ISSN 2219-9365

УДК 004.891
DOI: 10.31891/2219-9365-2021-67-1-19

ДЖУЛІЙ В. М., ЧЕШУН В. М.
Хмельницький національний університет
ДЖУЛІЙ А. В., ЧОРНЕНЬКИЙ В. І.
Університет економіки і підприємництва

ІМОВІРНІСНІ АЛГОРИТМИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

Результати проведеного аналізу та дослідження надають можливість вказати, що найбільш відомі IP-протоколи розподілу загальної секретної інформації необхідно вдосконалювати в двох напрямках: підвищення інформаційної безпеки IP-телефонії та покращення основних показників IP-протоколів Інтернет мереж.

Одним з методів забезпечення підвищення безпеки IP-протоколу формування загальної секретної інформації є відстеження і заборона виконання атаки типу «зустріч по середині» за рахунок використання в мережах IP-телефонії декількох паралельних незалежних каналів сеансів зв'язку.

Розглянуто актуальне завдання підвищення захищеності IP-телефонії та безпеки програмного розподілу загальної секретної інформації, що відрізняється від існуючого методу виявлення нелегітимного абонента впровадженням автоматизованої програмно-апаратної перевірки коду автентифікації. При використанні в даному випадку декілька каналів зв'язку, відповідна перевірка надає можливість виявити нелегітимного абонента.

Ключові слова: імовірнісні алгоритми, нелегітимний кореспондент, інформаційна взаємодія, інтернет-телефонія, криптографічний захист, канали зв'язку.

V. DZHULIY, V. CHESHUN
Khmelnytskyi National University
A. DZHULIY, V. CHORNENKYI
University of Economics and Entrepreneurship

PROBABILITY ALGORITHMS AND METHODS OF IP-TELEPHONY SECURITY

The urgent task of increasing the security of IP-telephony and security of software distribution of general classified information, which differs from the existing method of identifying an illegitimate subscriber, the introduction of automated software and hardware verification of the authentication line. When using in this case several communication channels, the corresponding check will give the chance to reveal the illegitimate subscriber. The results of the analysis and research provide an opportunity to indicate that the most well-known IP protocols for the distribution of general classified information need to be improved in two ways: improving the information security of IP - telephony and improving the basic indicators of IP protocols of Internet networks.

The Diffie-Hellman algorithm solves the following problems: provides an opportunity to identify an active illegitimate correspondent who uses voice synthesis software; to identify an active illegitimate IP correspondent - protocols in Internet telephony communication channels in the absence of previously distributed secret key information between correspondents, a trusted center. The method can be used in the evaluation of methods for monitoring the level of security of data packet-switched data in Internet telephony, which will provide the reliability of IP telephony and increase security.

One of the methods to increase the security of the IP protocol for the formation of general classified information is to monitor and prohibit an attack such as a "meeting in the middle" through the use of Internet IP telephony networks of several parallel independent communication channels. IP - a protocol with software verification of the authentication line of IP telephony does not provide an opportunity to determine which communication channel the illegitimate subscriber will perform active attacks. Also, the detection of an illegitimate subscriber in the communication channel is possible only after the successful completion of the protocol, the illegitimate subscriber can not be detected during the operation of the protocol.

Keywords: probabilistic algorithms, illegitimate correspondent, information interaction, Internet telephony, cryptographic protection, communication channels.

Вступ. Забезпечення підвищення ефективності та безпеки всіх галузей виробництва на сьогодні є однією з ключових проблем, тому актуальною є необхідність впровадження і розвитку сучасних інформаційних технологій. Поширення IP-телефонії через Internet мережі поставило під загрозу прибутки операторів телефонних мереж [1]. Проте, оператори AT&T, British Telecomunications, Deutsche Telecom, починають надавати послуги IP-телефонії.

Перевагою Internet-телефонії є низька вартість міжміських і міжнародних переговорів, вона дозволяє зменшити витрати на послуги передачі факсів і мультимедіа зв'язку за рахунок шифрування і стиснення голосового потоку [2, 3]. Internet-телефонія не використовує дороге устаткування на шляху передачі інформації пакетів з голосовим сигналом [4].

Аналіз останніх досліджень і публікацій. Розвиток нових IP-протоколів Internet мереж, а також передача потоку пакетних даних у вигляді голосових пакетів у відкритому вигляді через публічні мережі призвели до необхідності стандартизації IP-протоколів Internet мереж, а також криптографічного захисту даних для забезпечення безпечної Internet-телефонії [5, 6]. В результаті проведених заходів IP-протоколи Internet мереж розділені, у 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 [7].

Стандартизація протоколів, а також масове використання персональних комп'ютерів операторами IP-телефонії в якості терміналів, призвели до розробки спеціалізованого програмного забезпечення для IP-телефонії, а також до 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.

Для розподілу секретної інформації між кореспондентами IP-телефонії на даному етапі використовуються алгоритми асиметричного шифрування [8, 9, 10, 11]. До переваг використання алгоритмів асиметричного шифрування можна віднести розподіл секретної інформації між кореспондентами IP-телефонії. Недоліком є те що вони досить повільні, мають відносно велику довжину ключа, є не придатними для шифрування великих об’ємів інформації. Область їх застосування - розподіл секретної інформації між кореспондентами IP-телефонії, формування цифрового підпису.

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 [12, 13].

Постановка задачі. Проведений аналіз наукових досліджень технологій IP-телефонії в областях криптографічного захисту передачі інформації, забезпечення якості потоку даних з пакетною комутацією, 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 заздалегідь загального секретного ключа для операторів [14]. 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 методу та алгоритму забезпечення безпеки IP-телефонії, які будуть враховувати атаку типу "зустріч посередині".

Виклад основного матеріалу. Асиметричний алгоритм Діффі-Хелмана обміну секретною інформацією 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. Доцільно протокол Діффі-Хелмана використовувати в захищених каналах передачі голосової інформації, в яких унеможливується несанкціонований доступ до голