- розробка методу, на основі алгоритму Діффі-Хелмана, виявлення нелегітимного абонента, IP - протоколів розподілу ключів між кореспондентами IP-телефонії.

2 МОДЕЛЬ НЕЛЕГІТИМНОГО АБОНЕНТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

2.1 Безпека передачі голосової інформації в IP-телефонії

На сьогоднішній день IP-телефонія стає поширеним явищем Інтернет мереж, масово використається як великими корпораціями так і середніми і малими. Таким чином використовувані канали передачі голосової інформації в Інтернет мережах IP-телефонії стають загальнодоступними і забезпечення конфіденційності сервісів IP - телефонії набуває особливої актуальності. Для вирішення поставленої задачі можуть використовуватися різні варіанти розв'язання задачі: наприклад використання захищеного каналу між абонентами (VPN-тунель); використання спеціальних IP - протоколів Інтернет мережі, які забезпечать безпеку сервісів IP-телефонії.

Використання захищеного каналу між абонентами (VPN-тунель) набув широкого застосування при побудові віртуальних корпоративних Інтернет мереж, при цьому для його застосування абоненти повинні підтримувати VPN-протокол. Більшість пристроїв IP – телефонії не підтримують VPN (табл. 2.1). В табл. 2.1 наведено програмно – апаратне забезпечення захищеної IP-телефонії. Таким чином, для забезпечення безпеки сервісів IP - телефонії використовуються досить часто спеціальні IP - протоколи для забезпечення в Інтернет мережі безпеки IP-телефонії.

В Інтернет мережах до спеціальних протоколів які призвані забезпечити безпеку сервісів IP-телефонії можна віднести наступні протоколи Secured SIP, SDES, ZRTP, MIKEY,SRTP, S-MIME, DTLS. Спеціальні IP -протоколи можна розділити на 3 категорії [8]: спеціальні IP - протоколи захисту сигналізації (Secured SIP); спеціальні IP - протоколи генерації і розподілу між кореспондентами секретних ключів для використання в протоколах захисту медіаінформації (MIKEY, SDES, DTLS); спеціальні IP - протоколи захисту медіаінформації (SRTP)

Таблиця 2.1 – Програмно – апаратне забезпечення захищеної IP-телефонії

Виробник	Продукт	Реалізація	Протокол захисту			Підтримка VPN
			Встанов-лення з'єднання	Медіа трафік	Розподілен-ня ключів	
LinkSys	SPA8000	апаратна	SIPS/TLS	SRTP	немає даних	ні
LinkSys	Cisco SPA112	апаратна	SIPS/TLS	SRTP	немає даних	ні
Dlink	DVG-5008S	апаратна	немає даних	немає даних	немає даних	PPTP
AddPack	AP200	апаратна	SIPS/TLS	SRTP	немає даних	немає даних
Grand-stream	Grandstream	апаратна	SIPS/TLS	SRTP	SDES	ні
UM-Labs	UM-Labs	апаратна	SIPS/TLS	SRTP	ZRTP, SDES	немає даних
Counter-Path	Eye-beam	програмна	SIP/TLS	SRTP	TLS	ні
3XC	3CX softphone	програмна	SIP/TLS	SRTP	немає даних	ні
Asterisk	IP PBX	програмна	SIP/TLS	SRTP	ZRTP	ні
FreeSwitch	IP PBX	програмна	SIP/TLS	SRTP	SDES	ні
Phoner	Phoner softphone	програмна	SIP/TLS	SRTP	ZRTP	ні

Задача яка ставиться перед спеціальними IP - протоколами захисту сигналізації - забезпечення безпеки конфіденційної інформації, наприклад телефонні номери кореспондентів (учасників сеансу телефонного зв’язку IP – телефонії). Для вирішення поставленої задачі використовуються протоколи Secured SIP (SIP/TLS, SSIP) [8].

Протокол Secured SIP працює за аналогією і відповідності з протоколом HTTPS, при цьому організовується між абонентом IP - телефонії і сервером SSL тунель з використанням відкритого (несекретного) ключа і сертифікатів. SIP-повідомлення (сигналізація) передаються використовуючи при цьому організований тунель. До недоліків даного підходу слід віднести необхідність

використання інфраструктури відкритих (несекретних) і закритих (секретних) ключів, які використовується для забезпечення організації TLS.

IP - протокол Secure Real-time Transport Protocol – захищений протокол реального часу – широко використовується Інтернет мережами IP- телефонією для забезпечення конфіденційності при передачі по мережам голосової інформації, даний протокол реалізує функції криптографічного захисту інформації – шифрування/дешифрування, аутентифікацію голосової інформації повідомлень, як основу використовує алгоритм симетричного шифрування AES (розглянутий в розділі 1.1). Криптографічний захист (шифрування ключом сесії) пакетів голосової інформації, які передаються по Інтернет мережам реалізується IP - протоколом SRTP в режимі реального часу і не впливає ніяким чином на ІЧХ характеристики IP - протоколу RTP. Для криптографічного захисту пакетів голосової інформації, в режимі реального часу необхідна завчасно генерація криптографічних ключів. Цю задачу вирішують IP - протокол розподілу ключів.

Задачі закріпленні за IP -протоколом SRTP вираженні в виконанні наступних функцій: шифрування/дешифрування голосової інформації (повідомлень); аутентифікація голосових даних (повідомлень); стиснення інформації - RTP заголовків; захист від перезавантаження, відслідкування неможливості передачі повторних пакетів; захист та збереження смуги пропускання.

Шифрування/дешифрування переданого потоку даних, аутентифікація переданих повідомлень Інтернет мереж – виконання цих задач бере на себе IP - протокол SRTCP. До недоліків протоколу SRTCP можна віднести неможливість відключення опції аутентифікації. Опція аутентифікація голосової інформації є обов'язковою в протоколі SRTP і не може бути ніяким чином відключена

Для вирішення задачі генерації і розподілу між абонентами секретних ключів шифрування/дешифрування медіаінформації, призначені протоколи третьої групи. До протоколів третьої групи, для вирішення поставлених задач відносяться наступні IP -протоколи SDES, MIKEY, ZRTP, DTLS. IP- протокол MIKEY може використовуватися в декількох режимах, які визначають режим формування

загального секретного ключа сесії SRTP: режим генерації встановленого секретного ключа, режим генерації несекретного (відкритого) та закритого (секретного) ключа та режим генерації загального секретного ключа Діффі-Хелмана. Необхідно врахувати що режими генерації другий і третій не захищають від атаки “зустріч посередині” і вимагають необхідність реалізації механізму аутентифікації голосової інформації (повідомлень). Як транспорт для передачі голосової інформації (повідомлень) по IP мережам можна використовувати IP - протокол такі як SIP / SDP, так і IP - протокол RTSP.

Для формування в Інтернет мережах медіа-сесій точка-точка IP – телефонії з двома з двома кореспондентами, для вирішення даної задачі використовується IP - протокол DTLS для SRTP. IP - протокол DTLS як транспорт для передачі потоку даних між абонентами використовує IP протокол UDP з жорстким фіксуванням портів. Голосова інформації IP – телефонії (повідомлення) протоколу DTLS передаються сумісно з RTP пакетами даних. Тому кожна сесія учасників зв’язку містить інформацію для DTLS і також два пакети SRTP контексту (для IP - протоколів SRTP і SRTCP). Таким чином для абонентів зв’язку організуються сесії (IP – протоколам DTLS-асоціації), при цьому кореспонденти IP – телефонії обмінюються голосовою інформацією (повідомленнями DTLS handshake) (рис.2.1). Протокол DTLS, як основу використовує IP - протокол TLS, який в свою чергу використовує PKI (Public Key Infrastructure,) - інфраструктуру несекретних відкритих ключів, тому використання IP - протоколу TLS можливо у випадку наявності інфраструктури несекретних відкритих ключів (PKI).

Для генерації та розподілу ключів в Інтернет мережі IP – телефонії між учасниками сесії використовується найбільш перспективний IP - протокол ZRTP. IP - протокол успішно використовується в таких додатках як Android CsipSimple, також АТС FreeSwitch, Asterisk і телефонах Jitsi, Phoner, програмно-апаратних шлюзах IP – телефонії виробника компанії UM-Labs. IP -протокол ZRTP забезпечує гарантування безпечної передачі голосової інформації IP – телефонії в сесії зв’язку точка – точка. IP -протокол ZRTP вирішує наступні задачі: генерація

загальних секретних ключів SRTP сесії типу точка – точка; гарантує аутентифікації абонентів сесії зв'язку; гарантує забезпечення конфіденційності голосової інформації (повідомлень) IP -протоколу; також відслідковує атаки типу «зустріч посередині», таким чином гарантує захист від даних атак.

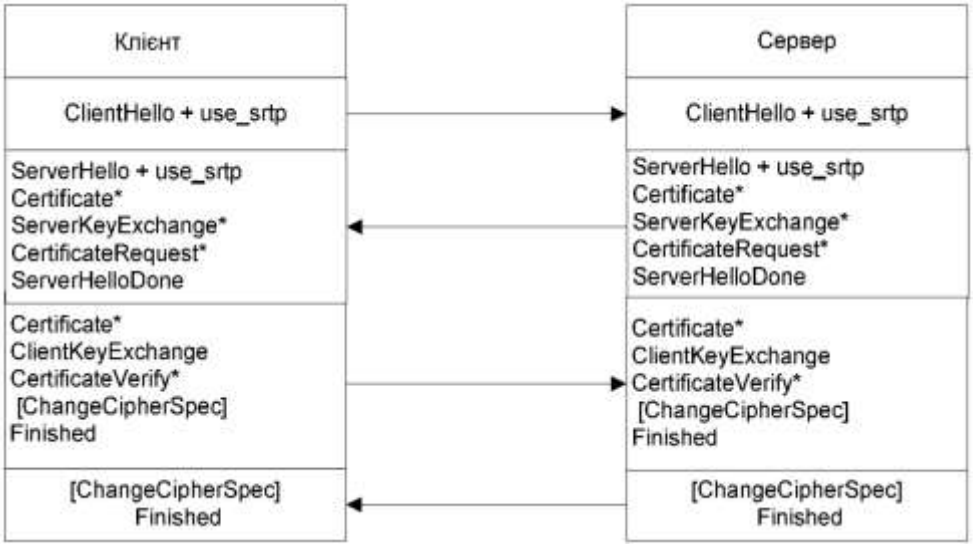


Рисунок 2.1 – IP – протокол DTLS - обмін повідомленнями

IP – протокол ZRTP IP – телефонії по топології в сесії зв'язку точка – точка, також є можливість використання протоколу в IP – мережах при багатопотоковому режимі, у випадку необхідності організації декілька захищених потоків даних. IP – протокол ZRTP IP – телефонії використовує для генерації загального секретного ключа сесії асиметричний алгоритм обміну ключами Діффі-Хелмана.

Сформулюємо вимоги до IP – протоколів Інтернет мереж для гарантованого і безпечного розподілу ключів IP - телефонії: підтримувати та гарантувати роботу абонентів сесії в топології клієнт-сервер, а також підтримувати топологію клієнт-клієнт. При цьому IP – протоколи повинні гарантувати безпеку при використання даних топології для організації сеансу між абонентами, а також забезпечити учасників загальним розподіленим секретним(закритим) ключем сесії, для захисту голосової інформації IP - протоколу SRTP; виконувати функцію генерації та розподілу загального секретного (закритого) ключа сесії без залучення додаткового програмного забезпечення між абонентами сесії. Реалізувати

функціонал шляхом інтеграції без застосування додаткового програмного забезпечення в існуючі на даний час системи зв'язку, а також в програмні термінали; підтримувати механізм генерації та розподілу загального секретного ключа (закритого) в сеансу зв’язку типу клієнт-клієнт без передачі закритого ключа в відкритому виді використовуючи канали зв'язку IP – телефонії; мати в своєму розпорядженні механізм виявлення та відслідковує атаки типу «зустріч посередині», таким чином гарантувати захист від атак даного типу; повинен використовувати як транспорт в IP – мережах протоколи доставки потоку даних TCP/UDP порти, для гарантованої роботи IP-телефонії.

Проведений аналіз та дослідження в області IP -телефонії по забезпеченню захисту та надійності передачі голосової інформації по Інтернет мережам показав необхідність вирішення наступних задач: розробка систем IP-телефонії з врахуванням при цьому підвищення захисту та надійності передачі голосової інформації по Інтернет мережам; проведення аналізу рівня безпеки, який забезпечується в Інтернет мережах системами IP-телефонії; проведення аналізу рівня безпеки, який забезпечується в Інтернет мережах окремими IP -протоколами IP-телефонії.

2.2 Інформаційна безпека захищеної IP-телефонії

На основі проведеного аналізу та дослідження, а також виходячи з особливостей IP-протоколів Інтернет мереж забезпечення безпеки IP-телефонії нелегітимний абонент може, на основі отриманої інформації, проводити різного типу атаки на працюючу систему IP-телефонії, яка на даний момент працює в захищеному режимі. Проведені дослідження показують існування декілька моделей нелегітимного абонента в IP-телефонії в Інтернет мережах. Імовірнісна модель нелегітимного абонента, яка детально описана в [3]. Імовірнісна модель нелегітимного абонента показує які дії та з використанням якого інструменту проводить нелегітимний абонент атаки при експлуатації захищеної IP-телефонії в

Інтернет мережах на ОС Windows. Імовірнісна модель нелегітимного абонента при цьому проводить аналіз та враховує різновиди атак, а також враховує особливості та характер атак на операційну систему Windows, з врахуванням використання операційною системою засобів захисту (криптографічних засобів). Імовірнісна модель нелегітимного абонента не враховує програмний розподіл загальної секретної інформації (закритих ключів), з використанням IP – протоколів рознесення ключів IP-телефонії в Інтернет мережах. Розглянута імовірнісна модель використовує попередній розподіл секретної інформації, тобто завчасна установка секрету учасникам сеансу. При застосуванні імовірнісної моделі нелегітимного абонента для здійснення атаки, задача якої отримання несанкціонований доступу до голосової інформації IP – технології в Інтернет мережах, вирішується тільки задача дешифрування переданого потоку даних при цьому використовується «атака в лоб» (метод перебору), вірогідність успішного завершення даної атаки достатньо низька при правильному вибору ключів сесії. Таким чином модифікація пакетів інформації можлива в разі успішної атаки, результатом якої є підбір пароля для реалізації процесу дешифрування перехоплених потоків даних.

Розглянемо модель нелегітимного абонента запропонованого та описаного в стандарті по питанням технічного та експортного контролю [29]. В запропонованому стандарті приведений опис загальної моделі нелегітимного абонента. Описана в стандарті модель не враховує також особливостей роботи в Інтернет мережах захищеної IP-телефонії. Технологія IP-телефонії має в своєму розпорядженні в застосуванні IP – протоколи, які призначенні для підвищення ефективності та забезпечення безпеки IP-телефонії, сюди можна віднести захист сигналізації, розподіл загальної секретної інформації між учасниками сеансу зв’язку, захист голосової інформації, при цьому не наведено інформації про здійснення атак на IP – протоколи IP-телефонії. В проведеному аналізу робіт [7] рекомендуються загальні вимог, які ждуть бути запропонування до мережі IP-телефонії в Інтернет мережах, також наводиться опис загальних характеристик та

виконуваних дій при здійсненні атак на мережу IP-телефонії. Рівень описаних атак відповідає діям середньостатистичного хакера при проведенні атак на сервіси IP – телефонії. На основі проведеного дослідження та аналізу відповідних робіт можна зробити наступний висновок: в розглянутих роботах не наводиться декомпозиція IP - протоколів Інтернет мереж безпечної IP - телефонії на відповідні складові, також не наведено опис успішних атак на IP - протоколи Інтернет мереж які безпосередньо використовуються в безпечній IP - телефонії. В розглянутих роботах [6] використовуються та описуються загальні підходи та принципи забезпечення підвищення надійності та захисту сервісів IP-телефонії, а також загальні підходи та принципи можливих дії нелегітимного абонента при атаках на сервіси IP-телефонії. В роботах не приділяється належної уваги атакам на протоколи розподілу загальної секретної інформації між учасниками сеансу зв'язку, захисту голосової інформації, при цьому не приводиться інформації про здійснення атак на IP – протоколи використовувані в IP-телефонії.

Таким чином виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях нелегітимного абонента, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP – протоколів Інтернет мереж, які використовуються безпечною IP-телефонії, запропонована модель повинна враховувати вказанні особливості.

Моделі які описані в розглянутих роботах не дозволяють визначити імовірність успішної атаки на отримання несанкціонованою доступу до потоку даних (голосової інформації) в мережі захищеної IP-телефонії, яка працює в режимі за схемою точка – точка, також не надають механізмів виявлення та захисту від атак типу «зустріч по середині», розглянуті моделі не враховують даний тип атак. В запропоновану модель нелегітимного абонента необхідно включити додаткові механізми, такі як: виявлення імовірність успішної атаки на отримання несанкціонованого доступу до потоку даних захищеної IP-телефонії,

яка працює в режимі за схемою точка – точка; також механізми виявлення та захисту від атак типу «зустріч по середині».

Виникнення загроз в Інтернет мережах безпеки голосової інформації в IP-телефонії може проявитися в результаті виникнення додаткового каналу потоку інформації в Інтернет мережах між нелегітимним абонентом (джерелом загрози) і кореспондентом носієм інформації, при цьому необхідно створення відповідних умов, які сприяють для виникнення порушення захищеності та безпеки голосової інформації. Наскільки актуальна загроза порушення захищеності та безпеки голосової інформації буде оцінюватися, також, типом джерела загрози - рівнем атаки, рівнем захищеності джерела голосової інформації та наявністю вразливостей, а також рівнем захищеності середовища поширення голосового інформаційного сигналу.

В залежності від типу інформації на яку виконується атака можна виділити наступні джерела загроз: загрози, які пов'язані з діяльністю конкретної організації, організації які володіють оснащеністю і мотивацією, високим потенціалом; загрози що направлені і зумовлені економічними, політичними, військовими та іншими цілями іноземних держав; також загрози, пов'язані з діяльністю організацій, що володіють мотивацією, обумовленої їх економічними, інформаційними та іншими цілями; загрози, пов'язані з діяльністю окремих фізичних осіб (злочинних елементів).

Рівень впливу на закриту інформацію, яку необхідно захистити, визначається можливостями джерела загроз, наскільки джерело загроз володіє інформацією про сервіси захисту IP – телефонії, також рівень впливу на закриту інформацію визначається рівнем механізмів якими володіє джерело загроз. Джерело загроз, яке здійснює дії (атаку) або займається підготовкою до дій(атаки) результатом яких є отримання несанкціонованого доступу до інформації з подальшим впливом на закриту інформацію є зловмисником інформаційної безпеки. В якості нелегітимного абонента будемо визначати фізичну особу, яка випадково чи не випадково здійснює дії (атаки) в своїх інтересах чи в інтересах даної організацій,

чи в інтересах інших організацій (можливо іноземних організацій) результатом яких є порушення захищеності та безпеки інформаційних ресурсів при її обробці програмно – апаратними, технічними та іншими сервісами в інформаційних системах.

При розробці уточненої модель нелегітимного креспондента більш доцільно розглядати зловмисників з точки зору рівня їх можливостей а також наявності прав несанкціонованого доступу до інформації, одноразового чи постійного. Таким чином модель нелегітимного креспондента буде враховувати рівень можливостей зловмисників, до першого рівня віднесемо нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP - телефонії. До другого рівня віднесемо нелегітимних абонентів які не мають відповідного рівня доступу до сервісів безпечної IP - телефонії.

Таким чином нелегітимними операторами (перший рівень) можуть в даному випадку можуть виступати: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів.

До нелегітимних абонентів (другий рівень) можуть в даному випадку бути віднесені: сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури.

Одним із напрямків забезпечення безпеки передачі голосової інформації в Інтернет мережах захищеної IP - телефонії це використання криптографічних IP – протоколів SRTP. Протокол SRTP реалізує функції криптографічного захисту потоку даних. Також для забезпечення безпеки передачі голосової інформації в Інтернет мережах захищеної IP - телефонії виникає необхідність використання IP – протоколів програмного розподілу загальної секретної інформації (ключів) для сесій SRTP.

Враховуючи те, що передача голосової інформації в Інтернет мережах безпечної IP- телефонії здійснюється з використанням загального доступу, а

монітори VoIP практично доступні будь-якій сторонній особі, як і легальний доступ до Інтернет мереж – таким чином на основі сказаного можливо зробити висновок про актуальність виникнення загроз віддаленого доступу і можливості їх реалізації нелегітимними абонентами, як першого так і другого рівнів.

2.3 Узагальнена модель нелегітимного кореспондента безпечної IP - телефонії

Реалізація моделі нелегітимного кореспондента безпечної IP - телефонії повинна бути конкретної, враховувати поведінку, властивості також характеристики конкретного об'єкту захисту VoIP. Виходячи з проведеного аналізу модель нелегітимного кореспондента безпечної IP - телефонії повинна враховувати структуру системи, сервіси безпеки також варіанти і способи використання ресурсів.

Існуючі моделі не враховують атаки на IP - протоколи розподілу загальної секретної інформації між учасниками сеансу зв’язку, захисту голосової інформації, відсутня інформації про здійснення атак на IP – протоколи використовувані в IP-телефонії, що складаються в застосуванні декількох протоколів для забезпечення безпеки, а також не описують атаки безпосередньо на ці протоколи.

Отже виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP – протоколів Інтернет мереж, які використовуються безпечною IP-телефонії, модель повинна враховувати вказанні особливості, мати механізми виявлення та захисту від атак типу «зустріч по середині». Для врахування в моделі вказаних недоліків розглянемо схему взаємодії кореспондентів захищеної IP-телефонії клієнт - клієнт, при відсутності попереднього програмного розподілення загального секретного матеріалу

(закритого ключа сесії), і також розглянемо можливі варіанти дій нелегітимного абонента в схемі клієнт - клієнт (рис. 2.2).

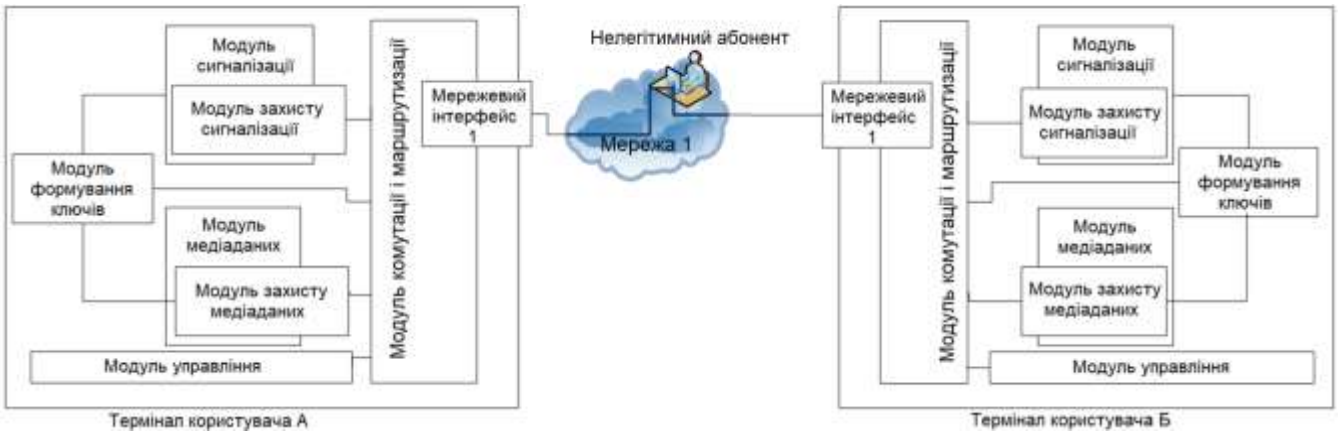


Рисунок 2.2 - Схема встановлення з'єднання в сценарії клієнт-клієнт

Нелегітимний абонента може використовувати наступні сценарії виконання атак: здійснення пасивної атаки, при цьому використовує перехоплення переданих даних, без їх подальшої зміни; здійснення активної атаки, при цьому знаючи рівень системи захисту її вразливості, недоліки а також використовуючи штатні засоби системи захисту для проведення атаки з метою несанкціонованого доступу до даних з подальшою їх модифікацією, або отримання додаткових засобів для впливу на систему з метою подальшого виконання атаки.

Розглянемо модель нелегітимний абонента, який Інтернет мережах IP - телефонії буде використовувати сценарій активної атаки, направлену використанні вразливості IP - протоколу Діффі-Хелмана. IP - протокол Діффі-Хелмана схильний до атаки «зустріч посередині» що є суттєвим недоліком цих протоколів. Так як, IP - протокол Діффі-Хелмана лежить в основі більшості протоколів програмного розподілу секретного матеріалу (закритих ключів) то виникає необхідність більш детального приділення їм уваги. IP - протокол Діффі-Хелмана протокол захищає від атаки пасивного нелегітимного абонента, однак, він нестійкий до атаки активного нелегітимний абонента.

При здійсненні активної атаки нелегітимним абонентом необхідно враховувати можливий рівень прав порушника, так порушник може знаходитися в одній підмережі з об’єктом на який направлена атака, в даному випадку може

мати достатньо прав для виконання успішної атаки, в іншому випадку порушник може знаходитися не в одній підмережі з об’єктом на який направлена атака, в даному випадку може не мати достатньо прав для виконання успішної атаки.

Під VoIP монітор абонента як правило мається на увазі, IP-телефон, шлюз безпечної IP-телефонії, стаціонарний комп'ютер, ноутбук, планшет, смартфон із встановленим для успішної взаємодії спеціалізованим програмним забезпеченням безпечної IP-телефонії. VoIP монітор надає можливість абонентам отримувати надавані послуги IP- телефонії, а також виконувати аудіо, відео виклики.

При проведені активних на VoIP монітор абонента будемо рахувати, що в одній підмережі з об’єктом захисту на який направлена атака може перебувати тільки нелегітимний оператор першого рівня.

Для отримання несанкціонованого доступу до сервісів IP телефонії нелегітимний абонент може використовувати для проведення успішної атаки наступні засоби і механізми: несанкціонований доступ на сервіси IP - телефонії, НСД може бути отриманий за рахунок атаки в лоб - перебору пароля; модифікація таблиці маршрутизації, часткове перенаправлення трафіку; виконання атаки «зустріч посередині» спеціалізований вплив на програмний розподіл загальної секретної інформації, а також на потоки даних, які передаються між абонентами IP - телефонії, мета даного типу атаки порушення конфіденційності і цілісності потоку даних; активна атака на шифр на переданий між абонентами, мета атаки - дешифрування даних і порушення конфіденційності; атака спрямована на програмне забезпечення одного або декількох абонентів, мета атаки – впровадження закладок в програмне забезпечення; активна атака з метою установка на вузлів оператора додаткового обладнання; активна атака на конфігураційні файли VoIP монітор, метою даної атаки є зміни налаштувань політики безпеки прийнятої в організації; активна атака направлена на перехоплення авторизаційних секретних даних, метою даної атаки є подальше управління обладнанням користувача, а також доступ до даних, які передаються між абонентами.

Для побудови математичної моделі нелегітимний абонента проведений аналіз можливих активних успішних атак (загроз) та проведено дослідження виявлення їх можливих джерел. Знаючи вразливості та рівень захищеності об’єкта, для якого необхідно провести захист, активний зловмисник може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об’єкта.

2.4 Модель нелегітимного абонента першого рівня безпечної IP - телефонії

Модель нелегітимного креспондента буде враховувати рівень можливостей зловмисників, до першого рівня віднесемо нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP - телефонії. До другого рівня віднесемо нелегітимних абонентів які не мають відповідного рівня доступу до сервісів безпечної IP - телефонії.

Таким чином нелегітимними операторами (перший рівень) в даному випадку можуть виступати: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів.

Визначмо цілі нелегітимних абонентів першого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії: $Ц_{ЗАХОБЛ\_1}$-захоплення обладнання оператора нелегітимним абонентом першого рівня; $Ц_{ЗАХМОН\_1}$ - захоплення монітору абонента нелегітимним кореспондента першого рівня. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP - телефонії. На основі проведеного аналізу алгоритмів поведінки нелегітимних абонентів розпочнемо розробку моделі нелегітимного абонента першого рівня по кожній з перерахованих цілей.

Захоплення обладнання оператора нелегітимним абонентом першого рівня. Розглянемо модель нелегітимного абонента першого рівня, задачею якого є проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії, результатом успішної активної атаки – захоплення обладнання оператора.

У порівнянні із нелегітимним абонентом другого рівня, нелегітимний абонента першого рівня має декілька переваг. На перших кроках виконання атаки він має певний рівень доступу на обладнання оператора зв'язку IP- телефонії, а також може мати можливість підключення і установки додаткового обладнання до мережі оператора IP- телефонії.

У випадку коли нелегітимний абонент не має достатнього рівня доступу на обладнання оператора, може спробувати отримати доступ, виконуючи атаку на перебір паролів для отримання більш високого рівня доступу до сервісів IP - телефонії. Алгоритм дій нелегітимного абонента першого рівня наведено на рис.2.3. Імовірність $p_{18_{ЗАХОБЛ\_1}}$ характеризує ймовірність, що у нелегітимного абонента першого рівня на початку виконання активної атаки є доступ відповідного рівня достатній для проведення подальших дій з метою отримання несанкціонованого доступу до потоку даних IP - телефонії. Імовірність $p_{18_{ЗАХОБЛ\_1}}$ може бути визначена, наступним чином:

$$p_{18_{ЗАХОБЛ\_1}} = \begin{cases} 1, \textit{ якщо нелегітимний абонент має достатній рівень доступу}; \\ 0, \textit{ якщо нелегітимний абонент не має достатній рівень доступу}. \end{cases}$$

Імовірність $p_{19_{ЗАХОБЛ\_1}}$ відображає ймовірність події, у випадку коли нелегітимний абонент підключив своє необхідне обладнання в мережі оператора IP - телефонії на вузол, через який є доступ до даних (медіа трафіку).

$$p_{19_{ЗАХОБЛ\_1}} = \begin{cases} 1, \textit{якщо нелегітимний абонент зміг встановити своє обладнання} \\ \qquad \textit{на вузлі оператора}; \\ 0, \textit{якщо нелегітимний абонент не зміг встановити своє обладнання} \\ \qquad \textit{на вузлі оператора}. \end{cases}$$

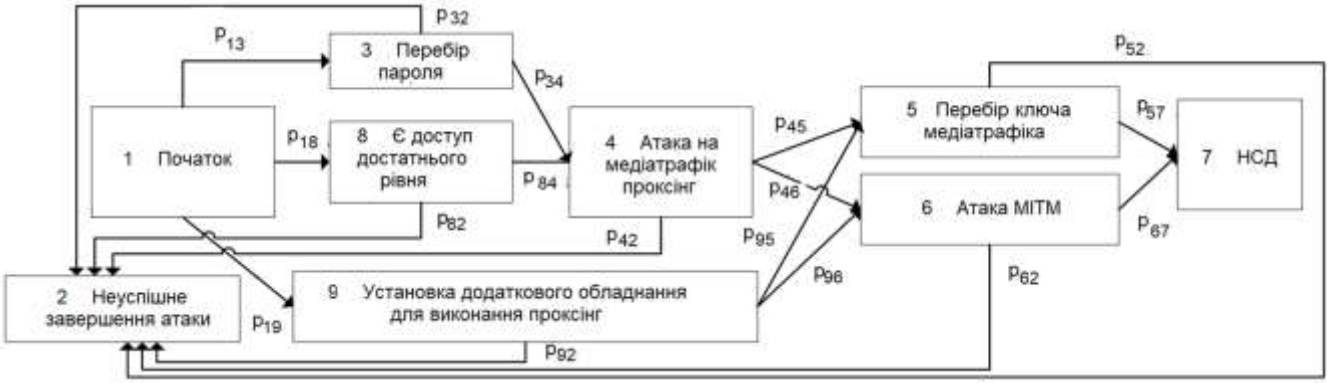


Рисунок 2.3 - Алгоритм дій при виконанні
захоплення обладнання оператора нелегітимним абонентом першого рівня

Обладнання, яке встановлюється нелегітимним абонентом повинно мати функціонал модифікації або віддзеркалення пакетів. Починаючи з цього моменту нелегітимний абонент для подальшого проведення активної атаки вибирає один з можливих наступних двох шляхів. Вибір продовження активної атаки залежить від встановленого обладнання та його технічних характеристик. Однак, навіть у випадку установки необхідного устаткування в нелегітимного абонента є ймовірність, що активна атака може бути проведена неуспішна. Наприклад - це може відбутися, якщо захищаючий об'єкт почне використовувати додаткові сервіси та механізми IP –телефонії для відстеження атаки (вторгнення) нелегітимного абонента або додаткові IP – протоколи IP - телефонії, використання яких не було враховано при проведені активної атаки нелегітимним абонентом, і не враховані в обладнанні нелегітимного абонента.

На основі отриманих результатів, які отримані проведеним аналізом, можливих дій нелегітимного абонента побудований відповідний імовірнісний граф, представлений на рис. 2.4. У наведеному імовірнісному графі виділена гілка, яка відповідає успішному виконанню атаки метою якої є отримання несанкціонованого доступу до потоку даних IP - телефонії і складена утворююча функція $H(x)$ цієї гілки. Для імовірнісного графа показаного на рис.2.4 представлені $P_{НСД}$.

Для імовірнісного графа захоплення обладнання оператора, представлені $P_{НСД} = H(x=1)$:

$$P_{НСДЦ_{ЗАХОБЛ\_1}} = \left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{45} + p_{19} + p_{95}\right)p_{57} +$$
$$+\left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{46} + p_{19} + p_{96}\right)p_{67},$$

де p_{ij} - ймовірність переходу з вершини *i* графа в вершину *j*.

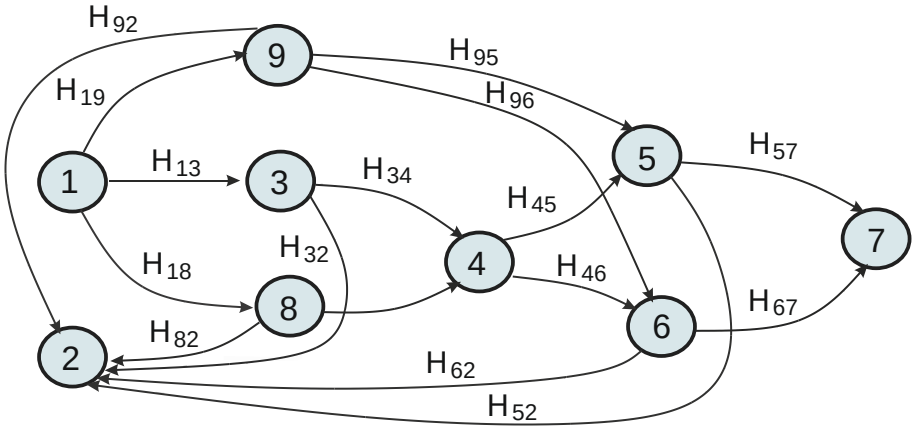


Рисунок 2.4 - Імовірнісний граф захоплення обладнання оператора нелегітимним абонентом першого рівня

Тоді ймовірність захисту від атаки несанкціонованого доступу до потоку даних IP - телефонії матиме наступний вигляд:

$$P_{ЗАХ\_НСДЦ_{ЗАХОБЛ\_1}} = 1 - P_{НСДЦ_{ЗАХОБЛ\_1}} = 1 - \left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{45} + p_{19} + p_{95}\right)p_{57} +$$
$$+\left(\left(p_{13B}p_{34} + p_{18}p_{84}\right)p_{46} + p_{19} + p_{96}\right)p_{67},$$

де p_{13} - ймовірність вибору активної атаки перебір пароля для доступу нелегітимного абонента до обладнання оператора IP - телефонії; p_{18} - ймовірність наявності в нелегітимного абонента успішного доступу достатнього рівня на обладнання оператора IP - телефонії; p_{19} - ймовірність наявності в нелегітимного абонента можливості установки необхідного обладнання для успішного виконання атаки; p_{34} - ймовірність для нелегітимного абонента успішного завершення атаки по перебору пароля для доступу до обладнання оператора IP – телефонії Інтернет мереж; p_{45} - ймовірність вибору атаки нелегітимним абонентом "злом шифру" для проведення дешифрування захищеного потоку даних IP – телефонії; p_{46} -

ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{57} - ймовірність успішного завершення нелегітимним абонентом активної атаки "злом шифру" для проведення дешифрування захищеного потоку даних IP – телефонії; p_{67} - ймовірність успішного завершення атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{95} - ймовірність вибору атаки нелегітимним абонентом "злом шифру" для проведення дешифрування захищенго потоку даних IP – телефонії; p_{96} - ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів) між учасниками сесії.

Захоплення монітору кореспондента нелегітимним абонентом з метою отримання несанкціонованого доступу до потоку даних IP – телефонії. Розглянемо модель нелегітимного абонента першого рівня, вирішенням задачі якого є отримання несанкціонованого доступу до потоку даних IP – телефонії, задача вирішується виконанням активної атаки ціллю якої є захоплення монітора кореспондента. Алгоритм дій нелегітимного абонента першого рівня наведено на рис. 2.5. На основі отриманих результатів, які отримані проведеним аналізом, можливих дій нелегітимного абонента ціллю якого є захоплення монітора побудований відповідний імовірнісний граф, представлений на рис.2.6. У наведеному імовірнісному графі захоплення монітора кореспондента виділена гілка, яка відповідає успішному виконанню атаки метою якої є отримання несанкціонованого доступу до потоку даних IP - телефонії і складена утворююча функція H (x) цієї гілки. Для імовірнісного графа захоплення монітора кореспондента представлені $P_{НСД}$.

Для імовірнісного графа захоплення монітора кореспондента представлена ймовірність успішного завершення атаки несанкціонованого доступу до потоку даних IP – телефонії - $P_{НСД} = H(x=1)$:

$$P_{НСДЦ_{ЗАХМОН\_1}} = p_{13}\left(p_{46}p_{34} + p_{56}p_{35}\right)\left(p_{67}p_{710} + p_{68}p_{810} + p_{69}p_{910}\right),$$

де p_{ij} - ймовірність переходу з вершини *i* графа в вершину *j*.

Рисунок 2.5 - Алгоритм дій при виконанні
захоплення монітора кореспондента нелегітимним абонентом першого рівня

Тоді ймовірність захисту від атаки несанкціонованого доступу до потоку даних IP - телефонії матиме наступний вигляд:

$$P_{ЗАХ\_НСДЦ_{ЗАХМОН\_1}} = 1 - P_{НСДЦ_{ЗАХМОН\_1}} =$$
$$= 1 - p_{13}\left(p_{46}p_{34} + p_{56}p_{35}\right)\left(p_{67}p_{710} + p_{68}p_{810} + p_{69}p_{910}\right)$$

де p_{13}- ймовірність проведення активної атаки при наявності віддаленого підключення до сервісів IP - телефонії; p_{34} - ймовірність вибору активної атаки перебір пароля для доступу нелегітимного абонента до обладнання оператора IP - телефонії; p_{46} - ймовірність для нелегітимного абонента успішного завершення атаки по перебору пароля для доступу до обладнання оператора IP – телефонії за обмежений час; p_{35} - ймовірність вибору активної атаки перебору пароля для доступу нелегітимного абонента до обладнання оператора IP - телефонії під час прослуховування трафіку кореспондента; p_{56} - ймовірність успішного завершення активної атаки нелегітимного абонента перехоплення пароля до наявного обладнання абонента під час прослуховування трафіку управління; p_{68} - ймовірність вибору активної атаки нелегітимним абонентом «зустріч по середині» для всіх IP - протоколів IP - телефонії; p_{810}- ймовірність успішного завершення активної атаки нелегітимним абонентом «зустріч по середині» для

всіх IP - протоколів IP - телефонії; p_{67} - ймовірність вибору активної атаки нелегітимним абонентом «установка закладки на програмне забезпечення на моніторі кореспондента»; p_{710} - ймовірність успішного завершення активної атаки нелегітимним абонентом «установка закладки на програмне забезпечення на моніторі кореспондента або відключення системи захисту»; p_{69} - ймовірність проведення активної атаки нелегітимним абонентом «повне або часткове відключення безпеки на сервісах IP – телефонії»; p_{910} - ймовірність успішного завершення атаки нелегітимним абонентом «повне або часткове відключення безпеки на сервісах IP – телефонії».

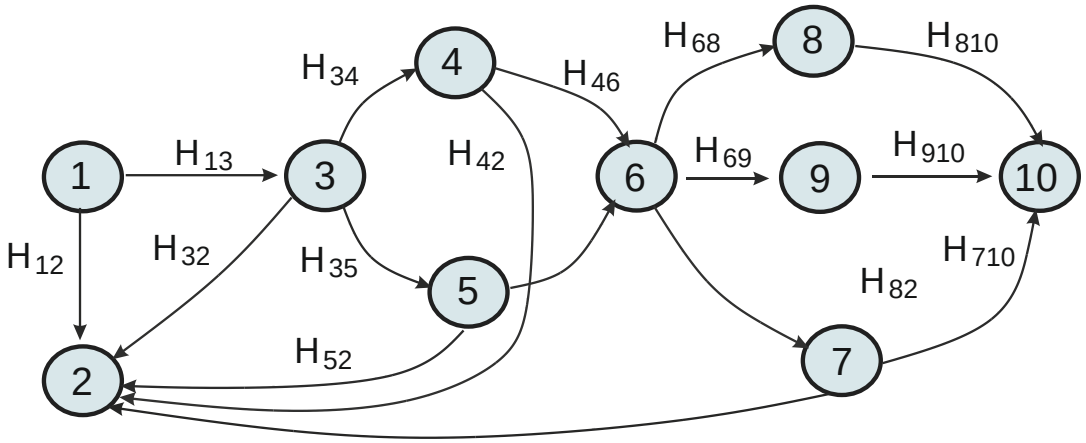


Рисунок 2.6 - Імовірнісний граф захоплення монітора кореспондента нелегітимним абонентом першого рівня

Значення деяких ймовірностей, які використанні при опису імовірнісного граф захоплення обладнання оператора, а також захоплення монітора кореспондента нелегітимним абонентом першого рівня, вимагають більш детальної оцінки експертами. Значення даних ймовірностей також залежать від нелегітимним абонентом, його рівня можливостей, рівня захисту та якості сервісів IP - телефонії.

2.5 Висновки

Проведений аналіз можливих активних успішних атак (загроз) та проведено дослідження виявлення їх можливих джерел. Знаючи вразливості та рівень захищеності об’єкта, для якого необхідно провести захист, активний зловмисник може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об’єкта.

Запропонована модель нелегітимного креспондента буде враховувати рівень можливостей зловмисників. Модель нелегітимного креспондента першого рівня враховує нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP – телефонії: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів.

Визначені цілі нелегітимних абонентів першого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії: $Ц_{ЗАХОБЛ\_1}$-захоплення обладнання оператора нелегітимним абонентом першого рівня; $Ц_{ЗАХМОН\_1}$ - захоплення монітору абонента нелегітимним кореспондента першого рівня. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP - телефонії. На основі проведеного аналізу алгоритмів поведінки нелегітимних абонентів почнемо розроблено модель нелегітимного абонента першого рівня по кожній з перерахованих цілей.

3 ІМОВІРНІСНІ АЛГОРИТМИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

3.1 Модель нелегітимного абонента другого рівня безпечної IP - телефонії

Модель нелегітимного креспондента буде враховувати рівень можливостей зловмисників, до другого рівня віднесемо нелегітимних абонентів які не мають відповідного рівня доступу до сервісів безпечної IP - телефонії. До нелегітимних абонентів (другий рівень) можуть в даному випадку бути віднесені: сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури.

Визначмо цілі нелегітимних абонентів другого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії: $Ц_{ЗАХОБЛ\_2}$ - захоплення обладнання оператора нелегітимним абонентом другого рівня; $Ц_{ЗАХМОН\_2}$ - захоплення монітору абонента нелегітимним кореспондентом другого рівня. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP - телефонії. На основі проведеного аналізу алгоритмів поведінки нелегітимних абонентів розпочнемо розробку моделі нелегітимного абонента другого рівня по кожній з перерахованих цілей.

Захоплення обладнання оператора нелегітимним абонентом другого рівня. Розглянемо модель нелегітимного абонента другого рівня, задачею якого є проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії, результатом успішної активної атаки – захоплення обладнання оператора.

Алгоритм дій нелегітимного абонента другого рівня наведено на рис. 3.1. Для виконання початку атаки нелегітимний абонента другого рівня повинен визначитися, на який сервіс IP - телефонії буде здійснювати активну атаку. Одним із можливих варіантів нелегітимному абоненту отримати необхідну інформацію

використати команду tracert, результатом виконання команди є проміжні вузли між нелегітимним абонентом і об'єктом атаки. Таким чином з великою ймовірністю можна вказати що ці вузли будуть задіяні в сеансі обміну поетками даних між двома абонентами.

Рисунок 3.1 - Алгоритм дій при виконанні захоплення обладнання оператора нелегітимним абонентом другого рівня

Після вибору сервіса IP-телефонії – атаки нелегітимним абонентом, буде спроба захопити управління цим сервісом IP-телефонії, виконуючи при цьому, активну атаку наприклад перебір пароля. Однак механізмами і сервісами IP-телефонії - віддалене управління технічно може бути заборонено для нелегітимного абонента з використанням списків доступу ACL. Імовірність p_{12} - ймовірність проведення активної атаки при наявності віддаленого відключення до сервісів IP-телефонії з боку нелегітимного абонента або у оператора встановлені ACL; імовірність p_{13} - ймовірність проведення активної атаки при наявності віддаленого підключення до сервісів IP – телефонії, подія, зворотна p_{12}.

Нелегітимним абонент вибирає доступний протокол для проведення активної атаки (telnet, ssh, SNMP, http / https) віддаленого управління сервісами IP – телефонії, об'єкт на який виконується атак типу «перебір пароля». Імовірність успішного завершення атаки типу «перебір пароля» за відведений час визначається наступним чином:

$$p_{34_{ЗАХОБЛ\_2}} = f\left(l,t,d,c\right), \tag{3.1}$$

де l - довжина логіна / пароля; t - відведений час, протягом якого буде успішне завершення атаки, виконати перебір; d - додаткові механізми та засоби обмеження IP - протоколу, що унеможливлюють виконання атаки типу «перебір пароля» за відведений час, а також відповідні програмно-апаратні та технічні можливості нелегітимного абонента; c - швидкість каналу зв'язку Інтернет мережі IP - телефонії, під час виконання атаки.

Імовірність $p_{34_{ЗАХОБЛ\_2}}$ ймовірність успішного завершення активної атаки типу «перебір пароля» нелегітимного абонента і зловмисник має доступ до обладнання оператора IP - телефонії; p_{32} - імовірність неуспішного завершення активної атаки типу «перебір пароля» нелегітимного абонента, за відведений час.

У разі успішного захоплення нелегітимним абонентом віддаленого управління сервісами IP – телефонії, зловмисник може досягти несанкціонованого доступу до потоку даних IP – телефонії використовуючи при цьому один з двох наступних шляхів: може виконати перебір пароля до переданого по Інтернет мережі медіа трафіку і виконувати прослуховування потоку даних IP - технології, або виконати атаку на механізм програмного розподілу загальної секретної інформації (ключів) і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації. Однак - успішне виконання розглянутих атак нелегітимним абонентом може не привести до досягнення цілі поставленої мети зловмисника несанкціонованого доступу до потоку даних, якщо при цьому не існує можливості виконати атаку типу «зустріч по середині» на медіа трафік, при цьому створивши та розмістивши відповідні правила на обладнанні оператора IP-телефонії, які дозволять нелегітимному абоненту пропускати трафік кореспндента через своє обладнання.

Імовірність успішної атаки нелегітимним абонентом на медіа трафік з метою отримання несанкціонованого доступу до потоку даних (атака типу «зустріч по середині», організація проксінг) можна визначити за наступною формулою:

$$1-p_{42_{ЗАХОБЛ\_2}}=\begin{cases}1, \textit{ якщо існує технічна можливість на обладнанні оператора створити правило для перенаправлення трафіку користувача в сторонузловмисника для виконання цілей "проксінг" MITM}\\ 0, \textit{ якщо не існує такої технічної можливості}\end{cases}$$

Під активною атакою нелегітимним абонентом розуміється зміна маршруту потоку даних передачі пакетів мультимедійних файлів, що дозволять нелегітимному абоненту пропускати трафік кореспндента через своє обладнання.

У разі успішного проведення атаки нелегітимний абонент може виконати підбір пароля до переданого по Інтернет мережі медіа трафіку і виконувати прослуховування потоку даних IP - технології, або виконати атаку на механізм програмного розподілу загальної секретної інформації (ключів) і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації.

При цьому ймовірності відображають: p_{45} - ймовірність, що нелегітимний абонент почав виконувати підбір пароля до переданого по Інтернет мережі медіа трафіку; p_{46} - ймовірність, що нелегітимний абонент почав виконувати атаку на механізм програмного розподілу загальної секретної інформації (ключів) на IP - телефонію. Імовірність p_{57} - означає успішну атаку нелегітимного абонента на підбір пароля до переданого по Інтернет мережі медіа трафіку. В даному випадку нелегітимному абоненту стає доступно виконувати прослуховування потоку даних IP - технології, або виконати атаку на механізм програмного розподілу загальної секретної інформації (ключів) і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації.

Імовірність p_{52} відображає неуспішне закінчення атаки нелегітимного абонента на підбір пароля до переданого по Інтернет мережі медіа трафіку по підбору пароля за обмежений час. $T_{ЗЛВ\_АКТ}$ - час на протязі якого дані актуальні – залежить від призначення даних. $T_{ЗЛВ\_ПРЛ}$ - час, необхідний на підбір пароля,

залежить від рівня технічних потужностей нелегітимного абонента - $ЗЛВ_{ПТ}$, які застосовуються для захисту мультимедійних файлів криптографічних примітивів і криптоалгоритмів - $ЗЛВ_{КР}$, довжини ключа - $ЗЛВ_{L}$, а також від ускладнюючих елементів (застосування ініціалізуючго вектора, додаткових лічильників і т. д.) - $ЗЛВ_{Д}$.

$$p_{57} = f\left(T_{ЗЛВ\_АКТ}, T_{ЗЛВ\_ПРЛ}\right) = f\left(T_{ЗЛВ\_АКТ}, ЗЛВ_{ПТ}, ЗЛВ_{КР}, ЗЛВ_{L}, ЗЛВ_{Д}\right) \quad (3.2)$$

$$p_{52} = 1 - p_{57} \quad (3.3)$$

Імовірність p_{67} визначає успішну атаку на механізм програмного розподілу загальної секретної інформації (ключів) і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації на механізм розподілу ключів. Під атакою в даній ситуації будемо розуміти вторгнення нелегітимного абонента в каналу зв'язку потоку даних IP- телефонії в момент обміну секретною інформацією між абонентами сесії IP - телефонії. Таким чином це дозволить нелегітимному абоненту виробити два секретних ключа – для обміну інформацією з кожним кореспондентом незалежно один від одного.. Тим самим, під час під час сеансу двох кореспондентів нелегітимний абонент виконує шифрування і дешифрування потоку даних мультимедійних файлів IP – телефонії з використанням власної секретної інформації. Імовірність успішної атаки залежить від рівня потужності використовуваних нелегітимним абонентом програмно-апаратних та технічних засобів для проведення для проведення атаки типу «зустріч по середині» на IP - протокол розподілу секретної інформації між абонентами сесії IP - телефонії.

Необхідно також врахувати, що для проведення активної атаки нелегітимним абонентом необхідна розробка відповідного програмного забезпечення, Імовірність p_{62} відображає неуспішне виконання активної атаки типу «зустріч по середині» нелегітимним абонентом і визначається як:

$$p_{62} = 1 - p_{67} \quad (3.4)$$

Для аналізу алгоритму поведінки дій нелегітимного абонента при виконання активної атаки типу «зустріч по середині» використовується відповідний математичний апарат теорії імовірнісних графів, дозволяє отримати для оцінку даного алгоритму та оцінити середній час необхідний для успішного виконання і ймовірність успішного завершення проведеної атаки. На рис. 3.2 представлений імовірнісний граф який описує алгоритм поведінки дій нелегітимного абонента при виконання активної атаки типу «зустріч по середині». Імовірнісний граф використовується в даному випадку для отримання утворюючої функції, для вирішення задачі переходу системи з початкового стану в кінцевий. Кожній гілки імовірнісного графа відповідає відповідна утворююча функція.

На основі отриманих результатів, які отримані проведеним аналізом, можливих дій нелегітимного абонента побудований відповідний імовірнісний граф, представлений на рис. 3.2. У наведеному імовірнісному графі виділена гілка, яка відповідає успішному виконанню атаки метою якої є отримання несанкціонованого доступу до потоку даних IP - телефонії і складена утворююча функція $H\ (x)$ цієї гілки. Для імовірнісного графа показаного на рис. 3.2 представлені $P_{НСД} = H(x=1)$:

$$P_{НСДЦ} = p_{13}p_{34}\left(p_{45}p_{57} + p_{46}p_{67}\right) \tag{3.5}$$

де p_{ij} - ймовірність переходу з вершини *i* графа в вершину j.

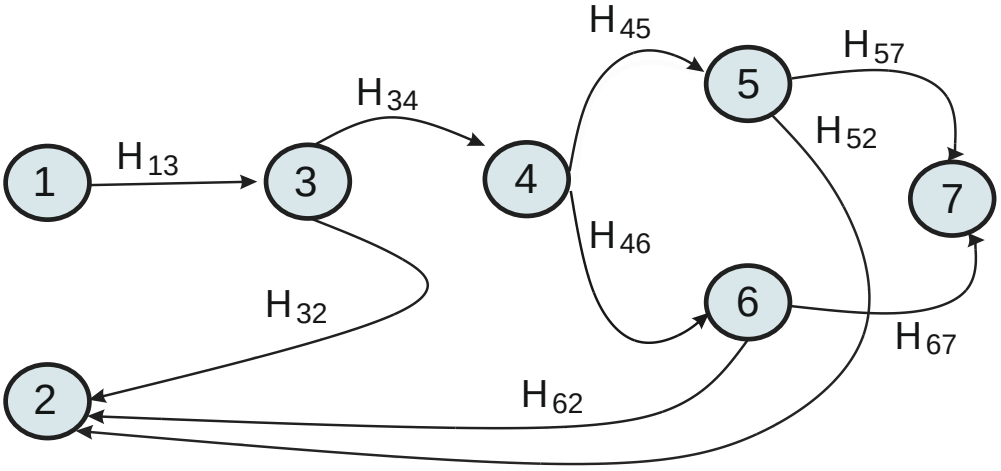


Рисунок 3.2 - Імовірнісний граф дій при виконанні захоплення обладнання оператора нелегітимним абонентом другого рівня

Захоплення монітору кореспондента нелегітимним абонентом другого рівня з метою отримання несанкціонованого доступу до потоку даних IP – телефонії..

Розглянемо модель нелегітимного абонента другого рівня, вирішенням задачі якого є отримання несанкціонованого доступу до потоку даних IP – телефонії, задача вирішується виконанням активної атаки ціллю якої є захоплення монітора кореспондента. Алгоритм дій нелегітимного абонента другого рівня наведено на рис. 3.3. На основі отриманих результатів, які отримані проведеним аналізом, можливих дій нелегітимного абонента більш детально розглянуті атаки які може виконати нелегітимний абонент, в залежності від доступу до шлюзу чи персонального комп'ютера кореспондента. При доступу до шлюзу нелегітимного абонента найбільш вірогідною є проведення активної атаки з проксінг всього трафіку з використанням обладнання нелегітимного абонента. Атака виконується за схемою, представленою на рис. 3.4, де на схемі показані IPI, IP2 - шлюзи кореспондента, а S_H - сервер нелегітимного абонента з встановленим на ньому спеціалізованого програмного забезпечення.

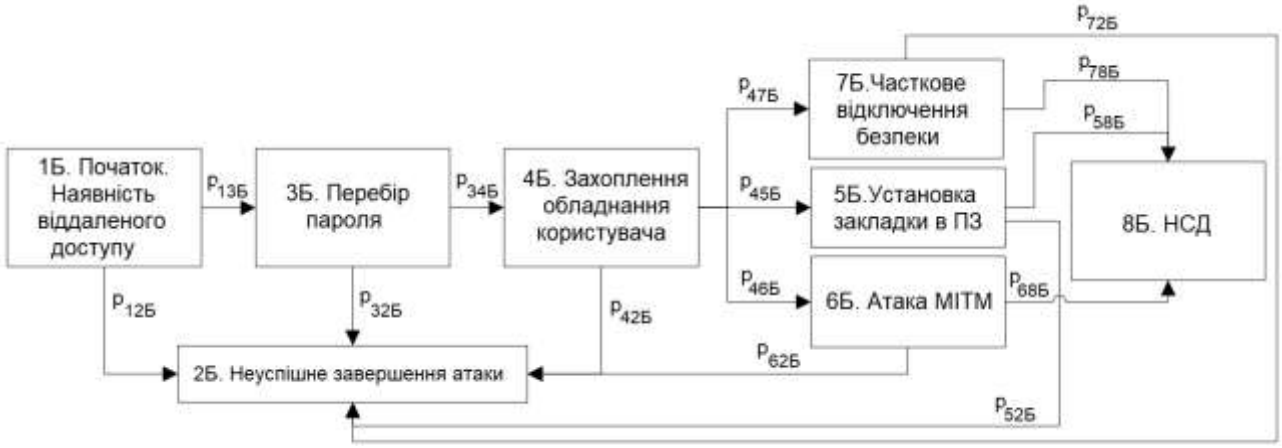


Рисунок 3.3 - Алгоритм дій при виконанні захоплення монітора кореспондента нелегітимним абонентом другого рівня

Для успішного проведення цієї атаки нелегітимному абоненту потрібно в отримати в першу чергу доступ до монітора кореспондента і захопити управління VoIP монітором і встановити відновідне спеціалізоване програмне забезпечення та виконати дії по його переналаштуванні. Наприклад - якщо у кореспондента на VoIP моніторі в режимі точка-точка в відповідному запису в телефонній книжці

шлюзу зберігаються номера - IP-адреса IP – телефонії, то нелегітимний абонент в стані підмінити IP - адресу на VoIP моніторі кореспондента Б в записнику на VoIP моніторі кореспондента А на свою - IP-адресу IP – телефонії, в результаті виконаних дій дзвінки (потоку даних) з телефону кореспондента А будуть приходити на сервер нелегітимного абонента - S_H. Таким чином в даній ситуації - сервер нелегітимного абонента буде виконувати взаємозв'язок через IP - протоколи IP – телефонії безпеки між власним сервером і кореспондентом Б від імені іншого абонента мережі IP- телефонії - кореспондента А. IP -протоколи безпеки Інтернет мережі також будуть виконуються IP – технологією між кореспондентами Б і сервером нелегітимного абонента. В результаті виконаних дій нелегітимний абонент отримує доступ до всього потоку даних(інформації), яка буде передається між кореспондентами А і Б, у відкритому доступі і при необхідності може модифікуватися нелегітимним абонентом а також при прослуховуватися. Перенаправлення потоку даних IP- телефонії від кореспондента А на сервер нелегітимного абонента S_H можна здійснювати не тільки за рахунок підміни IP - адресу на VoIP моніторі, а також і за рахунок зміни налаштувань на шлюзі кореспондента А, встановивши адресу сервера нелегітимного абонент S_H в якості проксі-сервера або в якості основного сервера Інтернет мережі IP-телефонії.

Рисунок 3.4 - Атака з проксінг при виконанні захоплення монітора
а) виконання розподілу загальної секретної інформації, б) встановлений захищений канал голосової інформації

При використанні VoIP монітора нелегітимним абонентом на якому встановлений програмний шлюз IP-телефонії найбільш вірогідним здійснення активної атаки є: атака з проксінг всього потоку даних медіатрафіка кореспондентів через сервер нелегітимного абонента S_H; або впровадження програми-хакера на VoIP монітор.

Суть атаки з впровадженням програми-хакера полягає в можливості установки на VoIP моніторі кореспондента спеціалізованого програмного забезпечення, задача якого передавати голосовій інформацію у відкритому вигляді з VoIP монітор кореспондента або передавати весь потік даних як вихідних так і вхідних пакетів з мережевого інтерфейсу IP-телефонії VoIP монітора кореспондента на сервер нелегітимного абонента S_H для подальшої відповідної обробки. Окрім цього для доступу до потоку голосової інформації, яка передається на сервер нелегітимного абонента S_H, зловмиснику необхідно також вимкнути на VoIP моніторі кореспондента А IP-протоколи безпеки IP-телефонії, або, переналаштувати режим роботи протокола IP-телефонії SRTP, відключити опцію шифрування переданої голосової інформації. IP-телефони і шлюзи захищеної IP-телефонії мають в своєму розпорядженні можливість віддаленого управління сервісами IP-телефонії, яка використовується абонентами для їх налаштування. Обчислювальні пристрої, які використовуються захищеною IP-телефонією також можуть мати дистанційне керування, яке може бути організоване внутрішніми програмно – апаратними засобами та механізмами використовуваної операційної системи, або з використанням спеціалізованого додаткового програмно-апаратного забезпечення. Існує також можливість відключення віддаленого управління кореспондентами захищеної IP-телефонії, також можливо обмежити використання віддаленого управління за рахунок сервісів IP-телефонії, застосуванням списків доступу.

Таким чином, для успішного проведення активної атаки нелегітимним абонентом, виникає необхідність в захопленні управління віддаленим VoIP монітором. Як показано успішність активної атаки в першу чергу залежить від

багатьох факторів в загальному це рівень захищеності IP-телефонії і також рівня потужності спеціалізованого програмного забезпечення та механізмів взлому нелегітимного абонента. Таким чином імовірність успішного проведення атаки представимо наступним чином:

$$p_{34_{ЗАХМОН\_2}} = \begin{cases} 1, \textit{ якщо у користувача терміналу включено віддалене управління} \\ \quad \textit{і немає налаштованих списків доступу на всі віддалені протоколи} \\ 0, \textit{ якщо у користувача терміналу включено віддалене управління} \\ \quad \textit{і є налаштовані списки доступу на всі віддалені протоколи} \\ 0, \textit{ якщо у користувача терміналу вимкнено віддалене управління} \end{cases}$$

В випадку наявності сервісів захищеної IP-телефонії віддаленого управління, нелегітимному абоненту для успішного проведення активної атаки необхідно з використанням спеціалізованого програмного забезпечення підібрати пароль (логін-пароль) для авторизації (отримання доступу) на VoIP моніторі кореспондента. При цьому вводиться допущення, що IP адреса об’єкта активної атаки відома нелегітимному абоненту і отримана заздалегідь. Таким чином підбір пароля (логіна-пароля) залежить від IP – протоколу, рівня захищеності IP-телефонії віддаленого управління, на який виконується активна атака нелегітимного абонента. Імовірність виконання успішної атаки по підбору пароля можна оцінювати за кінцевий інтервал часу T, так як ймовірність виконання успішної атаки по перебору пароля за нескінченний час буде дорівнює 1. Імовірність виконання успішної атаки по підбору пароля визначимо:

$$p_{45_{ЗАХМОН\_2}} = f\left(l, T, D, C\right), \tag{3.6}$$

де l - довжина пароля(логіна-пароля); T - відведений час, протягом якого буде успішне завершення атаки, виконати перебір; D - додаткові механізми та засоби обмеження IP - протоколу, що унеможливлюють виконання атаки типу «перебір пароля» за відведений час, а також відповідні програмно-апаратні та технічні можливості нелегітимного абонента; C - швидкість каналу зв'язку Інтернет мережі IP - телефонії, під час виконання атаки.

У разі успішного перебору пароля і отримання доступу до VoIP монітору креспондента, захоплення нелегітимним абонентом віддаленого управління сервісами IP – телефонії, зловмисник може отримати несанкціонований доступ до потоку даних IP – телефонії використовуючи при цьому один з двох наступних шляхів: установка закладки в спеціалізоване програмне забезпечення кореспондента, модифікація програмного забезпечення VoIP монітору; коригування налаштувань VoIP монітору кореспндента; здійснення атаки типу «зустріч по середині» на всі протоколів захищеної IP-телефонії.

Можливість проведення відповідної атаки визначається рівнем забезпечення програмно –апаратними та технічними засобами та механізмами нелегітимного абонента, а також наявністю в нелегітимного абонента спеціалізованих інструментів і засобів.

Сутність першої атаки нелегітимного абонента полягає в захопленні голосової інформації в обхід IP - протоколів IP-телефонії, або в відключенні IP - протоколів Інтернет мережі захищеної IP-телефонії, або в зміні режимів роботи IP - протоколів Інтернет мережі захищеної IP-телефонії, щоб можна було виконувати нелегітимним абонентом прослуховування голосової інформації (медіа трафіка). Сутність другої а також і третьої атаки полягає в корегуванні налаштувань VoIP монітору кореспндента IP-телефонії для реалізації атаки типу «зустріч по середині», при якій весь потоку даних IP - протоколів безпеки Інтернет мережі захищеної IP-телефонії проходять через нелегітимного абонента, який в свою чергу має можливість контролювати передану голосову інформацію, а також при необхідності виконувати модифікацію переданого потоку даних. Таким чином при проведені даної атаки нелегітимний абонента, виконує сценарій з'єднання по черзі з кожним з кореспондентів, при цьому використовує IP - протоколи безпеки Інтернет мережі захищеної IP-телефонії, відповідно представленої схеми на рис.3.5.

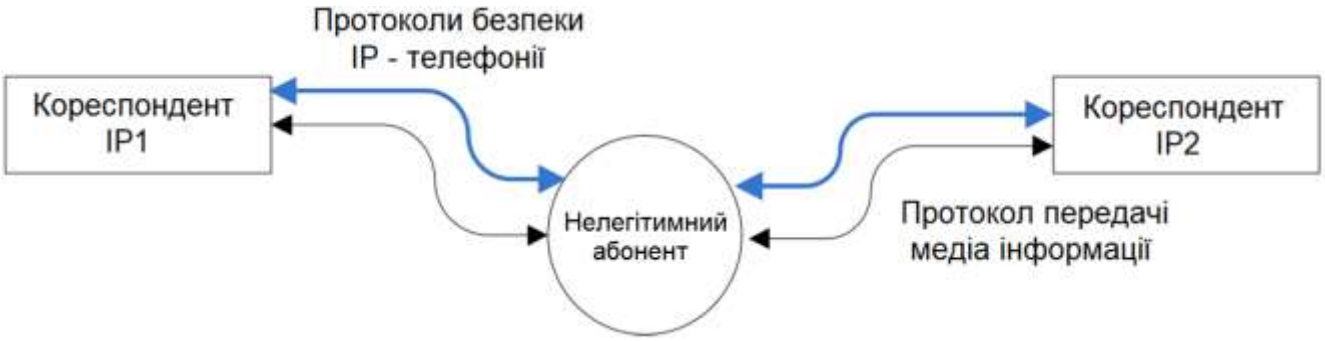


Рисунок 3.5 - Реалізація атаки «зустріч посередині» для IP - протоколів забезпечення безпеки VoIP-моніторів

Вибравши один з варіантів здійснення атаки, нелегітимний абонент після її успішного завершення в змозі отримати несанкціонований доступ до потоку даних IP - телефонії. Однак також при цьому існує ймовірність неуспішного виконання вибраного варіанта здійснення атаки, яка в даному випадку буде відображається віргідностями p_{72} і p_{62} відповідно. Наприклад - атака типу "модифікація налаштувань VoIP-монітора кореспондента" може також закінчитися неуспішно, якщо кореспондент своєчасно виявить модифікацію налаштувань відновить попередні налаштування, при цьому також змінивши паролі доступу до VoIP-монітора або відключивши при цьому віддалене управління. На основі можливих дій нелегітимного абонента побудований відповідний імовірнісний граф, представлений на рис. 3.6.

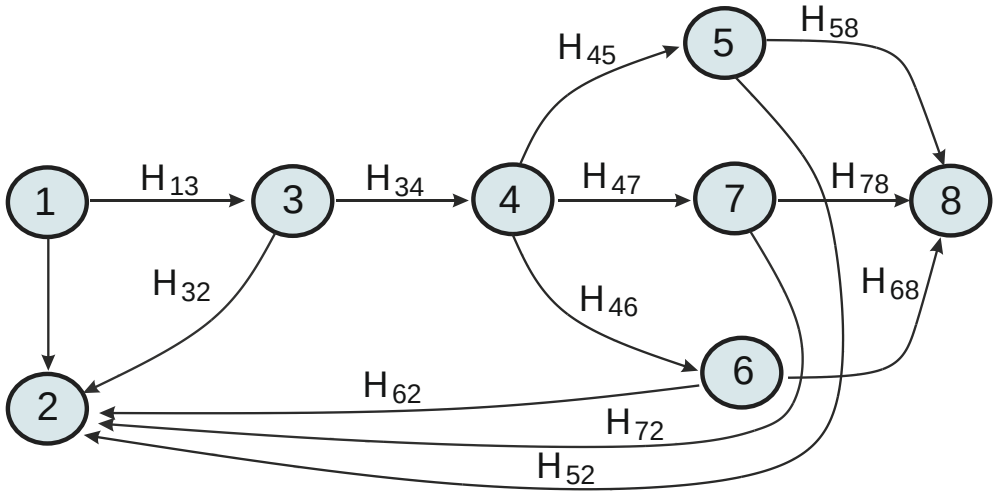


Рисунок 3.6 - Імовірнісний граф дій при виконанні захоплення VoIP-монітора нелегітимним абонентом другого рівня

У наведеному імовірнісному графі виділена гілка, яка відповідає успішному виконанню атаки метою якої є отримання несанкціонованого доступу до потоку даних IP - телефонії і складена утворююча функція H (x) цієї гілки. Для імовірнісного графа показаного на рис. 3.6 представлені $P_{НСД} = H(x=1)$:

$$P_{НСДЦ_{ЗАХМОН\_2}} = p_{13}p_{34}\left(p_{45}p_{58} + p_{46}p_{68} + p_{47}p_{78}\right) \qquad (3.7)$$

де p_{ij} - ймовірність переходу з вершини *i* графа в вершину *j*.

3.2 Оцінка імовірності нелегітимним абонентом успішного завершення атаки

Для кожного з розглянутих імовірнісних графів дій нелегітимного абонента наведені $P_{НСД}$:

$$P_{НСДЦ_{ЗАХОБЛ\_1}} = \left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{45} + p_{19} + p_{95}\right)p_{57} +$$
$$+\left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{46} + p_{19} + p_{96}\right)p_{67}$$

$$P_{НСДЦ_{ЗАХМОН\_1}} = p_{13}\left(p_{46}p_{34} + p_{56}p_{35}\right)\left(p_{67}p_{710} + p_{68}p_{810} + p_{69}p_{910}\right)$$

$$P_{НСДЦ_{ЗАХОБЛ\_2}} = p_{13}p_{34}\left(p_{45}p_{57} + p_{46}p_{67}\right)$$

$$P_{НСДЦ_{ЗАХМОН\_2}} = p_{13}p_{34}\left(p_{45}p_{58} + p_{46}p_{68} + p_{47}p_{78}\right),$$

де p_{ij} - ймовірність переходу з вершини *i* графа в вершину *j*.

$$P_{НСД} = \max\left\{P_{НСДЦ_{ЗАХОБЛ\_1}}, P_{НСДЦ_{ЗАХМОН\_1}}, P_{НСДЦ_{ЗАХОБЛ\_2}}, P_{НСДЦ_{ЗАХМОН\_2}}\right\} \qquad (3.8)$$

В випадку встановлення з'єднання між абонентами IP – телефонії в сценарії типу кореспондент-кореспондент без використання сервера а також при відсутності попередньо розподіленого загальної секретної інформації (ключового матеріалу), в даному випадку сам абонент є найбільш зацікавленою особою в приділення більшої уваги для підвищення безпеки IP – телефонії і при цьому зниження $P_{НСД}$. Коресподенти також можуть використовувати VoIP монітори, які підтримують в IP - телефонії функцію відключення віддаленого управління, що

призведе до $p_{13\_ЗАХМОН\_1}=0$, $p_{13\_ЗАХМОН\_2}=0$, і, в результаті отримаємо, $P_{НСДЦ_{ЗАХМОН\_1}}=0$, $P_{НСДЦ_{ЗАХМОН\_2}}=0$.

Однак, кореспондент не в змозі впливати на ймовірності $p_{ij\_ЗАХОБЛ\_2}$, $p_{ij\_ЗАХМОН\_2}$.

Таким чином в залежності від покрокових цілей нелегітимного абонента можна виділити декілька частих моделей нелегітимного абонента.

Також необхідно враховувати, що імовірності $p_{57\_ЗАХОБЛ\_1}$, $p_{57\_ЗАХОБЛ\_2}$ залежать від застосовуваного симетричного алгоритму шифрування. Фахівці а також рекомендації SRTP пропонують застосування симетричного алгоритму AES з ключем 256 біт. Успішна лобова атака такого алгоритму є вкрай малоймовірним. На основі проведеного аналізу та дослідження найбільш вірогідною атакою буде атака типу «зустріч по середині» на програмний розподіл загальної секретної інформації між учасниками сесії з боку нелегітимного абонента. Таким чином, можна також ввести допущення, що ймовірність вибору атаки «перебір пароля» на шифр наближається до 0 - $p_{45\_ЗАХОБЛ\_1}=0$, $p_{45\_ЗАХОБЛ\_2}=0$, а ймовірність вибору атаки типу «зустріч по середині» на програмний розподіл загальної секретної інформації між учасниками сесії з боку нелегітимного абонента $p_{46\_ЗАХОБЛ\_1}=1$, $p_{46\_ЗАХОБЛ\_2}=1$.

Тоді ймовірність успішної атаки з метою отримання несанкціонованого доступу до потоку даних виразимо наступним чином:

$$P_{НСД}=\max\left\{P_{НСДЦ\_ЗАХОБЛ\_1}, P_{НСДЦ\_ЗАХОБЛ\_2}\right\} \quad (3.9)$$

$$P_{НСДЦ_{ЗАХОБЛ\_2}}=p_{13\_ЗАХОБЛ\_2}p_{34\_ЗАХОБЛ\_2}p_{46\_ЗАХОБЛ\_2}p_{67\_ЗАХОБЛ\_2} \quad (3.10)$$

$$P_{НСДЦ_{ЗАХОБЛ\_1}}=\left(\left(p_{13}p_{34}+p_{18}p_{84}\right)\cdot\cdot p_{46}+p_{19}+p_{96}\right)\cdot p_{67} \quad (3.11)$$

Для дослідження ймовірнісно-часових характеристик необхідно розглянути протоколи розподілу загальної секретної інформації (ключів) захищеної 1P-телефонії, що відповідають вимогам до відповідних IP- протоколів: K_1 - підтримка

топології клієнт-сервер і клієнт-клієнт в Інтернет мережах IP – телефонії; K_2- функціонування без використання додаткових IP - протоколів IP – телефонії між кореспондентами для реалізації функції розподілу загальної секретної інформації (ключів); K_3- робота по можливості без передачі секретної інформації у відкритому вигляді по каналу зв'язку; K_4 - присутність механізму виявлення атак типу «зустріч по середині» без попередньо розподіленої загальної секретної інформації (ключів) між кореспондентами, а також при цьому без використання сертифікатів; K_5- використання як транспорт стека протоколів TCP/UDP портів, що застосовуються для IP-телефонії протоколами (SIP/RTP), або TCP/UDP портів, використання яких узгоджено в результаті встановлення з'єднання. Порівняння IP - протоколів приведено в таблиці 3.1.

Таблиця 3.1 - Оцінка протоколів розподілу ключового матеріалу на відповідність перерахованим вимогам

Вимоги до ПРК	Протоколи			
	DTLS	ZRTP	SDES	MIKEY
K_1	1	1	0	1
K_2	1	1	0	0
K_3	1	1	0	1
K_4	0	1	0	0
K_5	1	1	1	1
$Q_{ПРК}$	4	5	1	3

Оцінка кожного з протоколів проводиться у відповідності з функцією

$$Q_{ПРК}: Q_{ПРК} = \sum_{i=1}^{5} K_i$$

Протокол DTLS як видно з табл.3.1 не відповідає четвертій вивозі, так як DTLS розроблявся для роботи в топології клієнт - сервер і використовує встановлені відповідні сертифікати для захисту від атаки типу «зустріч по середині» у обох кореспондентів. Тому для DTLS K_4 = 0. На відміну від інших IP

протокол ZRTP має вбудований механізм SAS (Short Authentication String) для захисту від атаки типу «зустріч по середині». Тому для ZRTP K_4 = 1. Для SDES і MIKEY K_4= 0. Протокол MIKEY не задовольняє другій вимозі з таблиці 3.1, так як повідомлення протоколу можуть передаватися або в SIP / SDP-повідомлення, або поверх RTSP (Real Time Streaming Protocol), але в останньому випадку кореспонденти повинні додатково підтримувати протокол RTSP. Тому K_2= 0 для MIKEY. П'ята вимога при роботі поверх RTSP протоколу не виконується, але при цьому виконується друга вимога. При роботі MIKEY поверх в SIP / SDP-повідомлення п'ята вимога виконується, але не виконується друга вимога. Так як при оцінці $Q_{ПРК}$ використовується K_2= 0, то K_1= 1 для MIKEY. Протокол SDES не задовольняє першій і третій вимозі K_1 = 0 і K_3= 0, так як ключ передається між кореспондентами в відкритому вигляді в повідомленнях SDP і вимагає їх додаткового захисту. Для захисту як правило використовується додатковий IP -протокол SIPS. Однак, при з'єднанні клієнт-клієнт, коли у кореспондентів немає заздалегідь розподіленого загального секретного ключа, SIPS з'єднання з захистом від атаки типу «зустріч по середині» організувати неможливо. Протокол SDES не задовольняє другій вимозі, так як для передачі даних протоколу SDES використовуються повідомлення SIP / SDP. Відповідно K_2= 0 для SDES.

На основі проведеного аналізу представлених даних в табл.3.1 можна дати рекомендації по вибору IP протоколів це – IP - протоколи ZRTP і DTLS, рекомендовані протоколи мають найбільше значення $Q_{ПРК}$. Оцінка імовірнісно-часових характеристик виконується для вказаних IP –протоколів IP- телефонії. Результати проведеного аналізу та дослідження надають можливість вказати, що найбільш відомі IP-протоколи розподілу загальної секретної інформації (ключового матеріалу) необхідно вдосконалювати в двох напрямках: підвищення інформаційної безпеки IP - телефонії та покращення основних показників IP-протоколів Інтернет мереж.

Найбільш небезпечною атакою є атака типу «зустріч по середині» на IP - протоколи розподілу загальної секретної інформації (ключового матеріалу). Завдання формування загальної секретної інформації (ключового матеріалу) в умовах проведення атаки типу «атака по середині» вторгнення нелегітимного абонента на сучасному етапу є актуальною. Особливістю розглянутих робіт є те, що для формування загальної секретної інформації (ключового матеріалу) між кореспондентами використовується сценарій незалежності випадкових чисел в різних точках IP - телефонії передачі голосової інформації. У IP - протоколах формування загальної секретної інформації для IP - телефонії в основі яких лежить асиметричний алгоритм Діффі-Хелмана обмін секретною інформацією реалізується на мережевому рівні моделі OSI і таким чином ефекти випадкових чисел в різних точках IP - телефонії передачі голосової інформації однакові на каналах передачі потоку даних, тому розглянуті методи недоцільно використовувати для розподілу загальної секретної інформації для IP - телефонії.

Таким чином одним з методів забезпечення підвищення безпеки IP протоколу формування загальної секретної інформації є відслідкування і заборона виконання атаки типу «зустріч по середині» за рахунок використання в Інтернет мережах IP - телефонії декількох паралельних незалежних каналів сеансів зв'язку. Таким чином, використовувані в протоколі канали зв'язку повинні відповідати вимозі - не мати спільних точок, контролюючи які, зловмисник може одночасно атакувати використовувані канали.

3.3 Метод підвищення ефективності IP - протоколу розподілення секретної інформації ZRTP

Асиметричний алгоритм Діффі-Хелмана обміну секретною інформацією може бути може бути успішно атакованим активним нелегітимним абонентом. Тому при роботі протоколу Діффі-Хелмана під час обміну секретною інформацією необхідно забезпечити закритість та достовірність голосової інформації в каналах

зв’язку. Тому доцільно протокол Діффі-Хелмана обміну секретною інформацією використовувати в захищених каналах передачі голосової інформації, в яких унеможливується несанкціонованих доступ до голосової інформації та її модифікація або її підміна.

У разі необхідності в Інтернет мережі IP – телефонії встановлення захищеного з'єднання проти атак типу «зустріч по середині» між двома кореспондентами учасниками сесії, в даному випадку можлива ситуація що вони, можуть не мати загальних сертифікатів (загальний довірений центр), або протоколів секретною інформацією, а також при цьому можуть не мати загального захищеного каналу для встановлення зв'язку між собою.

У випадку наявності у кореспондентів сесії зв’язку IP – телефонії сертифікатів, різних центрів сертифікації, неможливо в даній ситуації перевірити достовірність кожного сертифікату, так як кожен з учасників сесії може не довіряти кореспондентів може не довіряти центру сертифікації іншого абонента. Для встановлення захищеного з'єднання між абонентами учасниками сесії IP - телефонії також виникає необхідність виконати генерацію та розподіл загальної секретної інформації (ключів) для реалізації цього з'єднання. Абоненти можуть в даній ситуації встановлення з'єднання використовувати алгоритми симетричного або алгоритми асиметричного шифрування IP - телефонії. Недоліком алгоритмів симетричного шифрування є необхідність передачі секретного ключа по відкритим каналам зв’язку. В нелегітимного абонента з’являється цілком вірогідна можливість перехоплення секретної інформації, що надають нелегітимному абоненту провести дешифрування переданих потоків даних в процесі сеансу зв'язку. Таким чином голосова інформація IP – телефонії буде доступна нелегітимному абоненту. При використанні алгоритмів асиметричного шифрування в разі передачі ключової інформації по відкритим каналам зв’язку передана інформація не буде прочитана нелегітимним абонентом, і випадку перехоплення переданого потоку даних IP – телефонії. Однак у випадку використання асиметричного алгоритму шифрування - при обміні відкритими (не

секретними) ключами, які використовуються для організації захищеного з'єднання IP – телефонії, в абонентів учасників зв’язку не буде можливості переконатися що несекретний ключ передається між ними без модифікації нелегітимним абонентом, як показано на рис. 3.7.

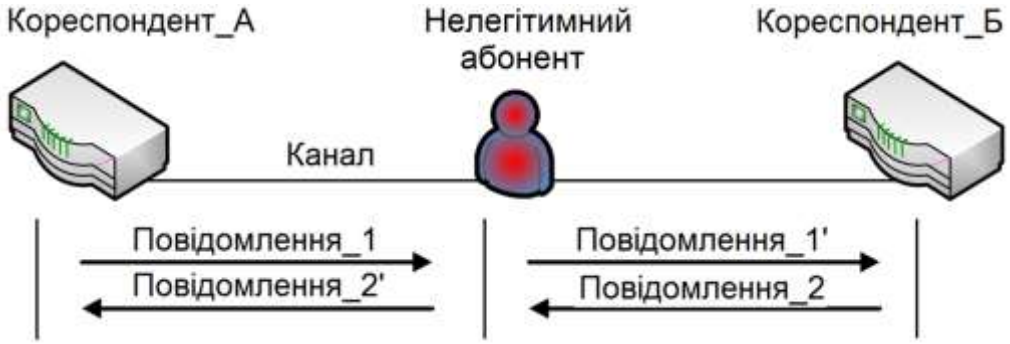


Рисунок 3.7 – Застосування атаки «зустріч по середині» при використанні асиметричного шифрування

Також до недоліків алгоритмів асиметричного щифрування слід віднести що несекретний-відкритий і секретний закритий ключі мають відносно великий розмір що утрудняє їх передачу по Інтернет мережі між абонентами зв’язку. Для підвищення безпеки генерації та обміну загальної секретної інформації пропонується використовувати наступні шляхи: підвищення безпеки передачі інформації за рахунок програмної перевірки аутентифікаційного рядка абонентів з використанням ще одного каналу зв'язку; а також використання сесії IP – телефонії декількох каналів зв'язку для виконання IP - протоколу розподілу загальної секретної інформації між абонентами сесії.

Захист від нелегітимного абонента в режимі використання сценарію клієнт-клієнт виконується за рахунок програмної перевірки аутентифікаційного рядка абонентів з використанням ще одного каналу зв'язку, при цьому аутентифікаційний рядок передається по голосовому каналу IP - телефонії в ручному режимі. Голосовий канал IP - телефонії в цьому випадку між абонентами сесії є додатковим каналом зв'язку Інтернет мережі, який діє паралельно по відношенню до IP-каналу IP - телефонії. Виникає необхідність в автоматизації процесу перевірки короткого аутетифікаційного рядка. Існуючий метод не

забезпечує необхідного рівня захищеності і не є безпечним, так як використовується в даному випадку один канал зв'язку між учасниками сесії IP – телефонії, а використовуванні на сучасному етапі засоби аналізу і синтезу голосової інформації дозволяють виконувати програмне вирізання відповідної інформації з потоку даних та подальшою заміною на відповідну інформацію, синтезовану нелегітимним абонентом.

Проведений аналіз та практичне дослідження показало, що існує висока ймовірність наявності між абонентами сеансу зв’язку, незалежних непересічних каналів зв’язку. Таким чином в основі запропонованих IP - протоколів IP – телефонії, використано перевага легітимних абонентів по відношенню до нелегітимних, перевага полягає в тому, що тільки легітимні абоненти учасники сесії мають доступ до отримання голосової інформації з двох і більше каналах потоку даних IP – телефонії одночасно, при цьому маючи в своєму розпорядженні інформацію про IP-адреси абонентів, яка я не є секретною також і для нелегітимних абонентів. Необхідно підкреслити, що запропонований метод модернізації IP- протоколів IP – телефонії розподілу загальної секретної інформації між абонентами сесії пропонується для підвищення захищеності, але даний IP- протоколів IP – телефонії не гарантує 100% достовірності. В якості оцінки модернізації IP- протоколів IP – телефонії використовуються наступні критерії величин наступних ймовірностей: ймовірність успішної активної атаки нелегітимним абонентом типу «зустріч по середині» $P_{УА\_ЗС}$; ймовірність виявлення активної атаки нелегітимним абонентом типу «зустріч по середині» $P_{ВА\_ЗС}$; ймовірність успішного розподілу та генерації загального секретного ключа $P_{У\_СК}$.

IP- протокол IP – телефонії ZRTP має в своєму розпорядженні механізм захисту активної атаки нелегітимним абонентом типу «зустріч по середині», виражений у вербальній перевірці короткого аутентифікаційного рядка по голосовому каналу між абонентами сесії IP – телефонії. В даному випадку після

успішного виконання IP- протоколу IP – телефонії ZRTP і встановлення голосового каналу між абонентами сесії в топології типу клієнт-клієнт без сервера, абоненти отримують відповідне значення короткого аутентифікаційного рядка - що представляє собою комбінацію символів обчислений та отриманих спеціалізованим алгоритмом. Один з абонентів учасник сесії вимовляє короткий аутентифікаційний рядок по голосовому каналу зв'язку IP – телефонії. Інший абонент який є також учасник сесії звіряє короткий аутентифікаційний рядок на своєму VoIP-моніторі зі значенням, отриманим по голосовому каналі. Якщо аутентифікаційні рядки співпадають, це означає, що в даному випадку відсутня активна атака нелегітимним абонентом типу «зустріч по середині», але може мати місце активна атака з підробкою аутентифікаційного рядка по голосовому каналу зв'язку. Якщо аутентифікаційні рядки не співпадають - має місце активна атака нелегітимним абонентом типу «зустріч по середині» в каналі передачі потоку даних. Таким чином, під час з'єднанні двох абонентів учасників сесії без участі сервера - аутентифікація в даному випадку буде виконуватися за рахунок відомостей абонентом голосових характеристик іншого абонента учасника зв’язку, а також за рахунок немодифікованої передачі потоку даних по двох каналах зв’язку - по першому по голосовому каналу SRTP і по другому каналу передачі даних.

Використання сучасного програмно-апаратного забезпечення та відповідних технологій достатньо просто виконають синтез голосової інформації так і аналіз голосу абонентів. Також виникає необхідність в розгляді наступних варіантів: абонентам відомі характеристики голосу один одного; другий варіант абонентам не відомі характеристики голосу.

У випадку першого варіанта, при встановленні з'єднанні викликаючий абонент, передає голосовою інформацією привітання а також ім'я іншого абонента викликаючої сторони. Після прийняття голосової інформації виконується вербальна перевірка аутентифікаційного рядка. Переданої голосової інформації може бути достатньо для синтезу голосової інформації абонента для підміни

одного набору символів на інші з метою модифікації аутентифікаційного рядка в голосовому каналі. В цьому випадку - перевірка аутентифікаційного рядка пройде успішно навіть при наявності активна атака нелегітимним абонентом типу «зустріч по середині» (рис. 3.8).

При використанні другого варіанту у випадку, коли абоненти не знають відповідних характеристик голосу один одного, не потрібно накопичення переданої голосової інформації даних, так як синтез в даному випадку можна виконувати маючи в своєму розпорядженні інформацію з використання будь-якого голосу. Таким чином як модернізація IP- протоколу IP – телефонії ZRTP пропонується впровадженням автоматизованої програмно-апаратної перевірки аутентифікаційного рядка. При використанні в даному випадку декілька каналів зв'язку, відповідна перевірка надасть можливість виявити нелегітимного абонента.

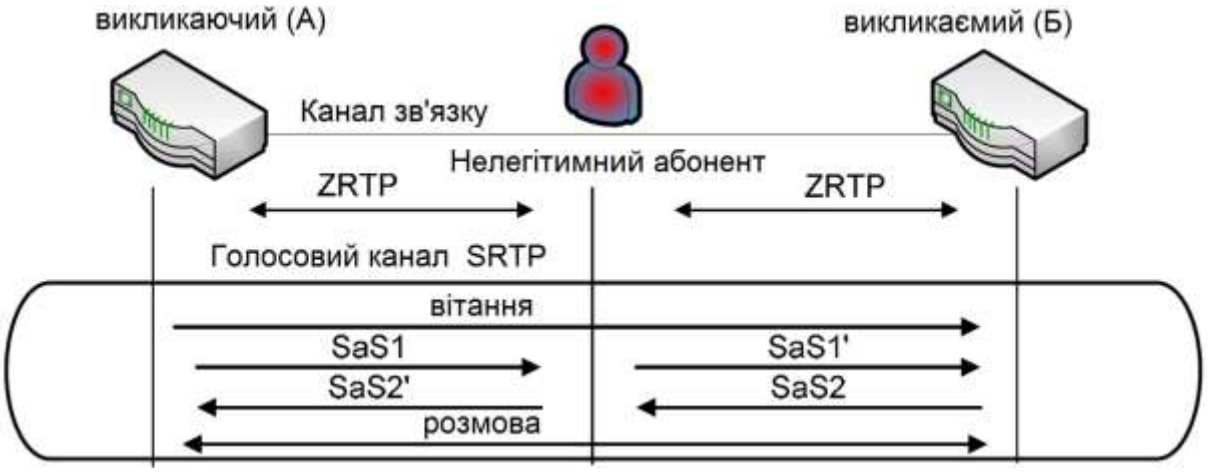


Рисунок 3.8 - Підміна аутентифікаційного рядка
в голосовому каналі зв'язку IP-телефонії

Інформація про IP-адреса яка необхідна для організації захищеного каналу сесії може бути отримана абонентами наступним чином: по телефону, при особистій зустрічі, по електронній пошті, та іншими доступними засобами зв’язку. Інформація про IP- адреса не є секретною для нелегітимного абонента і таким може бути передана по відкритих каналах зв'язку, на відміну від IP-адресів, загальна секретна інформація для алгоритмів симетричного шифрування є

закритою і доступ до неї призведе для нелегітимного абонента дешифрування потоку даних IP - телефонії. При перехопленні нелегітимним абонентом секретного симетричного ключа шифрування - нелегітимний абонент може відправляти дані легітимному абоненту, як і легітимний абонент. В даному випадку для підвищення захищеності даних як додатковий параметр можна використати IP-адреси для підвищення безпеки IP-телефонії, а також можливість отримання потоків даних, які були відправлені по декількох каналах зв'язку, легітимними абонентами при відсутності в даному випадку активної атаки нелегітимним абонентом типу «зустріч по середині» в декількох каналах зв'язку. Даний підхід для підвищення безпеки IP-телефонії протоколом ZRTP вимагає передачі повідомлення від учасників сеансу по іншому каналу зв'язку. Перевагою даного підходу є невисока складність розробки та реалізації програмними засобами IP – протоколу. Аутентифікаційний рядок передається в спеціалізоване програмне забезпечення по результату виконання IP - протоколу ZRTP. В даному випадку достатньо передати аутентифікаційний рядок абоненту по додатковому каналу зв'язку для виконання програмної автоматичної перевірки. Недоліком запропонованого підходу підвищення безпеки потоку даних у вигляді програмної автоматизованої перевірки ідентифікаційного рядка є те що виявлення нелегітимного абонента в каналі зв'язку можливе тільки після успішного завершення роботи протоколу, а не під час його виконання.

Для підвищення безпеки IP - телефонії необхідно оцінити можливості застосування двох і більше каналів зв'язку, для вирішення даної задачі необхідно: в першу чергу оцінити ймовірність наявності в маршруті загальної точки декількох каналах зв'язку при цьому необхідно розглянути варіанти використання різних операторів зв'язку між абонентами сесії; розробити алгоритм прийняття рішення про наявність в мережі нелегітимного абонента і оцінити ймовірності правильності прийняття можливих рішень. Для вирішення поставлених задач використаємо наступний алгоритм програмної автоматичної перевірки

аутентифікаційного рядка та виявлення активного нелегітимного абонента, який працює в одному з двох каналів зв'язку.

Алгоритм 3.1 Виявлення активного нелегітимного абонента, який працює в одному з двох каналів зв'язку

1. Учасники сесії А і В виконують обмін інформацією про IP-адреси: $IP_{A1}, IP_{A2}, IP_{B1}, IP_{B2}$, а також налаштовують відповідним чином таблицю маршрутизації.

2. Для організації захищеного з'єднання IP-телефонії, учасники сесії абоненти *A* і *B*, виконують IP-протокол ZRTP використовуючи при цьому канал зв'язку $IP_{A1} - IP_{B1}$, результатом роботи протокола ZRTP є отримання аутентифікаційного рядка (рис. 3.9).

3. Абонент *A* відправляє свій аутентифікаційний рядок SAS_A по каналу зв'язку $IP_{A2} - IP_{B2}$ абоненту *B*. Абонент *B* отримує аутентифікаційний рядок SAS_A'.

4. Абонент *B* відправляє свій аутентифікаційний рядок SAS_B по каналу зв'язку $IP_{A2} - IP_{B2}$ абоненту *A*. Абонент *A* отримує SAS_B '.

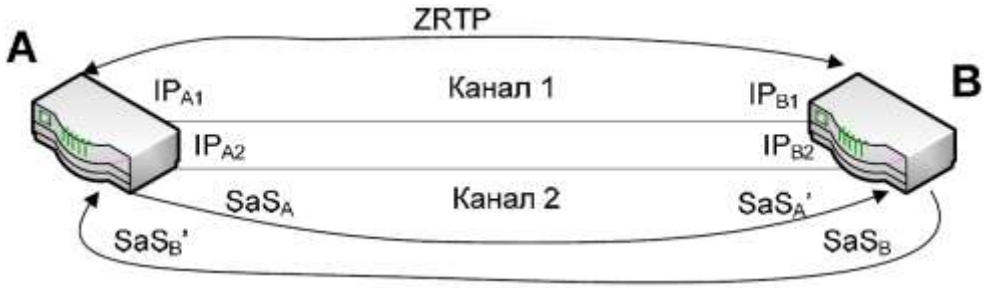


Рисунок 3.9 - Механізм програмної перевірки аутентифікаційного рядка

5. Абонент *B* виконує перевірку аутентифікаційних рядків SAS_A і SAS_B.

6. Якщо аутентифікаційні рядки співпадають то можна зробити наступний висновок що в мережі відсутній активний нелегітимний абонент в каналах зв'язку, або також що вірогідно присутній активний нелегітимний абонент одночасно в каналах зв'язку.

7. Якщо значення аутентифікаційних рядків не співпадають, абонент *B* отримує повідомлення від VoIP-монітора IP- телефонії про наявність нелегітимного абонента в каналі зв'язку.

8. Абонент *A* виконує перевірку на співпадання аутентифікаційних рядків SAS_A і SAS_B'. Якщо вони співпадають то можна зробити наступний висновок що в мережі відсутній активний нелегітимний абонент в каналах зв'язку, або також що вірогідно присутній активний нелегітимний абонент одночасно в каналах зв'язку.

9. Якщо значення аутентифікаційних рядків не співпадають, абонент *A* отримує повідомлення від VoIP-монітора IP- телефонії про наявність нелегітимного абонента в каналі зв'язку. Таким чином використання даного протоколу надасть нам інформацію про наявність активного нелегітимного абонента, який в стані провести активну атаку в одному з двох каналів зв'язку.

На основі приведеного алгоритму виконується обчислення ймовірністей: $P_{УА\_ЗС}$ - ймовірність успішної активної атаки нелегітимним абонентом типу «зустріч по середині»; $P_{ВА\_ЗС}$-ймовірність виявлення активної атаки нелегітимним абонентом типу «зустріч по середині»; $P_{У\_СК}$- ймовірність успішного розподілу та генерації загального секретного ключа.

Якщо нелегітимний абонент реалізував активну атаку типу «зустріч по середині» атака називається успішною, виконавши обмін загальною секретною інформацією між абонентами при використанні в даному випадку декілька каналів зв'язку, при цьому не виявивши себе при проведенні активної атаки. Така ситуація можливо в тому випадку, якщо один і той же нелегітимний абонент може контролювати потоки даних використовуваних каналів зв'язку і при цьому виконувати синхронну модифікацію потоків даних в кожному з каналів зв'язку.

Імовірність виконання успішної атаки типу «зустріч по середині» для протоколу з програмною перевіркою аутентифікаційного рядка відповідає ймовірності події, що нелегітимний абонент зможе одночасно прослуховувати і виконувати синхронну модифікацію потоків даних в кожному з каналів зв'язку.

Виявлення нелегітимного абонента дозволяє абонентам визначити, що існує вірогідність генерації компрометуючого секретного ключа, який дозволить нелегітимному абоненту дешифрувати і прослуховувати передану по каналам зв’язку інформацію, а також виконувати синхронну модифікацію потоків даних в кожному з каналів зв'язку. IP - протокол з програмною перевіркою аутентифікаційного рядка IP- телефонії не надає можливості визначити, на який саме канал зв'язку нелегітимний абонент буде виконувати активну атак. Також виявлення нелегітимного абонента в каналі зв'язку можливе тільки після успішного повного завершення роботи протоколу, нелегітимний абонент не може бути виявленим протягом роботи протоколу. Таким чином виникає необхідність розгляду додаткових варіантів модифікації IP - протоколу IP – телефонії ZRTP, із врахуванням наведених недоліків.

3.4 Висновки

Запропоновано метод підвищення захищеності IP – телефонії та безпеки програмного розподілу загальної секретної інформації, що відрізняється від існуючого методу виявлення нелегітимного абонента, впровадженням автоматизованої програмно-апаратної перевірки аутентифікаційного рядка. При використанні в даному випадку декілька каналів зв'язку, відповідна перевірка надасть можливість виявити нелегітимного абонента.

IP - протокол з програмною перевіркою аутентифікаційного рядка IP-телефонії не надає можливості визначити, на який саме канал зв'язку нелегітимний абонент буде виконувати активну атак. Також виявлення нелегітимного абонента в каналі зв'язку можливе тільки після успішного повного завершення роботи протоколу, нелегітимний абонент не може бути виявленим протягом роботи протоколу. Таким чином виникає необхідність розгляду додаткових варіантів модифікації IP - протоколу IP – телефонії ZRTP, із врахуванням наведених недоліків.

4 ДОСЛІДЖЕННЯ ЙМОВІРНІСНО-ЧАСОВИХ ХАРАКТЕРИСТИК ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ БЕЗПЕЧНОЇ IP-ТЕЛЕФОНІЇ

4.1 Метод підвищення ефективності протоколу розподілення ключів на основі алгоритму Діффі – Хелмана

При побудові повної мережі з використанням існуючих автономних систем не можливо вказати точний маршрут, по якому інформаційні пакети будуть передаватися між абонентами сесії, які підключені до автономних систем. Маршрутизація IP - пакетів в Інтернет мережі будь-якого оператора зв'язку залежить від завантаження каналів зв'язку, аварій що виникають на обладнанні використовуваного в мережі, а також від діючих додаткових наданих угод між операторами IP - телефонії, що визначають цінову політику і параметри наданих послуг.

Для забезпечення підвищення надійності та безпеки Інтернет мереж IP - телефонії пакетів пропонується для вирішення поставленої задачі застосовувати метод виявлення нелегітимного абонента IP - протоколів розподілу загальної секретної інформації, заснованих на алгоритмі обміну ключами Діффі-Хелмана, алгоритм дозволяє розподіл загальної секретної інформації з використанням одночасно декількох каналів зв'язку (рис. 4.1) і при цьому виявляти активного нелегітимного абонента.

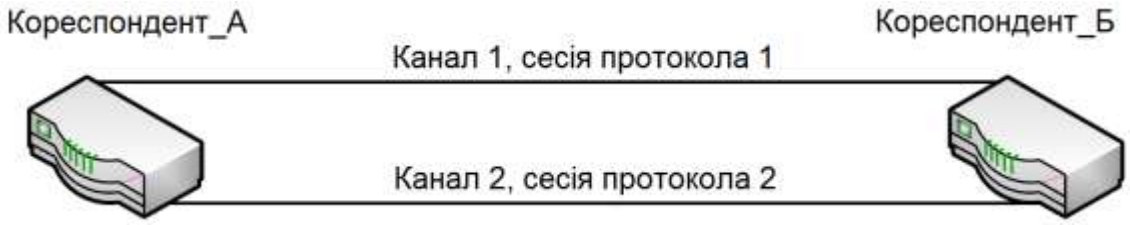


Рисунок 4.1 - Використання каналів зв'язку для обміну ключами

Наявність двох і більше каналів у одного абонента на сьогодні досить поширене явище. Наприклад якщо учасники сесії, які мають кожен в своєму розпорядженні два і більше підключень до мережі Інтернет і кожне підключення

абонентів виконується в Інтернет мережі через різних операторів зв'язку. Учасники зв’язку IP – телефонії мають IP-адресу в використовуваних каналах зв'язку Інтернет мережі. Учасники зв’язку IP – телефонії обмінюються своїми IP-адресами, які в подальшому будуть використовуватися в процесі встановлення зв'язку між абонентами. Інформація яка необхідна для організації захищеного каналу сесії може бути отримана абонентами наступним чином: по телефону, при особистій зустрічі, по електронній пошті, та іншими доступними засобами зв’язку.

Для успішної реалізації роботи IP - протоколу ZRTP за декількаами каналами зв'язку необхідно виконати інтеграцію багатоканального IP - протоколу з протоколами Інтернет мережі SIP / RTP для вирішення програмно-апаратних та технічних задач мати можливість визначення IP-адрес додаткових каналів, а також UDP/TCP портів для успішного виконання другого сценарію IP – протоколу Інтернет мережі, а також передачу відповідних параметрів в протокол IP – телефонії, клас IP – протоколу Інтернет мережі а також функцію IP – протоколу Інтернет мережі; таким чином реалізація перевірки роботи алгоритму обміну ключами Діффі-Хелмана по декільком каналах зв'язку і в залежності від результатів отриманих під час перевірки, продовжити виконання відповідних подальших дій; виконати інтеграцію з протоколами Інтернет мережі SIP / RTP.

Для реалізації двоканального підходу для підвищення безпеки потоку даних по каналам зв'язку IP – телефонії з використанням асиметричного алгоритму обміну ключами Діффі-Хелмана будемо передавати відповідно до протоколу однакові повідомлення. Абонент *A* відправляє по каналам зв'язку однакові повідомлення. Абонент *B* отримує повідомлення, відповідно до алгоритму проводить обчислення, перевіряє, чи отримані повідомлення співпадають. У випадку, якщо отримані повідомлення не співпадають - в одному з каналів виявлена присутність активного нелегітимного абонента, що виконує активну атаку типу «зустріч посередині». Абонент *B* відповідає абоненту *A* про наявність в одному з каналів активного нелегітимного абонента, відправляючи по каналах зв'язку повідомлення використовуючи алгоритм Діффі-Хелмана. Абонент *A*

отримує відповідне повідомлення і перевіряє їх на співпадання. У випадку, якщо отримані повідомлення співпадають – це означає відсутність активного нелегітимного абонента в каналах зв'язку, або , що також вірогідно що активний нелегітимний абонент один і той же присутній в обох каналах зв'язку. Взаємодія абонентів Інтернет мережі IP – телефонії при використанні модифікованого протоколу ZRTP представлена на рис. 4.2.

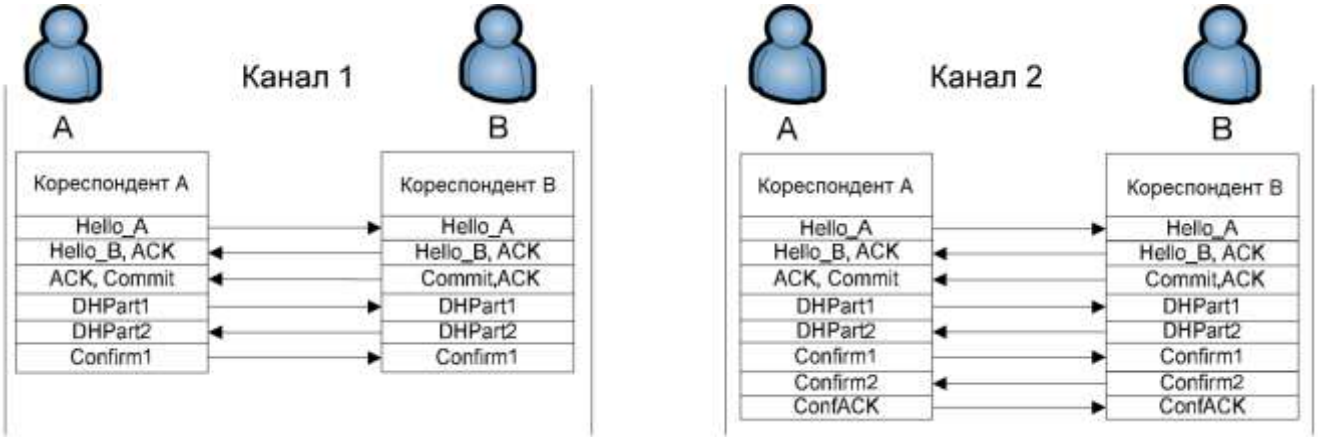


Рисунок 4.2 Взаємодія абонентів Інтернет мережі IP – телефонії при використанні модифікованого протоколу ZRTP

Розглянемо ймовірність $P_{НСДЦ_{ЗАХОБЛ\_2}}$, яка визначає що нелегітимний абонент може виконувати активну атаку типу «зустріч по середині» в одному з двох каналів зв'язку Інтернет мережі IP -телефонії пакетів. Дана ймовірність відповідає неуспішній можливості виконання атаки типу «зустріч по середині», так як дана активна атака виявляється використанням модифікованого протоколу ZRTP.

Виконується розрахунок ймовірностей подій: $P_{ВА\_ЗС}\, P_{УА\_ЗС}\, P_{У\_СК}$. Активна атака називається успішної, якщо що нелегітимний абонент реалізував активну атаку типу «зустріч по середині», при цьому попередньо виконавши обмін секретною інформацією з обома абонентами по двом каналах зв'язку Інтернет мережі IP - телефонії. Під час проведення успішної атаки нелегітимний абонент не виявляє себе. Це є можливим тільки в тому разі, коли нелегітимний абонент (один і то й же) може контролювати всі канали зв'язку, які використовують учасники сесії IP -

телефонії і при цьому нелегітимний абонент в стані виконувати синхронну модифікацію потоку даних між учасниками сесії IP -телефонії в кожному з каналів зв'язку. Імовірність виконання успішної активної атаки $P_{УА\_ЗС2}$ для IP - протоколу який використовує два канали відповідає ймовірності здійснення події, що нелегітимний абонент може одночасно прослуховувати і в той же час виконувати модифікацію повідомлень в двоканальному зв'язку одночасно $P_{УА\_НА2} = \left(P_{НСДЦ_{ЗАХОБЛ\_2}} \right)^2$.

Виявлення нелегітимного абонента дозволяє користувачам визначити, що може бути вироблений компрометувати ключ, що дозволяє дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію повідомлень. Ймовірність виявлення нелегітимного абонента залежить від числа використовуваних каналів зв'язку, а також від здатності алгоритму розподілу ключів визначити існування зловмисника в конкретному або конкретних каналах зв'язку з сукупності використовуваних. Ймовірність виявлення нелегітимного абонента $P_{В\_ЗАХОБЛ2}$ при використанні двоканального методу відповідає ймовірності знаходження нелегітимного абонента в одному каналі зв'язку при відсутності нелегітимного абонента в іншому каналі зв'язку IP - телефонії. Імовірність наявності нелегітимного абонента в першому каналі при відсутності нелегітимного абонента в іншому каналі зв'язку визначиться наступним чином: $P_{НА1К\_NO\_2К} = (1 - P_{НСВА}) P_{НСВА}$.

Імовірність наявності нелегітимного абонента в другому каналі зв'язку IP – телефонії при відсутності нелегітимного абонента в першому каналі зв'язку визначиться наступним чином:

$$P_{НА2К\_NO\_1К} = (1 - P_{НСВА}) P_{НСВА} = P_{НСВА} - P_{НСВА}{}^2.$$

$$P_{ВА2} = P_{НА1К\_NO\_2К} + P_{НА2К\_NO\_1К} = 2(1 - P_{НСВА}) P_{НСВА}$$

Під успішної подією генерації загального секретного ключа розуміється, що нелегітимного абонента не виявлено ні в одному каналі зв'язку і абонентами

генерації загального секретного ключа для шифрування потоку даних, які передаються по каналам зв’язку. Це можливо тільки в разі відсутності нелегітимного абонента в каналах зв'язку, або при використанні можливості алгоритму розподілу загальної секретної інформації визначати точне місцезнаходження нелегітимного абонента в конкретному (конкретних) каналах зв'язку. Імовірність успішної генерації секретного ключа $P_{УК2}$ для двоканального IP - протоколу відповідає імовірності відсутності нелегітимного абонента одночасно в обох каналах зв'язку. Імовірність відсутності нелегітимного абонента в одному каналі зв'язку P_{NO_HA}:

$$P_{NO\_HA} = 1 - P_{HCBA} \text{ тоді: } P_{УК2} = P_{NO\_HA}{}^2 = \left(1 - P_{HCBA}\right)^2.$$

Розглянемо варіант виявлення нелегітимного абонента з використанням трьох каналів зв'язку IP – телефонії передачі даних. Допустимо, що по трьох каналах зв'язку IP – телефонії передається однакова інформація обміну ключами Діффі-Хелмана. Приклад взаємодії абонентів при використанні модернізованого IP - протоколу ZRTP наведено на рис. 4.3. Ініціатор сеансу зв’язку відправляє по трьох каналах зв'язку IP – телефонії три однакових повідомлення. Інший абонент отримує повідомлення, проводить, при цьому необхідні обчислення, а також перевіряє, чи отримані повідомлення співпадають по трьох використовуваних каналах зв'язку. У випадку, неспівпадання повідомлень, активний нелегітимний абонент присутній в каналах зв'язку IP – телефонії, та виконує атаку типу «зустріч посередині» або активний нелегітимний абонент контролює одночасно всі три канали зв'язку IP – телефонії.

Абонент відповідає, відправляючи по відповідним трьом каналах зв'язку у відповідь інформацію отриману на основі IP - протоколу Діффі-Хелмана. Абонент сеансу отримує повідомлення і перевіряє на співпадання отримані повідомлення В даній ситуації розглянемо декілька варіантів роботи IP - протоколу при використанні методу виявлення нелегітимного абонента: якщо порівнюванні повідомлення однакові – це означає, або відсутній активний нелегітимний абонент

у всіх каналах зв'язку IP – телефонії, або існує активний нелегітимний абонент IP – телефонії у всіх трьох каналах зв'язку; якщо одне тільки повідомлення відрізняється від інших, в даній ситуації або присутній активний нелегітимний абонент в відповідному каналі зв'язку, або присутні два активних нелегітимних абоненти в двох інших каналах зв'язку IP – телефонії; у випадку якщо всі повідомлення різні, означає присутність двох окремо працюючих активних нелегітимних абонентів, які в даному випадку не мають між собою каналу зв'язку.

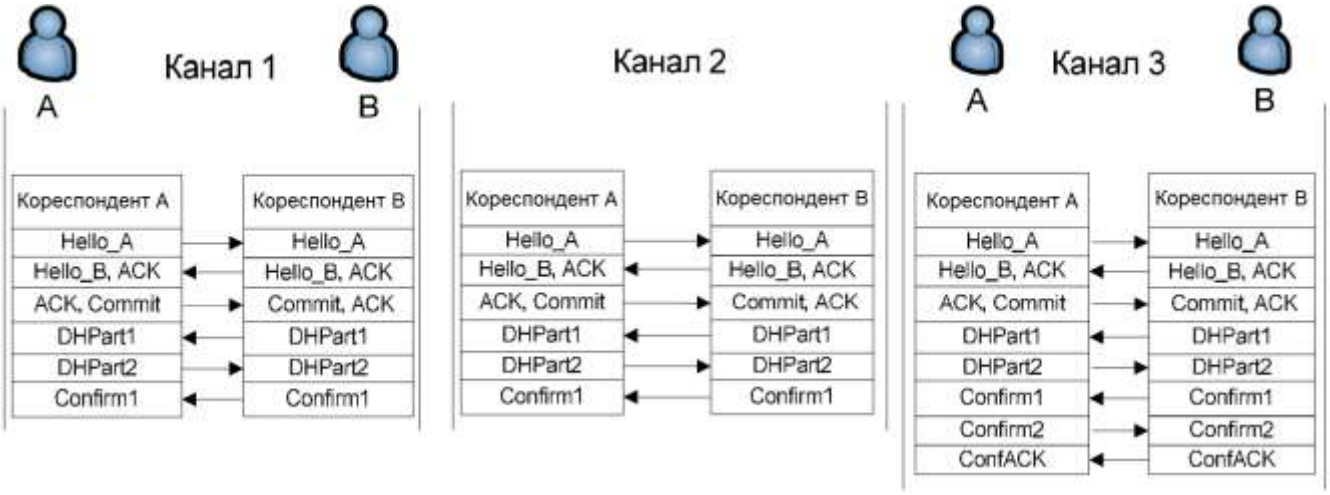


Рисунок 4.3 - Взаємодія кореспондентів при роботі одночасно по трьох каналах зв'язку.

Таким чином, IP -протокол дозволяє: при наявності одного нелегітимного абонента в одному з трьох каналів зв'язку IP – телефонії визначити канал з нелегітимним абонентом; при наявності нелегітимного абонента одночасно в двох каналах зв'язку IP – телефонії виявити наявність нелегітимного абонента, при цьому без визначення каналів зв'язку IP – телефонії, що містять нелегітимного абонента. Однак, IP - протокол не дозволяє при знаходженні нелегітимного абонента одночасно в трьох каналах зв'язку IP – телефонії визначити наявність нелегітимного абонента. Таким чином, відповідно, можна виділити два режими роботи методу підвищення безпеки IP - телефонії: ВНА: режим роботи з виявленням нелегітимного абонента (3-ВНА); ВКНА: режим роботи з виключенням нелегітимного абонента (3-ВКНА).

При роботі в режимі ВНА в разі виявлення неспівпадання хоча б одного з трьох повідомлень – IP - протокол завершується з помилкою, повідомляючи користувача про присутність нелегітимного абонента в каналі зв'язку IP - телефонії. У разі роботи в режимі ВКНА при виявленні неспівпадання одного з трьох переданих повідомлень - формується повідомлення про наявність нелегітимного абонента в конкретному каналі зв'язку, IP - телефонії при цьому протокол продовжує роботу і при цьому контролює повідомлення в тих каналах зв'язку IP - телефонії, де не виявлено нелегітимного абонента. Таким чином забезпечується виключення нелегітимного абонента. Імовірність виключення нелегітимного абонента $P_{ПрВНА}$ для трьох канального IP - протоколу відповідає події присутності нелегітимного абонента в одному з каналів зв'язку IP - телефонії при його відсутності, в даному сеансі зв’язку, в двох інших каналах $P_{ПрВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ} \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2$.

Однак, при наявності активного нелегітимного абонента одночасно в двох каналах зв'язку із трьох використовуваних каналів, а також, при цьому синхронної модифікації повідомлень в двох каналах зв'язку IP - телефонії нелегітимним абонентом, використовуваний механізм виключення може викликати некоректне визначення каналу з нелегітимним абонентом, що призведе, в даному випадку до помилкового вибору двох каналів зв’язку IP - телефонії, в яких присутній нелегітимний абонент, як надійних. Це дозволить нелегітимному абоненту успішно виконати обмін загальною секретною інформацією з абонентами сесії, здійснивши, при цьому успішну атаку типу «зустріч по середині». Імовірність помилкового виключення, в даному випадку відповідає ймовірності події, що нелегітимний абонент перебуває одночасно в двох каналах зв'язку IP - телефонії $P_{ПомВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ}^{\ 2} \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)$.

Ця ймовірність буде також складовою частиною ймовірності успішної атаки типу «зустріч посередині».

Виконаємо розрахунок ймовірностей для протоколу трьох канального обміну в режимі ВНА $P_{УА}$, $P_{ВА}$, $P_{УК}$.

Імовірність успішної атаки $P_{УАНА\_ВНА}$ Для тре канального протоколу в режимі ВНА відповідає ймовірності події, що нелегітимний абонент може прослуховувати і виконувати модифікацію повідомлень в трьох каналах зв'язку одночасно $P_{УАНА\_ВНА} = \left(P_{НСВ\_ЗАХОБЛ}\right)^3$.

Ймовірність виявлення нелегітимного абонента $P_{ВАНА\_ВНА}$ для трьох канального IP - протоколу Інтернет мережі в режимі ВНА відповідає ймовірності знаходження нелегітимного абонента в одному або двох каналах зв'язку при відсутності нелегітимного абонента в іншому каналі зв'язку. Імовірність присутності нелегітимного абонента в одному з каналів зв'язку IP – телефонії при відсутності нелегітимного абонента в двох інших каналах зв'язку:

$$P_{НА1К\_NO\_НА23К} = 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$$

Імовірність наявності нелегітимного абонента в двох з трьох каналів зв'язку при відсутності нелегітимного абонента в одному з каналів зв'язку:

$$P_{НА23К\_NO\_НА1К} = 3 \cdot \left(1 - P_{НСВА}\right) \cdot {P_{НСВА}}^2$$

$$P_{ВАНА\_ВНА} = P_{НА1К\_NO\_НА23К} + P_{НА23К\_NO\_НА1К} =$$

$$= 3 \cdot \left(1 - P_{НСВА}\right)^2 \cdot P_{НСВА} + 3 \cdot \left(1 - P_{НСВА}\right) \cdot {P_{НСВА}}^2$$

Імовірність успішної генерації загальної секретної інформації $P_{УКНА\_ВНА}$ для трьох канального IP - протоколу в режимі ВНА відповідає вірогідності відсутності нелегітимного абонента в трьох каналах зв'язку $P_{УКНА\_ВНА} = \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^3$.

Виконаємо розрахунок ймовірностей $P_{УА}$, $P_{ВА}$, $P_{УК}$ для протоколу трьох канального обміну в режимі ВКНА.

Імовірність успішної атаки $P_{УАНА\_ВКНА}$ для трьох канального протоколу відповідає ймовірності події, що нелегітимний абонент може прослуховувати і виконувати модифікацію повідомлень в двох або трьох каналах зв'язку одночасно.

$$P_{УАНА\_ВКНА} = P_{НСВ\_ЗАХОБЛ}{}^3 + 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right) \cdot P_{НСВЗАХОБЛ}{}^2$$

Ймовірність виявлення нелегітимного абонента $P_{ВАНА\_ВКНА}$ для трьох канального протоколу в режимі ВКНА відповідає ймовірності знаходження нелегітимного абонента в одному каналі зв'язку при відсутності нелегітимного абонента в двох інших каналах зв'язку і буде мати вигляд $P_{ВАНА\_ВКНА} = 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$.

Імовірність успішної генерації загальної секретної інформації $P_{УКНА\_ВКНА}$ для трьох канального IP - протоколу в режимі ВКНА відповідає вірогідності відсутності нелегітимного абонента в двох або трьох каналах зв'язку $P_{УКНА\_ВКНА} = \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^3 + 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$.

Для простого IP – протоколу обміну ключами Діффі-Хелмана, що працює по одному каналу зв’язку, наступні ймовірності матимуть вигляд $P_{У\_ЗАХОБЛ} = P_{НСВ\_ЗАХОБЛ}$, $P_{В\_ЗАХОБЛ1} = 0$, $P_{УК1} = 1 - P_{НСВ\_ЗАХОБЛ}$.

Модифікація IP - протоколу при роботі одночасно по декількох незалежних каналах зв’язку істотно зменшує ймовірність проведення успішної атаки «зустріч по середині». Ефективність захисту зростає зі збільшенням числа незалежних каналів зв’язку IP - телефонії. Модифікація в режимі виявлення нелегітимного абонента з використанням трьох каналів зв'язку, в даному випадку має найбільшу ймовірність виявлення нелегітимного абонента, а також, при цьому найменшу ймовірність успішної атаки нелегітимного абонента. Модифікація в режимі виключення нелегітимного абонента із застосуванням декількох (трьох) каналів має найбільшу ймовірність успішної генерації загальної секретної інформації між

учасниками зв’язку. Для реалізації вибирається одна з модифікацій в залежності від цілей і доступних ресурсів, виражених в числі доступних каналів зв'язку.

Результати проведених досліджень показують, що при підключенні абонентів одночасно до декількох операторів зв'язку IP – телефонії незалежні двійки маршрутів присутні завжди. Імовірність успішного формування загальної секретної інформації при використанні багатоканальної схеми з виявленням нелегітимного абонента при цьому зменшується незначно. У схемі з виключенням нелегітимного абонента ймовірність збільшується, але при використанні каналів зв’язку IP – телефонії великої протяжності можливо співпадання вузлів проходження маршрутів потоку даних, що, в даному випадку, може призвести до зниження ефективність роботи модифікованого IP - протоколу.

4.2 Метод оцінки ймовірнісно-часових характеристик протоколів IP-телефонії

Проведений аналіз IP - протоколів безпеки VoIP, показує, що IP - протоколи можна представити у вигляді і повідомлень і фаз, спрямованих для виконання кінцевої задачі IP - протоколу. Можливі два варіанти завершення роботи IP - протоколу - успішне завершення і неуспішне завершення. Успішним називається таке завершення IP -протоколу, при якому досягається мета ініціалізації протоколу. Наприклад - для протоколів розподілу ключів IP-телефонії успішним вважається завершення, якщо абоненти в результаті виконання протоколу отримали ключовий матеріал для роботи SRTP. Неуспішним називається завершення протоколу, при якому не досягається кінцева мета протоколу. Стосовно до ПРК IP-телефонії - неуспішним вважається завершення, якщо кореспонденти не погодили ключі для роботи SRTP.

Як правило, будь-який протокол можна розділити на логічні частини - фази. Фази різних протоколів можна описати з використанням примітивів. Слід зауважити, що для багатьох протоколів безпеки IP-телефоні передбачена повторна

передача повідомлень в тих випадках, коли повідомлення не вдалося доставити до респондента, або ніхто не почув у відповідь підтвердження прийому повідомлення. Дану особливість необхідно враховувати при оцінці ймовірнісно-часових характеристик .

При аналізі протоколів має сенс оцінювати такі ІЧХ, як середній час виконання IP – протоколу і ймовірність успішного завершення. Дані характеристики оцінюються за заданими початковими умовами, при яких виконується протокол.

Для аналізу ІЧХ покладаємося, що повідомлення протоколу передаються в дискретному каналі Інтернет мережі без пам'яті, параметром якого є швидкість *c*, ймовірність побутової помилки p_0, а також затримка *d*. Для кількісної оцінки ІЧХ характеристик протоколів пропонується використовувати метод ймовірних графів. Суть методу полягає в тому, що будь-який процес з кінцевим числом станів можна описати імовірнісним графом, гілки якого характеризуються утворюючими функціями (УФ), аргументом яких є p_{ij} - ймовірність переходу з *i*-ї в *j*-у вершину, а час *t* - параметром, визначальним процес.

Розглянемо простий процес передачі повідомлення від одного кореспондента до іншого. Нехай *n* - довжина пакета в бітах. тоді ймовірність успішної передачі пакету $p_{успішн}$, матиме вигляд: $p_{успішн} = (1 - p_0)^n$ Імовірність, що пакет з *n* біт переданий з помилкою, буде мати вигляд: $p_{втрата} = 1 - (1 - p_0)^n$.

Наведений процес описується імовірнісним графом, представленим на рис. 4.4, де f_1, f_2 - утворюючі функції гілок.

Утворююча функція для гілки 1-2 матиме вигляд $f_1(x) = (1 - p_0)^n \cdot x^{n/c+d}$, утворююча функція для гілки 1-3 матиме вигляд $f_2(x) = (1 - (1 - p_0))^n \cdot x^{n/c+d}$.

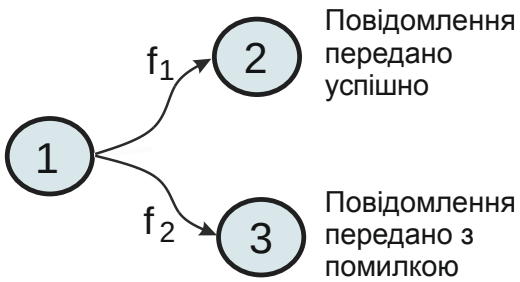


Рисунок 4.4 - Граф передачі повідомлення між кореспондентами

Утворююча функція застосовується для розрахунку $T_{середн}$ - середнього часу виконання протоколу: $T_{середн} = \dfrac{df_1(x)}{dx}(x=1)$

Утворююча функція також використовується для розрахунку ймовірності успішного завершення, яка визначається, як значення утворюючої функції в точці x = 1: $P = f_1(x=1)$.

Розглянемо алгоритм для таких примітивних протоколів, як "протокол з нескінченним повтором повідомлень необмежену кількість разів", "протокол з повтором повідомлень обмежене число раз", а також "протокол з повтором повідомлень обмежене число раз зі змінним часом затримки між повторами".

Розглянемо застосування алгоритму на примітивному протоколі з нескінченним повторам повідомлень необмежену кількість разів, завданням якого є передача одного повідомлення довжиною *n* від кореспондента до респондента, і виконання повторної відправки повідомлення в разі, якщо повідомлення доставлено не було.

Граф, що описує протокол при нескінченному числі передач одного повідомлення, наведено на рис. 4.5.

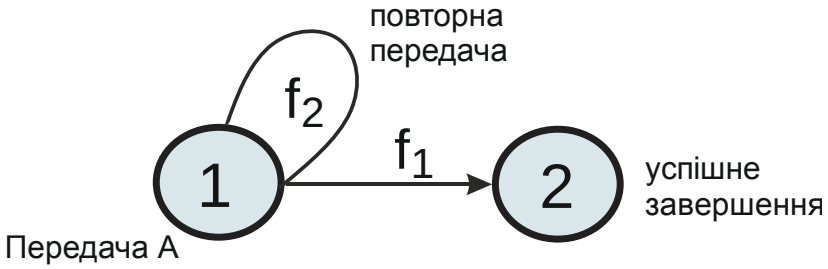


Рисунок 4.5 - Граф, що описує протокол при нескінченному числі повторів

Утворююча функція такого ймовірного графа в має вигляд: $f(x)=\sum_{i=1}^{v} p_i x^{t_i}$,

де, p_i - ймовірність переходу з першого стану в другий; t_i - час, необхідний для цього переходу; *v* - число повторних передач повідомлення.

Утворююча функція застосовується для розрахунку середнього часу виконання протоколу: $T_{середн}=\frac{df(x)}{dx}(x=1)$

Утворююча функція використовується для обчислення ймовірності успішного завершення, яка визначається, як значення утворюючої функції в точці x = 1: $P=f(x=1)$.

Так як досліджуваний протокол має два стани – початок передачі даних і завершення передачі даних, показаних на графі на рис. 4.5, то протокол завжди буде закінчуватися успішно.

Представлений протокол ускладняється введенням додаткового параметра - часу очікування перед повторним повідомленням. Тоді при розрахунку часу переходу від однієї вершини графа до іншої вершини графа необхідно враховувати час передачі повідомлення протоколу в каналі зв'язку, так і затримки, викликані очікуванням перед повторною передачею, які так само можуть залежати від ітерації. тоді: $f_1 = p_1 \cdot x^{a_1}$, $f_2 = p_2 \cdot x^{a_2}$,

де, p_1 - ймовірність успішного прийому повідомлення абонентом; a_1 - час передачі повідомлення, с; p_2 - ймовірність неуспішного прийому повідомлення абонентом; a_2 - час очікування перед повторним повідомленням, однакове для всіх повторів, с.

Утворююча функція графа матиме вигляд: $f_{12p}=\frac{f_1}{1-f_2}$.

Додатково вводиться ускладнення протоколу, виражене в обмеженні *k* числа повторів повідомлень, що призводять до успішного завершення передачі даних. В

цьому випадку, в протоколі з кінцевим числом повторних передач з'являється третій стан неуспішного завершення (рис. 4.6).

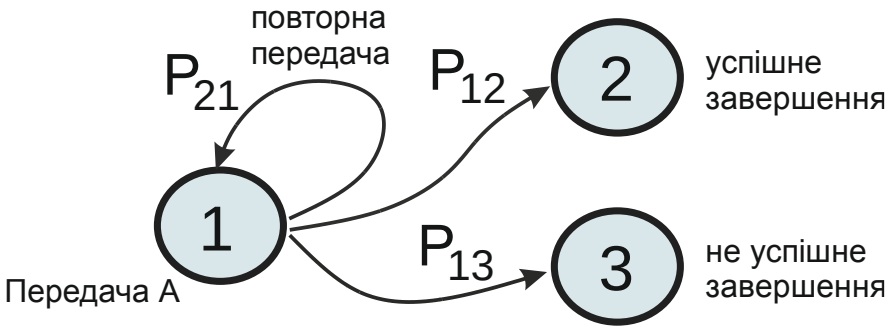


Рисунок 4.6 - Граф етапу першої фази при кінцевому числі повторів

Спрощення графа наведено на рис. 4.7. Утворююча функція f_{12k}, що враховує кінцеве число повторів, рівне *k*, і відповідна гілки успішного завершення матиме вигляд:

$$f_{12k}(x) = p_1 x^{a_1} + p_1 x^{a_1} \cdot p_2 x^{a_2} + \ldots + p_1 x^{a_1} \left(p_2 x^{a_2} \right)^k$$

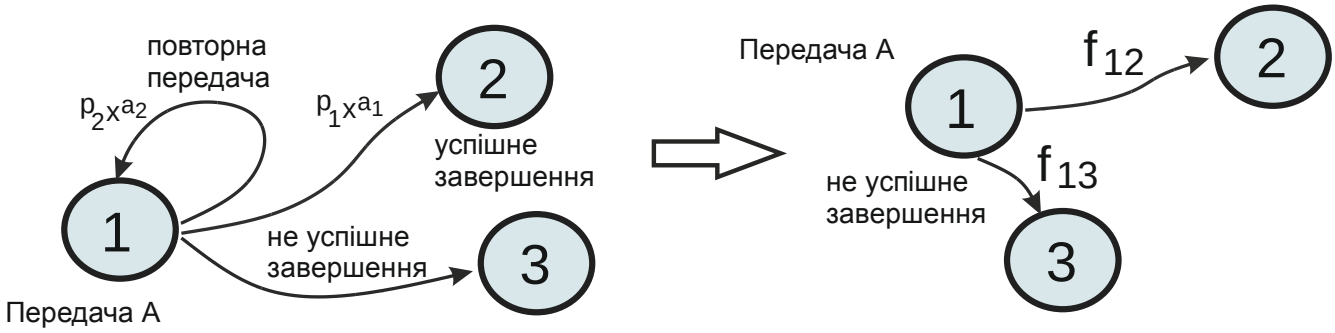


Рисунок 4.7 - Граф протоколу повторних повідомлень при кінцевому *k* повторів

У випадку з однаковим часом затримки повтору утворююча функція f_{12k}, відповідна успішному завершенню, буде мати вигляд: $f_{12k} = p_1 x^{a_1} \sum_{i=0}^{k} \left(p_2 x^{a_2} \right)^i$.

Утворююча функція f_{13k}, переходу з точки 1 в точку 3, відповідна гілки неуспішного завершення, має вигляд: $f_{13k} = p_1 x^{a_1} \dfrac{\left(p_2 x^{a_2} \right)^{k+1}}{1 - p_2 x^{a_2}} = \dfrac{f_2^{k+1} \cdot f_1}{(1 - f_2)}$.

Тоді середній час переходу з точки 1 в точку 2 $T_{середн} = \frac{df_{12k}}{dx}(x=1)$.

Введено допущення, що часи очікування при повторі повідомлення a_{2i} будуть різними. Ця особливість характерна для IP - протоколу з потворою повідомлень k раз зі змінним часом затримки між повторами. Тоді утворююча функція матиме вигляд: $f_{12k} = p_2 \frac{\left(x^{a_{22}}\right)^2}{x^{a_{21}}}$.

При різному часі послідовність не є геометричною прогресією і до неї не може бути застосована раніше наведена формула і утворююча функція f_{12k} гілки успішного завершення буде мати вигляд:

$$f_{12k} = p_1 x^{a_1}\left(1 + p_2 x^{a_{21}} + \left(p_2\right)^2 x^{a_{21}+a_{22}} + ... + \left(p_2\right)^2 x^{a_{21}+a_{22}+...+a_{2k}}\right)$$

Виконано оцінку протоколу з кінцевим k-числом повторних передач зі змінною затримкою a_{2i} між повторами передачі даних.

4.3 Висновки

Запропоновано метод виявлення активного нелегітимного абонента IP - протоколів розподілу загальної секретної інформації, заснованих на алгоритмі обміну ключів Діффі-Хелмана, особливість методу полягає у використанні декількох відкритих каналів зв'язку. Забезпечує зниження вірогідності проведення активним нелегітимним абонентом успішної атаки «зустріч по середині», а також присутність механізму визначення активного зловмисника в каналі зв'язку, при відсутності наперед розподіленої загальної секретної інформації. Метод накладає обмеження на використовувані канали зв'язку, в тому плані, що канали зв'язку повинні бути незалежні.

ВИСНОВКИ

У дипломній роботі вирішена задача підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії та скорочення часу встановлення захищеного з'єднання за рахунок покращення ІЧХ IP - протоколів, та отримані основні результати:

1. Математична модель активного нелегітимного абонента для захищеної IP-телефонії Інтернет мережі, надає можливість враховувати цього атаку нелегітимного абонента «зустріч по середині» на протокол розподілу секретної інформації, дозволяє обчислити ймовірність успішної атаки, отримання несанкціонованого доступу до закритої інформації, успішність завершення атаки залежить від значень ймовірностей проміжних атак .

2. Метод оцінки ІЧХ протоколів розподілу загальної секретної інформації захищеної IP-телефонії Інтернет мережі, враховує особливості IP-протоколів, а саме обмеження числа повторних передач потоку даних.

3. Представлена модифікація протоколу розподілу загальної секретної інформації ZRTP, дозволяє об'єднати потоки даних про підтримуваних криптографічних наборах і блоків протоколу Діффі - Хелмана.

4. Метод виявлення активного нелегітимного абонента протоколів розподілу загальної секретної інформації ключів, використовується при роботі за сценарієм типу клієнт-клієнт для кінцевих абонентів, які не мають наперед розподіленої секретної інформації. Метод забезпечує з високою ймовірністю встановити надійне захищене з'єднання між абонентами, а також виявити активного нелегітимного абонента в каналі зв'язку, що реалізує атаку «зустріч по середині» на протокол розподілу загальної секретної інформації ключів.

За темою роботи опубліковано 1 теза та 1 наукова стаття.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Баскаков И.В. IP-телефония в компьютерных сетях. / И.В. Баскаков, А.В. Пролетарский, Р.А. Федотов— М.: ИНТУИТ, 2010. — 183 с.

2. Бирюков А.А. Информационная безопасность защита и нападение. А.А. Бирюков – М.: ДМК Пресс, 2012. – 474 с.

3. Ботуз С.П. Интеллектуальные интерактивные системы и технологии управления удаленным доступом./ С.П. Ботуз – М.: Соломон-Прессс, 2014. –360 с.

4. Вишневский, В. В. Энциклопедия Wi-Max. Путь к 4G./ В. В. Вишневский, С.Л. Портной –М.: Техносфера, 2015. –471с.

5. Гольдштейн, Б.С. Сети связи пост-NGN /Б.С. Гольдштейн, А.Е. Кучерявый. –СПб.:БХВ-Петербург, 2014. –160с.: ил.

6. Гулечко М.С. Загрози інформаційної безпеки в IP-телефонії/ В.М. Джулій, М.С. Гулечко, Ю.В. Хмельницький, І.В. Толок / Тези доповідей XVII міжнародної наукової конференції студентів, аспірантів та молодих учених. / ред. кол. Д. Струнін (голова ВНТ ВІКНУ) – К., - 2020. –С.109

7. Гулечко М.С. Аналіз поточного стану дій в області захищеної IP- телефонії / М.С. Гулечко, В.М.Джулій, В.Ю. Тітова //Всеукраїнська науково – практична конференція молодих науковців і студентів «Інтелектуальний потенціал 2020», 9-10.11.2020, - ХНУ.- Частина 2. Комп‘ютерні системи та кібербезпека – 30с.

8. Дэвидсон Дж. Основы передачи голосовых данных по сетям IP. / Дж. Дэвидсон., М.Бхатия– М.: Вильямс, 2012. –400 с.

9. Ермаков А. Основы конфигурирования корпоративных сетей Cisco. А. Ермаков – М.: ФГБОУ "Учебно-методический центр по образованию на железнодорожном транспорте", 2013. — 457 с.

10. Жиляков Е. Г., Фирсова А. А. Об анализе и синтезе речевых сигналов в IP-телефонии / Е. Г. Жиляков, А. А. Фирсова // Вестник НТУ ХПИ . 2010. №43. С. 84

11. Кузьменко Н.Г. Компьютерные сети и сетевые технологии/ Н.Г. Кузьменко– М: Наука и техника, 2013. – 368 с.

12. Калинин М. ICND1 1.0 / ICND2 1.1 Использование сетевого оборудования Cisco. / М. Калинин - Части 1- 2. – М.: Центр обучения «Специалист» при МГТУ им. Баумана, 2013. – 1028 с.

13. Кутузов, О. И. Инфокоммуникационные сети. Моделирование и оценка вероятностно-временных характеристик [Текст] : монография / О. И. Кутузов, Т. М. Татарникова - СПб. : ГУАП, 2015. – 381 с.

14. Кутузов, О. И. Моделирование систем и сетей телекоммуникаций: учеб. пособие/О. И. Кутузов, Т. М. Татарникова. СПб.: РГГМУ, 2012–572с.

15. Левин М. Библия хакера 2. Книга 1 / М. Левин. – М.: Майор, 2013.–638 с.

16. Лекции по теории графов: учебное пособие для студентов / В.А. Емеличев, О.И. Мельников, В.И. Сарванов, Р.И. Тышкевич.–3-е изд.–М.: УРСС: Либроком, 2013. – 382 с.

17. Макарова О. С. Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «Хакера» // О. С. Макарова - Доклады ТУСУР. 2012. №1-2 (25).

18. Мартин, Роберт Быстрая разработка программ. Принципы, примеры, практика. /Роберт Мартин, Джеймс Ньюкирк — Изд-во: Диалектика-Вильямс, 2004. — 752 с.

19. Матвеев М. Д. Администрирование Windows 10 / М. Д. Матвеев, Р. Г. Пронди и др. – Санкт-Петербург: Наука и техника, 2013. – 396 с.

20. Мишин Н. Школа сисадмина. Курс лекций "Сети" Н.Мишин - М.: Вильямс, 2015. — 728 с.

21. Молочков В.П. Компьютерные сети / Молочков В.П. – М.: ИНТУИТ, 2013. — 982 с.

22. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы /В. Г. Олифер, Н. А.Олифер - СПб.: Питер, 2017. - 992 с.

23. Партыка Т. Л. Информационная безопасность учебное пособие / Т. Л. Партыка, И. И. Попов. – М.: ФОРУМ, 2011. – 432 с.

24. Привалов А. А. Модель процесса вскрытия параметров сети передачи данных оператора IP-телефонной сети компьютерной разведкой организованного нарушителя / А.А. Привалов, Н.В. Евглевская, К.Н. Зубков // Известия Петербургского университета путей сообщения. 2014. №2 (39).

25. Проскурин В. Г. Защита программ и данных: учебное пособие / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М.: Академия, 2017. – 198 с.

26. Рашид А. Построение защищенных корпоративных сетей./ А.Рашид – М.: ДМК - Пресс, 2013. – 250 с.

27. Романец Ю. В. Защита информации в компьютерных системах и сетях. / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 20011.–366 с.

28. Салмре, Иво Конечный автомат для пользовательского интерфейса. Программирование мобильных устройств на платформе .NET Compact Framework. / Иво Салмре – Изд-во: Издательский дом "Вильямс", 2016. – 736с.

29. Сердюк В. А. Организация и технологии защиты информации / В. А. Сердюк. – М.: Издательский дом Государственного университета – Высшей школы экономики, 2011. – 571 с.

30. Соболь Б.В., Сети и телекоммуникации. /Б. В. Соболь, Г.А. Манин, Е.Д. Герасименко - Учебное пособие. - М.: Феникс, 2015. — 191 с.

31. Суворов А.Б. Основы технологий массовых телекоммуникаций. / А.Б. Суворов— М.: Феникс, 2014. — 509 с.

32. Тарасюк М. В. Защищенные информационные технологии / М. В. Тарасюк. – М.: Солон-пресс, 2004. – 191 с.

33. Татт У. Теория графов / У. Татт, пер. с англ. Г. П. Гаврилова. – М. Мир, 2008. – 424 с.

34. Теоретические основы компьютерной безопасности / П.Н.Девянин, О.О. Михальский, Д. И. Правиков, А. Ю. Щербаков. –М.: Радио и связь, 2000.–192 с.

35. Трубачев А. П. Оценка безопасности информационных технологий / А. П. Трубачев и др. под. общ. ред. Галатенко В. А. – М.: СИП РИА, 2001. – 356 с.

36. Харари Ф. Теория графов / Фрэнк Херари; пер. с англ. И предисл. В.П, Козырева; под. ред. Г.П. Гаврилова. – 3-е изд., стер. – М.: УРСС, 2016. – 290 с.

ДОДАТОК А
(обовязковий)
Код (лістинг) програмного забезпечення обміну ключами Діффі-Хелмана

```
public static void createKey()throws Exception
{
    KeyPairGenerator kpg = KeyPairGenerator.getInstance("DiffieHellman");
    kpg.initialize(512);
    KeyPair kp = kpg.generateKeyPair();
    KeyFactory kfactory = KeyFactory.getInstance("DiffieHellman");

    DHPublicKeySpec kspec = (DHPublicKeySpec) kfactory.getKeySpec(kp.getPublic(),
DHPublicKeySpec.class);
}

public static void createSpecificKey(BigInteger p,BigInteger g)throws Exception
{
    KeyPairGenerator kpg = KeyPairGenerator.getInstance("DiffieHellman");
    DHParameterSpec param = new DHParameterSpec(p,g);
    kpg.initialize(param);

    KeyPair kp = kpg.generateKeyPair();

    KeyFactory kfactory = KeyFactory.getInstance("DiffieHellman");

    DHPublicKeySpec kspec = (DHPublicKeySpec) kfactory.getKeySpec(kp.getPublic(),
DHPublicKeySpec.class);
}

static boolean isPrime(long n)
{
    if (n%2 == 0)
    {
        return false;
    }

    for(int i = 3 ; i*i<=n;i+=2)
    {
        if(n%i==0)
            return false;
    }
    return true;
}

public static void main(String [] args) throws Exception
{

    Random randomGenerator = new Random();

    long pValue = randomGenerator.nextInt(1000000);
    long gValue = randomGenerator.nextInt(100000);
    long correctPValue;

    boolean checkPrime = isPrime(pValue);
    System.out.println("the number generated is "+pValue);
    System.out.println(checkPrime);

    while(checkPrime == false)
```

```
{
    long pValue2 = randomGenerator.nextInt(1000000);
    boolean checkPrimeInLoop = isPrime(pValue2);
    //System.out.println("value in loop is "+pValue2);
    if(checkPrimeInLoop == true)
    {
        pValue=pValue2;
        break;
    }
}


long checkSP = (pValue*2)+1;
boolean checkSafePrime = isPrime(checkSP);
//System.out.println(checkSafePrime);
while(checkSafePrime==false)
{
    long pValue3=randomGenerator.nextInt(1000000);
    boolean checkPrimeInLoop = isPrime(pValue3);
    long pValue5=(pValue3*2)+1;
    //boolean checkSafePrimeInLoop = isPrime(pValue4);
    boolean checkSafePrime2InLoop = isPrime(pValue5);

    if(checkSafePrime2InLoop == true && checkPrimeInLoop == true)
    {
        pValue=pValue3;
        break;
    }

}

System.out.println("the safe prime is"+pValue);//safe prime

while(gValue>pValue)
{
    long gValue2=randomGenerator.nextInt(100000);

    if(gValue2<pValue)
    {
        gValue=gValue2;
        break;
    }
}

long getDivisor = (pValue-1)/2;
BigInteger bi1,bi2,bi3,bi4;

bi1=BigInteger.valueOf(getDivisor);

bi2 = BigInteger.valueOf(pValue);

bi3 = BigInteger.valueOf(gValue);

bi4= bi3.modPow(bi1,bi2);

long calculatedValue = bi4.longValue();


while(calculatedValue == 1)
{
    long gValue3=randomGenerator.nextInt(100000);
```

```
            long getDivisorInLoop = (pValue-1)/2;
            BigInteger bi5,bi6,bi7,bi8;

            bi5=BigInteger.valueOf(getDivisorInLoop);

            bi6 = BigInteger.valueOf(pValue);

            bi7 = BigInteger.valueOf(gValue3);

            bi8= bi7.modPow(bi5,bi6);

            long calculatedValueInLoop = bi8.longValue();
            System.out.println(calculatedValueInLoop);
            if(calculatedValueInLoop!=1)
            {
                gValue=gValue3;
                break;
            }
        }

        BigInteger generatorValue,primeValue;

        generatorValue = BigInteger.valueOf(gValue);
        primeValue = BigInteger.valueOf(pValue);

        createKey();

        int bitLength=512;

        createSpecificKey(generatorValue,primeValue);

    }
```

ДОДАТОК Б
(обовязковий)
Перелік наукових праць

к.т.н., доц. Джулій В.М. (ХмНУ)
к.пед.н., доц. Толок І.В. (ВІКНУ)
к.т.н., доц. Хмельницький Ю.В. (ХмНУ)
Гулечко М.С. (ХмНУ)

Забезпечення інформаційної безпеки IP-телефонії

Сучасному періоду розвитку телекомунікацій відповідають зростаючі обсяги трафіку в корпоративних мережах, зокрема, в мережах Інтернет провайдерів. Причинами поширення IP-телефонії послужили низька вартість в порівнянні з аналоговою телефонією, викликана застосуванням недорогих мереж з комутацією пакетів, а також універсальність і мобільність, що дозволяє перетворити мову в потік даних в будь-якій точці мережевої інфраструктури.

Розвиток нових протоколів, а також передача голосових пакетів у відкритому вигляді через публічні мережі привели до появи і стандартизації протоколів забезпечення безпеки IP-телефонії. Стандартизація протоколів, а також поширене використання персональних комп'ютерів в якості терміналів користувача для послуг IP-телефонії привели до розробки великого числа програм для IP-телефонії, в тому числі програмного забезпечення з відкритим вихідним кодом, що дозволяє розширювати можливості і використовувати додаткові алгоритми в програмах.

При оцінці впливу протоколів забезпечення безпеки на якість потрібно враховувати особливості IP-телефонії в порівнянні з традиційною телефонією. Так, в традиційній телефонії час відгуку вузла зв'язку, тобто час з початку передачі інформації про заняття абонентської лінії до моменту отримання кінцевим обладнанням сигналу готовності до прийому номера, визначається готовністю станції обслужити виклик. У IP-телефонії цей час визначається кінцевим обладнанням і не залежить від поточного стану телефонної станції. Однак, параметр "час встановлення з'єднання" для IP-телефонії включає в себе час відгуку вузла IP-телефонної станції, а також час, необхідний для взаємодії між кореспондентами, або кореспондентом і телефонною станцією. Відлік цього часу починається після закінчення набору номера користувачем і

закінчується отриманням сигналу очікування відповіді або зайнятості від респондента.

Необхідно оцінити, як протоколи безпеки IP-телефонії можуть впливати на нормовані показники функціонування мереж телефонної мережі зв'язку. Застосування SIP-S може впливати на норму "втрати викликів" в разі, якщо при сценарії абонент-абонент один з кореспондентів використовує політику безумовного використання SIP-S, а другий не підтримує SIP-S протокол. Деяка затримка додатково може виникати за рахунок часу, необхідного на організацію TLS каналу між кореспондентами, необхідного для роботи SIP-S протоколу.

Список використаних джерел:

1. Борисов М. А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев – М.: УРСС: Либроком, 2013. – 370 с.

Аналіз поточного стану дій в області захищеної IP- телефонії

Гулечко М.С., Джулій В.М., Тітова В.Ю.
Хмельницький національний університет

Протоколи IP-телефонії поділяються на дві великі групи, а саме протоколи передачі медіа інформації по пакетним мережам, а також протоколи управління встановленням з'єднання. В першу групу входить протокол RTP (Real-time Transport Protocol), що працює поверх UDP (User Datagram Protocol) протоколу. Сукупність протоколів RTP / UDP / IP забезпечує транспортний механізм для мовного трафіку. Протоколи другої групи забезпечують управління при обслуговуванні виклику між абонентами. До цієї групи належать протоколи SIP (Session Initiation Protocol), H.323, MGCP (Media Gateway Control Protocol). Протоколи встановлення з'єднання можуть працювати як поверх UDP транспорту, так і по TCP (Transmission Control Protocol). Таким чином, сукупність протоколів (SIP / H.323 / MGCP) / (UDP / TCP) / IP формують сигнальний механізм для передачі мовного і медіа трафіку.

В силу загальнодоступності використовуваних каналів передачі голосової інформації в IP мережах особливої актуальності набуває забезпечення конфіденційності VoIP-сервісів. Для вирішення цього завдання можуть бути використані різні підходи: забезпечення прямого захищеного каналу між кореспондентами (наприклад, VPN-тунель); застосування спеціальних протоколів забезпечення безпеки для IP-сервісів.

Перший спосіб набув широкого поширення при побудові віртуальних корпоративних мереж, але для його реалізації кореспонденти повинні підтримувати VPN-протокол. Однак, багато VoIP-пристрої не підтримують VPN. Тому, для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії.

До спеціальних протоколів забезпечення безпеки IP-телефонії відносяться протоколи Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Ці протоколи можна розділити на 3 категорії: протоколи захисту сигналізації (Secured SIP); протоколи захисту медіаінформації (SRTP); протоколи генерації і розподілу ключів для протоколів захисту медіаінформації (MIKEY, SDES, ZRTP, DTLS).

Протоколи захисту сигналізації призначені для забезпечення безпеки інформації про телефонні номери, підтримуваних кодеків. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP / TLS). Цей протокол працює за аналогією з протоколом HTTPS, організовуючи між кореспондентом і сервером SSL тунель з використанням сертифікатів і відкритого ключа. Всі SIP-повідомлення (сигналізація) передаються з цього тунелю. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовується для організації TLS.

Для забезпечення конфіденційності при передачі мови широко використовується захищений протокол реального часу - Secure Real-time Transport Protocol (SRTP), який реалізує функції криптографічного захисту - шифрування і аутентифікації мовних повідомлень на основі алгоритму шифрування AES.

Криптографічний захист пакетів голосової інформації виконується протоколом SRTP в режимі реального часу і не вносить змін в ймовірносно-часові характеристики протоколу RTP. Але для його роботи необхідно попереднє формування криптографічних ключів. Це завдання вирішує протокол розподілу ключів (ПРК).

Рекомендація RFC 3711 описує дві складових - власне протокол SRTP для перенесення і криптозахисту медіа даних, а також протокол SRTCP (Secure Real-time Transport Control Protocol) для управління медіа сесією.

Основними завданнями протоколу SRTP є виконання таких функцій: шифрування переданих голосових даних; аутентифікація переданих повідомлень; захист від передачі повторних пакетів; збереження смуги пропускання, стиснення RTP заголовків.

Основними завданнями протоколу SRTCP є виконання таких функцій: шифрування переданих даних; аутентифікація переданих повідомлень. Аутентифікація і шифрування можуть працювати незалежно один від одного. Таким чином, можливий варіант, коли шифрування вимкнено і SRTP здійснюється виключно з метою аутентифікації. Обмеженням протоколу є те, що аутентифікація повідомлення обов'язкова в SRTP і не може бути відключена.

Протоколи генерації і розподілу ключів для захисту медіаінформації.

Протоколи третьої групи, за аналогією з протоколами розподілу ключів в бездротових мережах, призначені для генерації і розподілу між кореспондентами ключів шифрування медіаінформації. Для вирішення цього завдання можна використовувати протоколи MIKEY, SDES, ZRTP, DTLS.

Протокол обміну ключами MIKEY описаний в рекомендаціях RFC3830 і RFC6309. MIKEY має кілька режимів роботи, що визначають спосіб формування секретного ключа сесії SRTP: режим встановленого ключа, режим відкритого ключа та режим Діффі-Хелмана. Причому другий і третій режими не захищають від атаки вторгнення в середину (MiTM, Man In the Middle) і вимагають реалізації механізму аутентифікації повідомлень. Транспортом для переносу повідомлень протоколу може виступати як SIP / SDP, так і протокол RTSP (Real Time Streaming Protocol). SDES (Session Description Protocol Security) описується в RFC4568. Суть протоколу полягає в тому, що один з кореспондентів передає ключ в SIP повідомленні по сигнальному каналу. Кореспондент отримує його і використовує для шифрування. Однак при цьому обмін сигнальними повідомленнями повинен бути захищений від зловмисника. З цієї причини - SDES може

використовуватися тільки при наявності SIP / TLS захищеного з'єднання з цифровим сертифікатом сервера. Також даний спосіб не забезпечує безпеки з кінця в кінець. Це означає, що якщо з'єднання буде виконуватися через IP АТС, SDES буде виконувати розподіл ключів між кореспондентом А і IP PBX, між кореспондентом Б і IP-телефонною станцією, але не між кореспондентами А і Б безпосередньо.

Протокол DTLS для SRTP описується в RFC 5764. Протокол описує формування медіа-сесій точка-точка з двома учасниками з жорстким фіксуванням портів UDP кореспондента і респондента. Повідомлення протоколу передаються спільно з RTP пакетами. Кожна сесія містить одну DTLS асоціацію і два SRTP контексту (для SRTP і SRTCP). Для організації сесії (DTLS-асоціації) кореспонденти виконують обмін повідомленнями, DTLS handshake. Так як в основі протоколу лежить TLS, що використовує інфраструктуру відкритих ключів (Public Key Infrastructure, PKI), то застосування TLS можливо теж тільки при наявності PKI.

Одним з найбільш перспективних протоколів генерації ключів є ZRTP. Протокол застосовується в додатку для Android CsipSimple, програмних телефонах Jitsi, Phoner, програмних АТС FreeSwitch і Asterisk, апаратних VoIP шлюзах компанії UM-Labs. Відмінною особливістю ZRTP протоколу є можливість забезпечення безпеки від точки до точки, від одного кореспондента до іншого. Завданнями протоколу ZRTP є: генерація ключових параметрів SRTP сесії; забезпечення конфіденційності повідомлень протоколу; забезпечення аутентифікації кореспондентів; захист від атаки вторгнення посередині, як з використанням, так і без використання інфраструктури відкритих ключів.

Протокол передбачає роботу кореспондентів по топології точка-точка, при цьому окремо виділяється можливість застосування протоколу при багатопотоковому режимі, коли необхідно організувати кілька захищених медіа потоків. Крім того, передбачений режим роботи з легітимним посередником, яким може бути, наприклад, корпоративна телефонна станція. Кожен з кореспондентів-учасників протоколу повинен мати встановлений ідентифікатор (ZID), який повинен бути унікальний.

В основі протоколу - обмін ключами по алгоритму Діффі-Хелмана. Особливістю протоколу є передача параметрів всередині RTP пакетів, залишаючи пакети сумісними з RTP / AVP профілем. В цьому випадку, ZRTP-несумісним пристроєм ZRTP-пакети просто відхиляються і не впливають на встановлене з'єднання.

Для аутентифікації кореспондентів, а також виключення атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткого аутентифікаційного рядка (SAS, Short Authentication String), а також частини ключового матеріалу від попередніх сесій між кореспондентами. Для контролю цілісності переданих повідомлень

кожне повідомлення ZRTP включає в себе код CRC, а також код аутентифікації повідомлення MAC (Message Authentication Code). MAC обчислюється, як ключова хеш-функція, яка узгоджується на першій фазі протоколу.

Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються і при перевірці CRC ZRTP пакета. Протокол виконується послідовно в чотири фази: виявлення; підтвердження; обчислення ключів; завершення. У загальному випадку, ZRTP працює на самому початку розмови кореспондентів, відразу після завершення роботи протоколу SIP, як починає працювати в сторони протокол RTP

Існуючі дослідження в області робіт із захисту голосових зв'язків можна розділити на кілька категорій, а саме: розробка безпечних систем IP-телефонії; аналіз безпеки, що забезпечується системами IP-телефонії; аналіз безпеки, що забезпечується окремими протоколами VoIP, а також аналіз самих протоколів.

При оцінці впливу протоколів забезпечення безпеки на якість потрібно враховувати особливості IP-телефонії в порівнянні з традиційною телефонією. Так, в традиційній телефонії час відгуку вузла зв'язку, тобто час з початку передачі інформації про заняття абонентської лінії до моменту отримання кінцевим обладнанням сигналу готовності до прийому номера, визначається готовністю станції обслужити виклик. У IP-телефонії цей час визначається кінцевим обладнанням і не залежить від поточного стану телефонної станції.

Необхідно оцінити, як протоколи безпеки IP-телефонії можуть впливати на нормовані показники функціонування мереж телефонної мережі зв'язку. Застосування SIP-S може впливати на норму "втрати викликів" в разі, якщо при сценарії абонент-абонент один з кореспондентів використовує політику безумовного використання SIP-S, а другий не підтримує SIP-S протокол. Деяка затримка додатково може виникати за рахунок часу, необхідного на організацію TLS каналу між кореспондентами, необхідного для роботи SIP-S протоколу.

Протоколи розподілу ключів впливають на час встановлення з'єднання або на час організації захищеного мовного каналу, в залежності від місця спрацювання протоколу в сценарії з'єднання. Так протокол ZRTP може працювати після встановлення з'єднання, починаючи з етапу, коли один з кореспондентів зняв трубку. В цьому випадку, протокол впливає на норму "час встановлення з'єднання". Інші протоколи також вимагають передачу додаткових повідомлень, що може збільшувати значення нормованих параметрів.

Перелік посилань

1. Борисов М. А. Основы программно-аппаратной защиты информации. / М. А. Борисов, И. В. Заводцев, И. В. Чижов. – М.: УРСС: Либроком, 2013. – 370 с.

2. Гольдштейн Б.С. IP-телефония. / Б.С.Гольдштейн, А.В.Пинчук, А.Л.Суховицкий. - М.: Радио и связь, 2015-336 с.

3. Тарнавський Ю. А. Технології захисту інформації: підручник / Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

4. Бойко Ю. М. Теоретичні аспекти підвищення завадостійкості й ефективності обробки сигналів в радіотехнічних пристроях та засобах телекомунікаційних систем за наявності завад : монографія / Ю. М. Бойко, В. А. Дружинінін, С. В. Толюпа. - Київ : Логос, 2018. - 227 с.

5. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.

6. Шинкарук О.М. Основи функціонування багатоканальних систем передачі інформації: навч. посіб./ О.М. Шинкарук, Ю.М. Бойко, І.І. Чесановський. – Хмельницький : ХНУ, 2011. – 245с.

7. Кодування джерел інформації та каналів зв'язку: навчальний посібник / [Беркман Л.Н., Бондарчук А.П., Гайдур Г.І., Чумак Н.С.]. – Київ: НН ІТІ ДУТ, 2018. – 91 с.

Інформаційна модель захисту інформації.

Даценко В.С., Тітова В.Ю., Шевчук І.М.
Хмельницький національний університет

Розуміючи інформаційну безпеку як «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян та організацій», правомірно визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації та цілі, а також інші умови і дії, що порушують безпеку [1]. При цьому, природно, слід розглядати і заходи захисту інформації від неправомірних дій, що призводять до заподіяння шкоди.

Практика показала, що для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання. При цьому слід враховувати, що модель не копіює оригінал, а є простішою. При цьому, модель повинна бути досить загальною, щоб описувати реальні дії з урахуванням їх складності [2].

Можна запропонувати компоненти моделі захисту інформації на першому (інформаційному) рівні декомпозиції. На нашу думку, такими компонентами інформаційної моделі можуть бути:

ДОДАТОК В
Презентація

Тема Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів

Мета магістерської роботи полягає в криптографічному захисту інформації в сеансах Інтернет-телефонії, що призведе до підвищення рівня безпечності голосового потоку по Internet мережах і на основі використання програмного розподілу ключів змешити час сеансу встановлення безпечного з'єднання..

Наукова задача – розробка методу підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик IP - протоколів розподілу ключів.

Об'єкт дослідження: є технологія Інтернет-телефонії - безпечної передачі голосового потоку по Internet мережах на базі IP протоколів з пакетною комутацією потоку даних

Предмет дослідження: застосування моделей, методів і IP – протоколів забезпечення криптографічного захисту та стиснення потоку даних при застосуванні технології Інтернет - телефонії. Імовірносно-часові характеристики IP – протоколів.

Задачі досліджень у роботі формулюються наступним чином:

1. Дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості.
2. Розробка моделі нелегітимного абонента для оцінки рівня надійності безпечної IP-телефонії;
3. Розробка методу оцінки параметрів IP-протоколів програмного розподілу ключів між кореспондентами IP-телефонії;
4. Розробка методу, на основі алгоритму Діффі-Хелмана, виявлення нелегітимного абонента, IP - протоколів розподілу ключів між кореспондентами IP-телефонії.

Наукова новизна роботи визначає:

1. Модель нелегітимного абонента. Модель нелегітимного абонента враховує атаку "зустріч посередині" на IP – протоколи, що надасть можливість підвищення захищеності Інтернет-телефонії.

2. Метод виявлення нелегітимного абонента на основі алгоритму Діффі-Хелмана. Вирішує наступні задачі: виявити нелегітимного абонента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності розподіленої секретної ключової інформації між кореспондентами, довіреного центру.

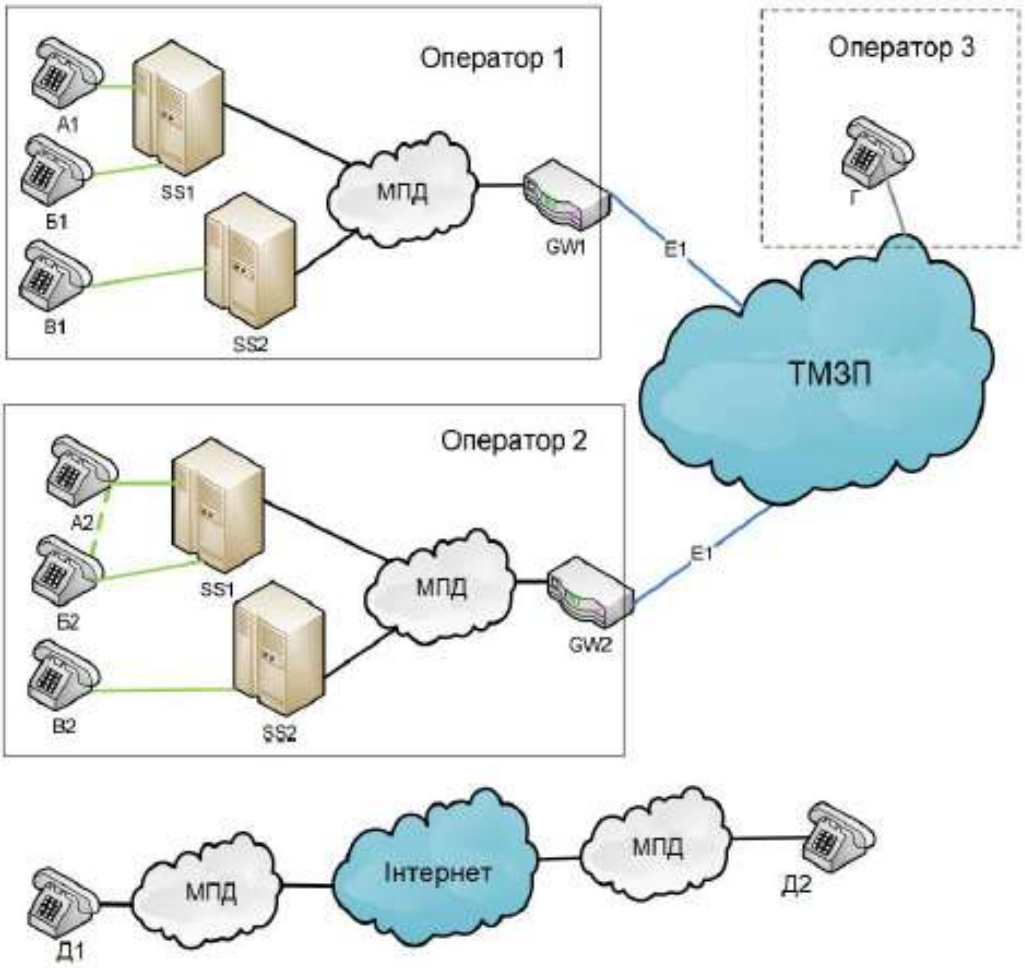
Методи дослідження. Для вирішення поставлених задач в дипломній роботі використовувалися методи системного аналізу, імовірнісних графів, випадкових процесів і математичної статистики, теорії ймовірності, методів чисельного аналізу, комбінаторики.

Практична цінність Модель нелегітимного абонента може використовуватися при оцінці методів контролю рівня захищенності потоку даних з пакетною комутацією в Інтернет-телефонії, що надасть можливість збезпечення надійності IP-телефонії та підвищення захищенності.

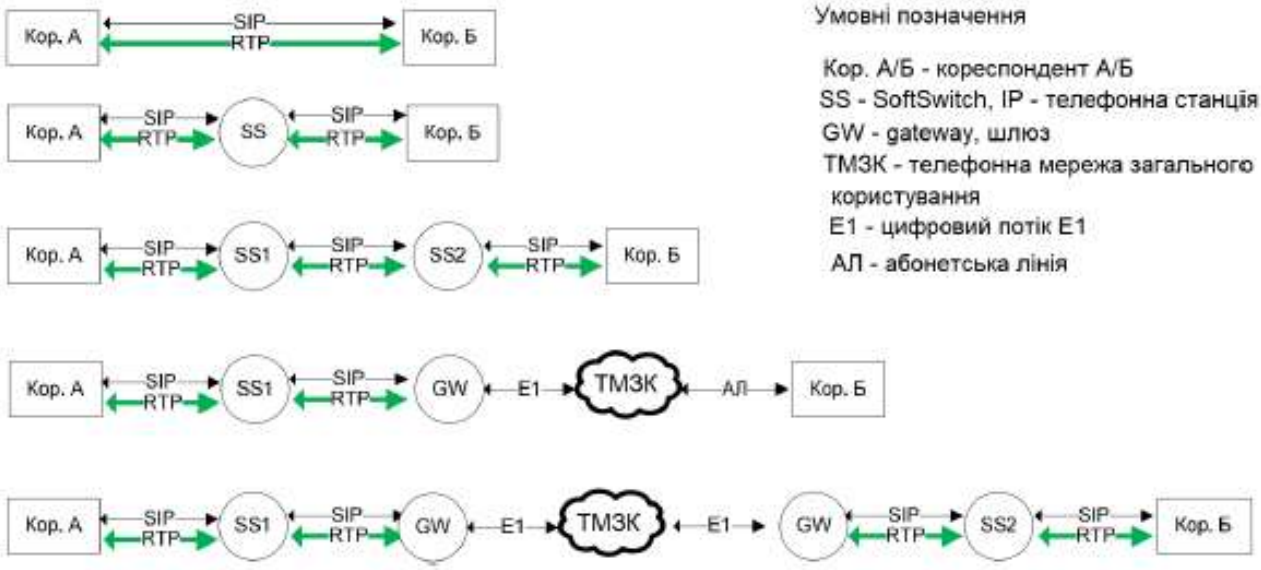
Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на всеукраїнських та міжнародних науково-технічних конференціях,

Публікації. По темі магістерської роботи опубліковано 1 - теза доповідей на всеукраїнських конференціях, 1 стаття.

Принципова схема підключення оператора VoIP



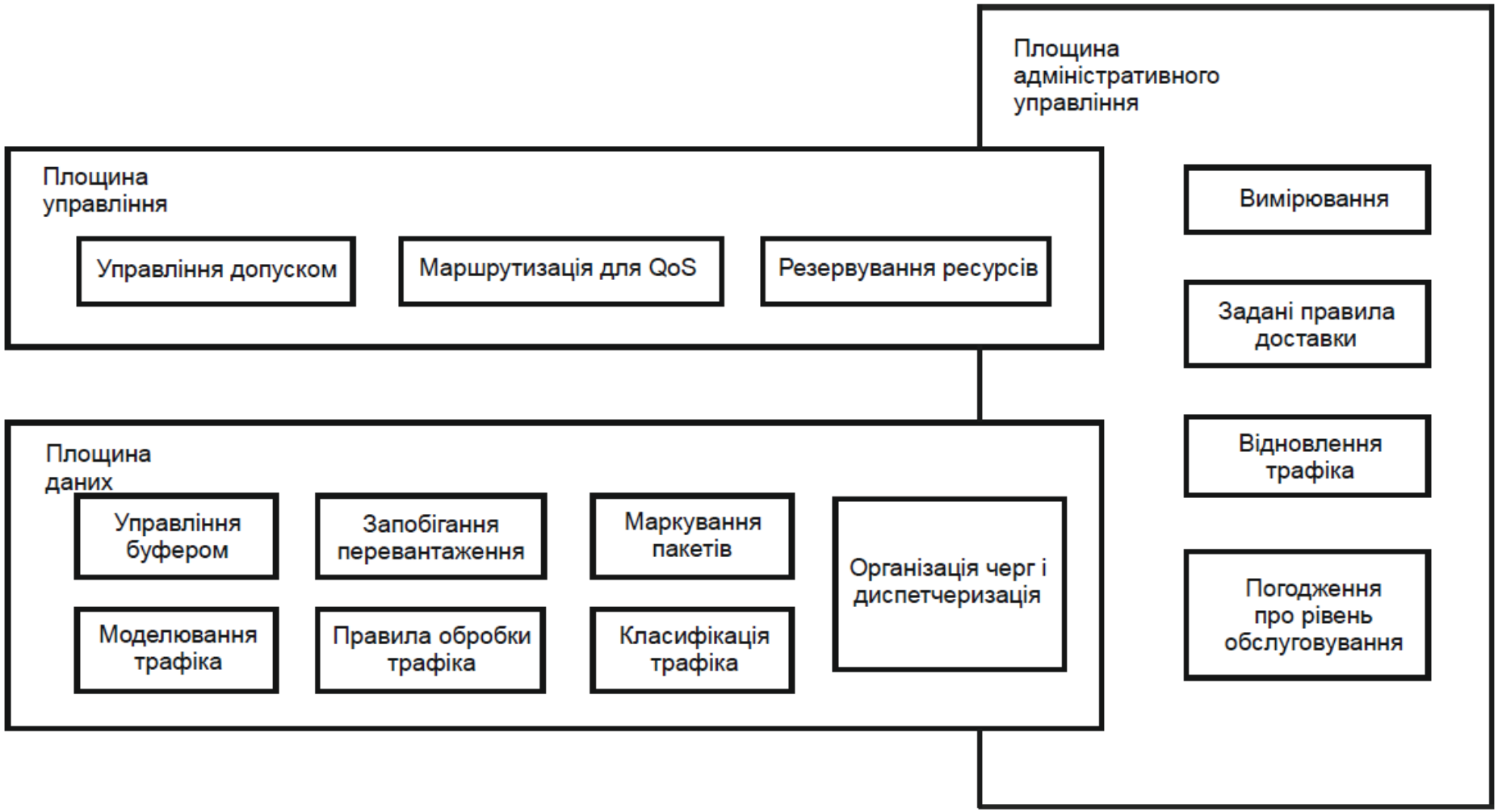
Сценарії підключення оператора VoIP



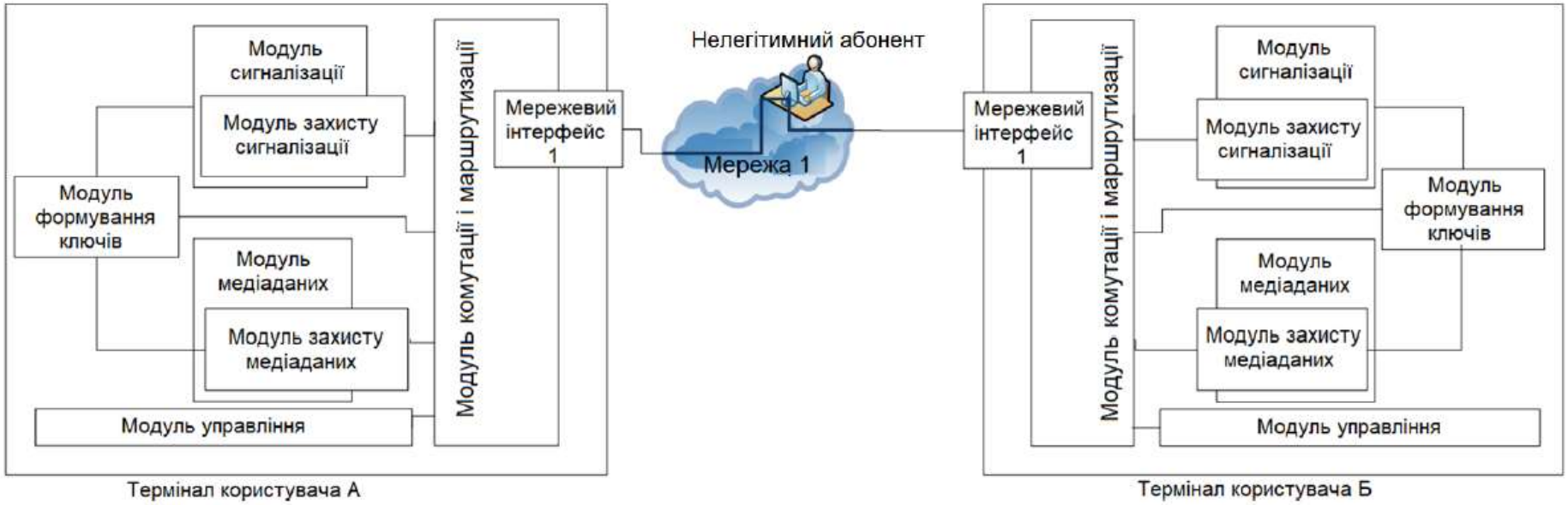
Умовні позначення

Кор. А/Б - кореспондент А/Б
SS - SoftSwitch, IP - телефонна станція
GW - gateway, шлюз
ТМЗК - телефонна мережа загального користування
E1 - цифровий потік E1
АЛ - абонетська лінія

Архітектурна модель підтримки якості IP – телефонії (QoS)



Варіанти дій нелегітимного абонента в схемі встановлення з'єднання клієнт – клієнт



Цілі активного нелегітимного абонента проведеня активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії:

$Ц_{ЗАХОБЛ\_1}$-захоплення обладнання оператора;

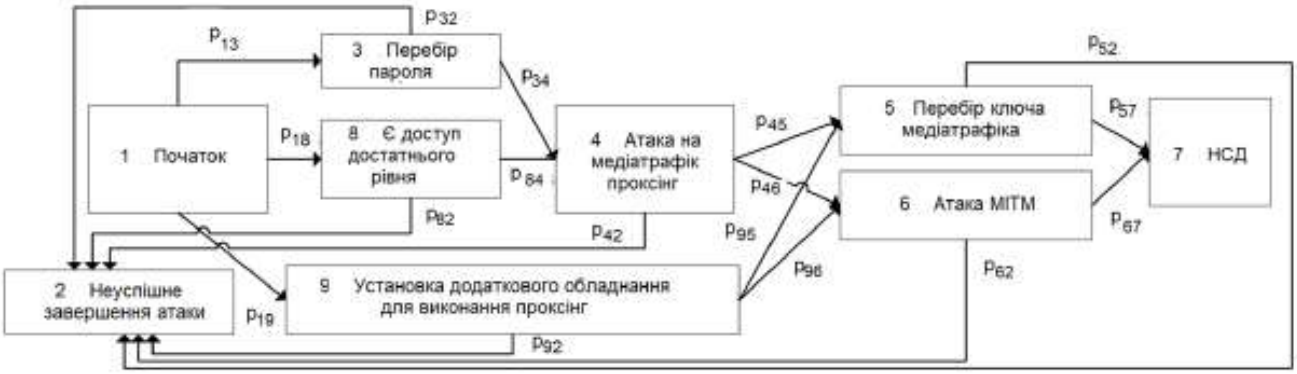
$Ц_{ЗАХМОН\_1}$ - захоплення монітору оператора.

Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних IP - телефонії.

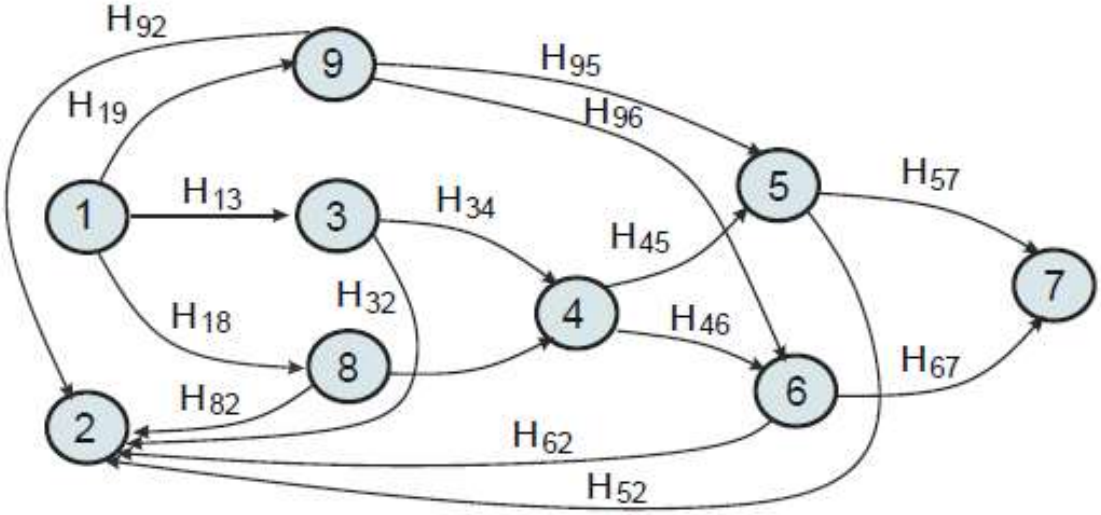
Модель нелегітимного абонента першого рівня безпечної IP – телефонії

(Перший науковий результат)

Алгоритм дій при виконанні захоплення обладнання оператора нелегітимним абонентом



Імовірнісний граф захоплення обладнання оператора нелегітимним абонентом



Імовірність успішної атаки несанкціонованого доступу до даних:

$$P_{НСДШ_{ЗАХОБЛ\_1}} = \left(\left(p_{13}p_{34} + p_{18}p_{84} \right) p_{45} + p_{19} + p_{95} \right) p_{57} +$$
$$+ \left(\left(p_{13}p_{34} + p_{18}p_{84} \right) p_{46} + p_{19} + p_{96} \right) p_{67},$$

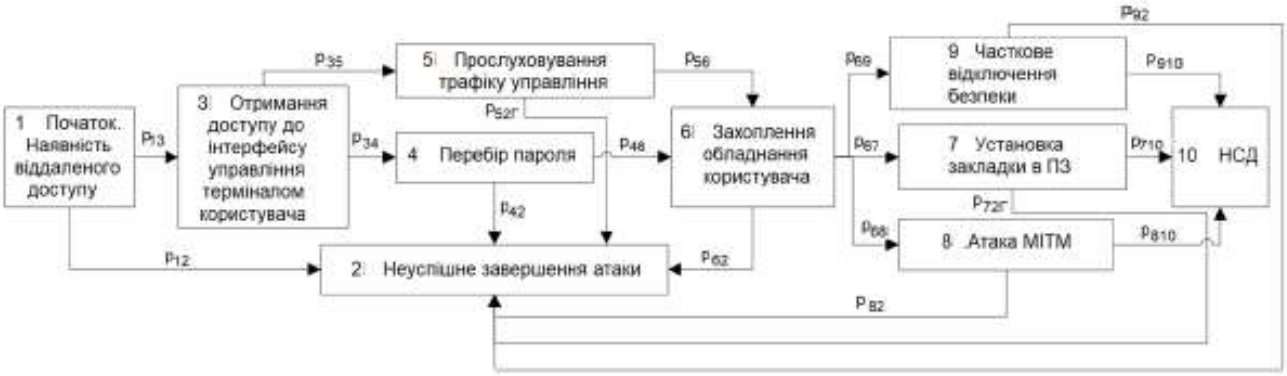
Імовірність захисту від атаки несанкціонованого доступу:

$$P_{ЗАХ\_НСДШ_{ЗАХОБЛ\_1}} = 1 - P_{НСДШ_{ЗАХОБЛ\_1}} = 1 - \left(\left(p_{13}p_{34} + p_{18}p_{84} \right) p_{45} + p_{19} + p_{95} \right) p_{57} +$$
$$+ \left(\left(p_{13B}p_{34} + p_{18}p_{84} \right) p_{46} + p_{19} + p_{96} \right) p_{67}$$

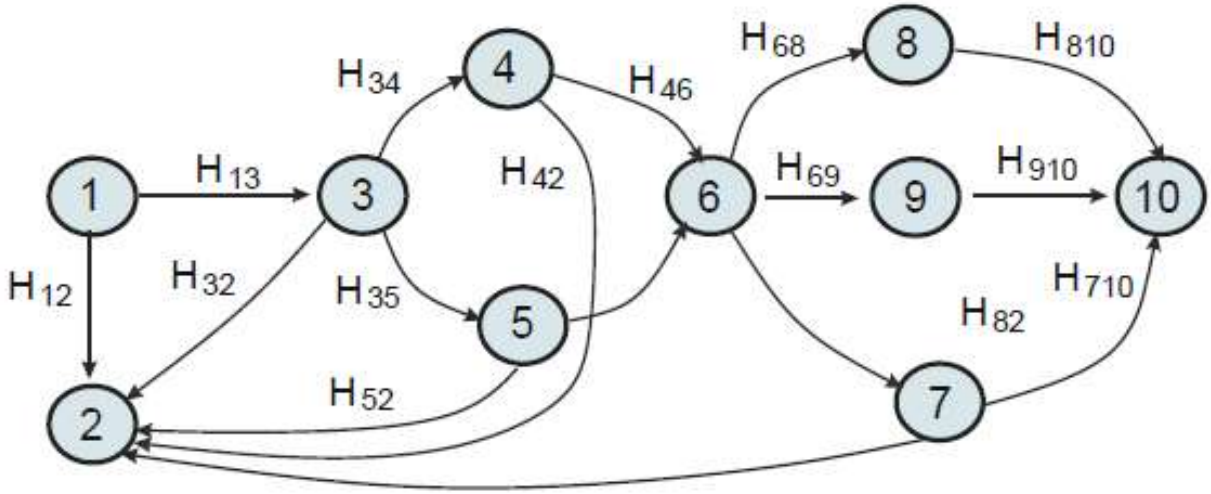
Модель нелегітимного абонента першого рівня безпечної IP – телефонії

(Перший науковий результат)

Алгоритм дій по захопленню монітора кореспондента нелегітимним абонентом



Імовірнісний граф по захопленню монітора кореспондента нелегітимним абонентом



Імовірність успішної атаки несанкціонованого доступу до даних:

$$P_{НСДШ_{ЗАХМОН\_1}} = p_{13}\left(p_{46}p_{34} + p_{56}p_{35}\right)\left(p_{67}p_{710} + p_{68}p_{810} + p_{69}p_{910}\right)$$

Імовірність захисту від атаки несанкціонованого доступу:

$$P_{ЗАХ\_НСДШ_{ЗАХМОН\_1}} = 1 - P_{НСДШ_{ЗАХМОН\_1}} =$$

$$= 1 - p_{13}\left(p_{46}p_{34} + p_{56}p_{35}\right)\left(p_{67}p_{710} + p_{68}p_{810} + p_{69}p_{910}\right)$$

Метод підвищення ефективності IP - протоколу розподілення секретної інформації

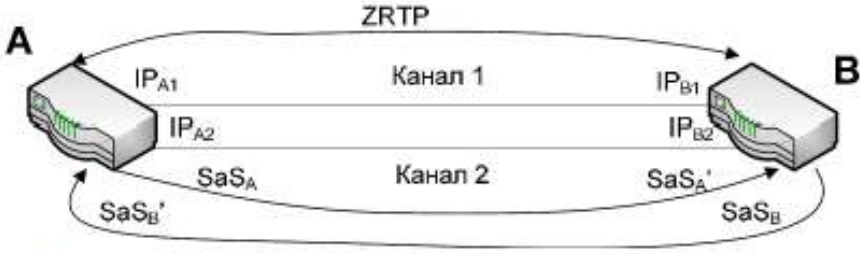
(Другий науковий результат)

1. Учасники сесії А і В виконують обмін інформацією про IP-адреси: $IP_{A1}, IP_{A2}, IP_{B1}, IP_{B2}$, а також налаштовують відповідним чином таблицю маршрутизації.

2. Для організації захищеного з'єднання IP-телефонії, учасники сесії абоненти *A* і *B*, виконують IP-протокол ZRTP використовуючи при цьому канал зв'язку $IP_{A1} - IP_{B1}$, результатом роботи протокола ZRTP є отримання аутентифікаційного рядка

3. Абонент *A* відправляє свій аутентифікаційний рядок SAS_A по каналу зв'язку $IP_{A2} - IP_{B2}$ абоненту *B*. Абонент *B* отримує аутентифікаційний рядок SAS_A'.

4. Абонент *B* відправляє свій аутентифікаційний рядок SAS_B по каналу зв'язку $IP_{A2} - IP_{B2}$ абоненту *A*. Абонент *A* отримує SAS_B'.



Механізм програмної перевірки аутентифікаційного рядка

5. Абонент *B* виконує перевірку аутентифікаційних рядків SAS_A і SAS_B.

6. Якщо аутентифікаційні рядки співпадають то можна зробити наступний висновок що в мережі відсутній активний нелегітимний абонент в каналах зв'язку, або також що вірогідно присутній активний нелегітимний абонент одночасно в каналах зв'язку.

7. Якщо значення аутентифікаційних рядків не співпадають, абонент *B* отримує повідомлення від VoIP-монітора IP- телефонії про наявність нелегітимного абонента в каналі зв'язку.

8. Абонент *A* виконує перефірку на співпадання аутентифікаційних рядків SAS_A і SAS_B'. Якщо вони співпадають то можна зробити наступний висновок що в мережі відсутній активний нелегітимний абонент в каналах зв'язку, або також що вірогідно присутній активний нелегітимний абонент одночасно в каналах зв'язку.

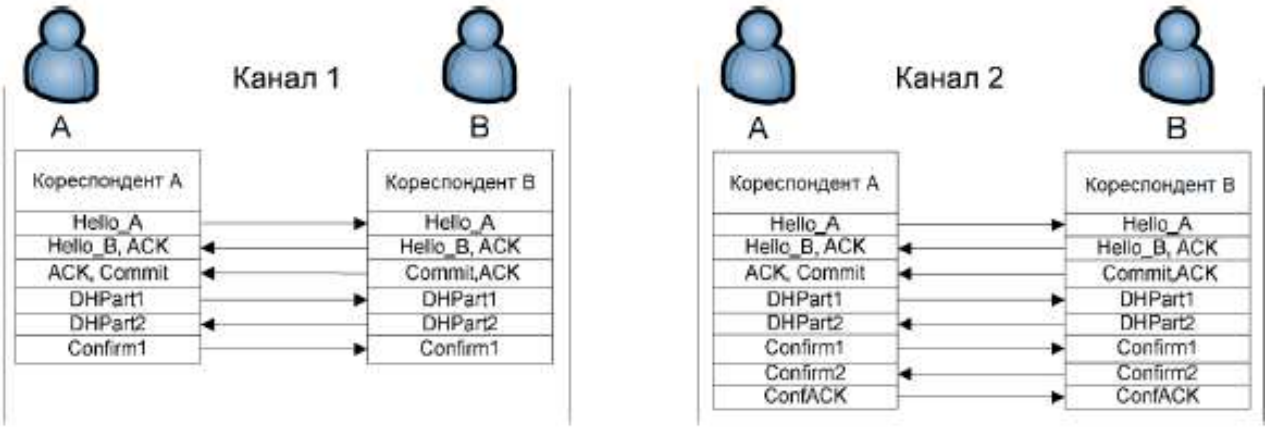
9. Якщо значення аутентифікаційних рядків не співпадають, абонент *A* отримує повідомлення від VoIP-монітора IP- телефонії про наявність нелегітимного абонента в каналі зв'язку.

Таким чином використання даного методу надасть нам інформацію про наявність активного нелегітимного абонента, який в стані провести активну атаку в одному з двох каналів зв'язку.

Метод підвищення ефективності протоколу розподілення ключів на основі алгоритму Діффі – Хелмана

(Другий науковий результат)

Взаємодія абонентів Інтернет мережі IP – телефонії при використанні двоканального методу



$P_{VA\_HA2} = \left(P_{НСДЦ_{ЗАХОБЛ\_2}}\right)^2$ - ймовірність здійснення події одночасного прослуховування і модифікації повідомлень в двоканальному зв'язку

$P_{HA1K\_NO\_2K} = (1 - P_{HCBA})P_{HCBA}$ - ймовірність присутності нелегітимного абонента в першому каналі при відсутності нелегітимнного абонента в другому каналі зв'язку

Імовірність наявності нелегітимнного абонента в другому каналі зв'язку IP – телефонії при відсутності зловмисника в першому каналі зв'язку визначиться наступним чином:

$$P_{HA2K\_NO\_1K} = (1 - P_{HCBA})P_{HCBA} = P_{HCBA} - P_{HCBA}{}^2$$

$$P_{BA2} = P_{HA1K\_NO\_2K} + P_{HA2K\_NO\_1K} = 2(1 - P_{HCBA})P_{HCBA}$$

Імовірність відсутності нелегітимнного абонента в одному каналі зв'язку P_{NO_HA}:

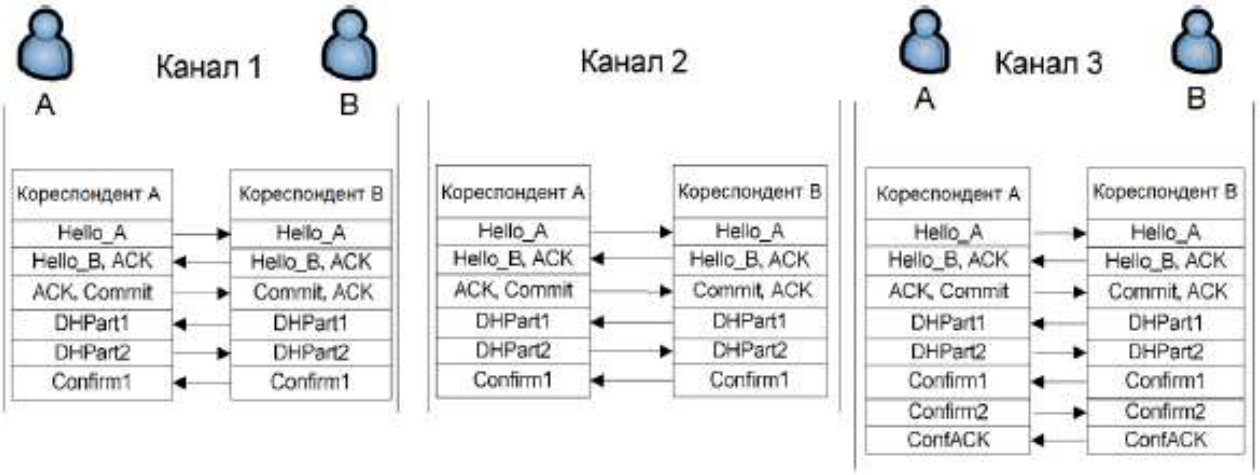
$$P_{NO\_HA} = 1 - P_{HCBA} \text{ тоді: } P_{VK2} = P_{NO\_HA}{}^2 = (1 - P_{HCBA})^2.$$

Під успішної подією генерації загального секретного ключа розуміється, що нелегітимного абонента не виявлено ні в одному каналі зв'язку і кореспондентами вироблений загальний секретний ключ для шифрування потоку даних, які передаються по каналам звязку. Це можливо тільки в разі відсутності нелегітимнного абонента в каналах зв'язку, або при використанні можливості алгоритму розподілу загальної секретної інформації визначати точне місцезнаходження нелегітимнного абонента в конкретному (конкретних) каналах зв'язку.

Метод підвищення ефективності протоколу розподілення ключів на основі алгоритму Діффі – Хелмана

(Другий науковий результат)

Взаємодія абонентів Інтернет мережі IP – телефонії при використанні трьохканального методу



$P_{ПрВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ} \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2$ - ймовірність правильного виключення нелегітимного абонента для трьохканального IP - протоколу

$P_{ПомВНА} = 3 \cdot P_{НСВ\_ЗАХОБЛ}{}^2 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)$ - Імовірність помилкового виключення нелегітимного абонента для трьохканального IP - протоколу

Імовірність наявності нелегітимного абонента в двох з трьох каналів зв'язку при відсутності нелегітимного абонента в одному з каналів зв'язку:

$$P_{НА23К\_NO\_НА1К} = 3 \cdot \left(1 - P_{НСВА}\right) \cdot P_{НСВА}{}^2$$

$$P_{ВАНА\_ВНА} = P_{НА1К\_NO\_НА23К} + P_{НА23К\_NO\_НА1К} =$$

$$= 3 \cdot \left(1 - P_{НСВА}\right)^2 \cdot P_{НСВА} + 3 \cdot \left(1 - P_{НСВА}\right) \cdot P_{НСВА}{}^2$$

Імовірність успішної генерації загальної секретної інформації $P_{УКНА\_ВКНА}$ для трьохканального IP - протоколу

$$P_{УКНА\_ВКНА} = \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^3 + 3 \cdot \left(1 - P_{НСВ\_ЗАХОБЛ}\right)^2 \cdot P_{НСВ\_ЗАХОБЛ}$$

У схемі з виключенням нелегітимного абонента імовірність збільшується, але при використанні каналів зв'язку IP – телефонії великої протяжності можливе співпадання вузлів проходження маршрутів потоку даних, що, в даному випадку, може призвести до зниження ефективність роботи модифікованого IP - протоколу.

ВИСНОВКИ

У дипломній роботі вирішена задача підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії та скорочення часу встановлення захищеного з'єднання за рахунок покращення ІЧХ IP - протоколів, та отримані основні результати:

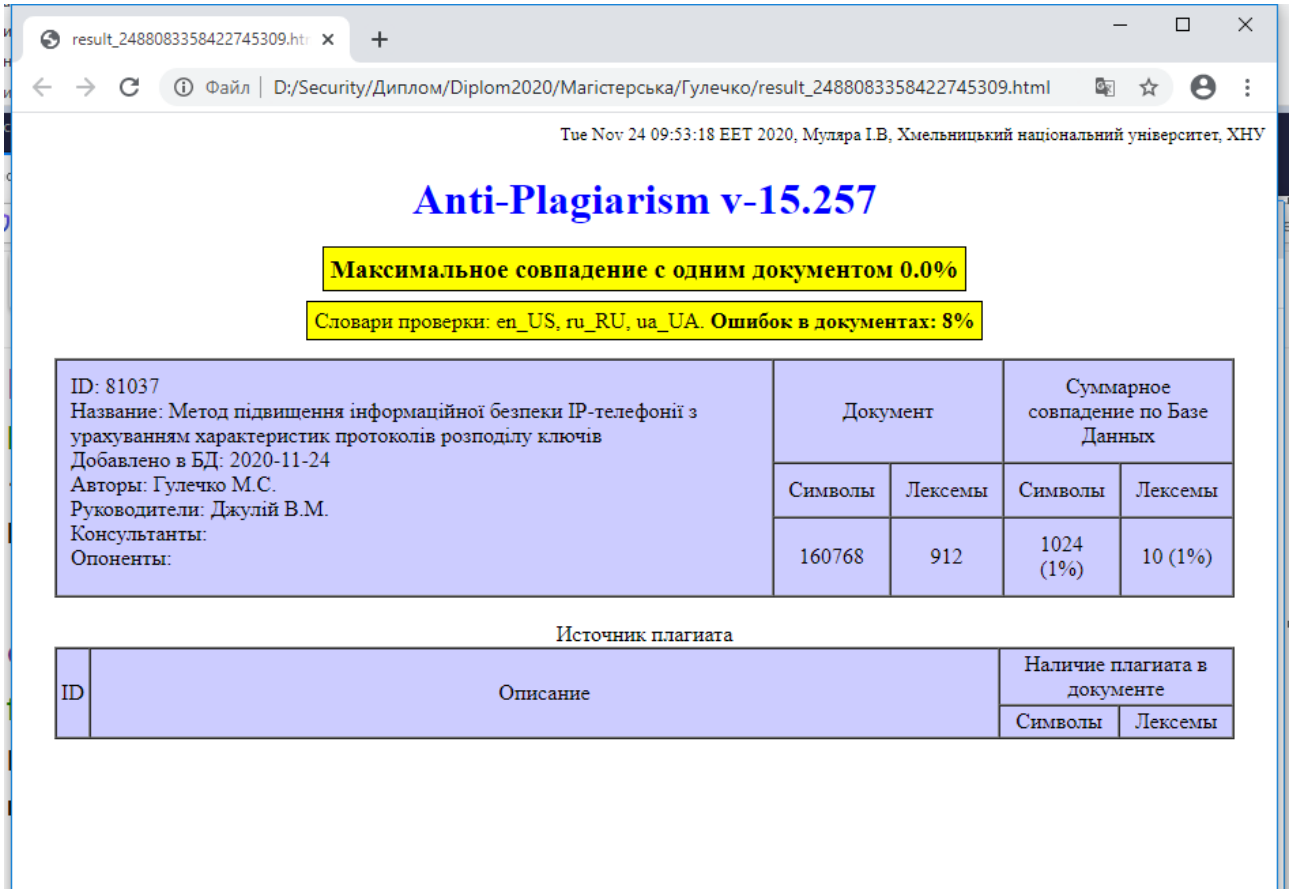
1. Математична модель активного нелегітимного абонента для захищеної IP-телефонії Інтернет мережі, надає можливість враховувати цього атаку нелегітимного абонента «зустріч по середині» на протокол розподілу секретної інформації, дозволяє обчислити ймовірність успішної атаки, отримання несанкціонованого доступу до закритої інформації, успішність завершення атаки залежить від значень ймовірностей проміжних атак .

2. Метод оцінки ІЧХ протоколів розподілу загальної секретної інформації захищеної IP-телефонії Інтернет мережі, враховує особливості IP-протоколів, а саме обмеження числа повторних передач потоку даних.

3. Представлена модифікація протоколу розподілу загальної секретної інформації ZRTP, дозволяє об'єднати потоки даних про підтримуваних криптографічних наборах і блоків протоколу Діффі - Хелмана.

4. Метод виявлення активного нелегітимного абонента протоколів розподілу загальної секретної інформації ключів, використовується при роботі за сценарієм типу клієнт-клієнт для кінцевих абонентів, які не мають наперед розподіленої секретної інформації. Метод забезпечує з високою ймовірністю встановити надійне захищене з'єднання між абонентами, а також виявити активного нелегітимного абонента в каналі зв'язку, що реалізує атаку «зустріч по середині» на протокол розподілу загальної секретної інформації ключів.

За темою роботи опубліковано 1 теза та 1 наукова статья.



result_248808335842274530 ×

Файл | D:/Security/Диплом/Diplom2020/Магістерська/Гулечко/result_248808335842274530.html

Tue Nov 24 09:53:18 EET 2020, Муляра І.В, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 8%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 81037 Название: Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів Добавлено в БД: 2020-11-24 Авторы: Гулечко М.С. Руководители: Джулій В.М. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	160768	912	1024 (1%)	10 (1%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

User name:
Kafedra kiberbezpeky

Check ID:
1005202936

Check date:
26.11.2020 13:17:07 EET

Check type:
Doc vs Internet + Library

Report date:
26.11.2020 13:19:07 EET

User ID:
100005590

File name: **ГулечкоМС_Магістерська_пл**

Page count: **102** Word count: **22055** Character count: **168907** File size: **12.61 MB** File ID: **1005327302**

1.09% Matches

Highest match: **0.41%** with Internet source (**http://internal.khntusg.com.ua/fulltext/PAZK/UCHEBNIKI/Ekonom_pidpr_2012.pdf**)

1.09% Internet sources	126	..... Page 104

No Library sources found

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters	40

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРІ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів

Автор: Гудечко Михайло Сергійович

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: Програмування та захист КСМ

Науковий керівник: Джулій Володимир Миколайович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	✓
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження: до захисту допускається

4.12.2020

Дата

Підписи

Клюх Ю.П.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

освітнього ступеня «магістр»

Магістр Гулечко Михайло Сергійович
Тема Метод підвищення інформаційної безпеки IP-телефонії з урахуванням характеристик протоколів розподілу ключів
Спеціальність 123 «Комп'ютерна інженерія»
спеціалізація «Комп'ютерні системи та мережі»

Обсяг дипломної роботи освітнього ступеня «магістр»:

кількість листів креслень 11 ; кількість сторінок записки 109

1. Короткий зміст ДР та прийнятих рішень В рамках магістерської роботи вирішена задача підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії та скорочення часу встановлення захищеного з'єднання за рахунок покращення ЧХ IP - протоколів, та отримані основні результати: математична модель активного нелегітимного абонента для захищеної IP-телефонії Інтернет мережі, надає можливість враховувати атаку нелегітимного абонента «зустріч по середині»; представлена модифікація протоколу розподілу загальної секретної інформації ZRTP, дозволяє об'єднати потоки даних про підтримуваних криптографічних наборах і блоків протоколу Діффі – Хелмана; метод виявлення активного нелегітимного абонента протоколів розподілу загальної секретної інформації ключів, використовується при роботі за сценарієм типу клієнт-клієнт для кінцевих абонентів, які не мають наперед розподіленої секретної інформації.

2. Висновок про відповідність ДР дипломному завданню Дипломна робота освітнього ступеня «магістр» у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині дипломної роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обгрунтовується актуальність теми роботи, дається аналіз досліджуваної проблеми і обгрунтовується застосовуваний підхід до її вирішення, формулюються цілі і завдання дослідження, описується наукова новизна і практична значимість отриманих результатів. У першому розділі якісно та в повній мірі проаналізовано сучасний стан існуючих алгоритмів, методів підвищення надійності захищеної IP-телефонії. Наступні розділи присвячені розробці моделі та методу структурної організації захищеної IP-телефонії та класифікації атак в каналах зв'язку. Розглянуто питання оцінки залежності ймовірносно-часових характеристик IP - протоколів.

4. Позитивні сторони проекту Дипломна робота містить ряд інноваційних рішень, зокрема, в розробці моделей і алгоритмів виявлення атак типу «зустріч по середині» з урахуванням фундаментальних характеристик IP-телефонії, в отриманих розрахункових виразах, моделях і алгоритмах, що реалізують проектування Інтернет мереж захищеної IP-телефонії.

5. Негативні сторони проекту Як показано в роботі зі збільшенням числа каналів надійність IP-телефонії зростає, в той же час вірогідність перетину каналів також зростає, що веде в свою чергу до фактичного зменшення каналів. Як визначається надійність в даній ситуації?

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми дипломної роботи з дотриманням стандартів. В загальному графічне оформлення виконане на достатньому рівні. Пояснювальна записка відповідає нормам для її оформлення.

7. Відгук про роботу в цілому В загальному дипломна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики дипломної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8.Інші зауваження

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої дипломної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)

Лисенко Сергій Миколайович, доцент, кафедра комп'ютерної інженерії та системного програмування, Хмельницького національного університету

«02» грудня 2020р. _____ (підпис)

ХНУ Зам. 54, тир. 6000, 2007.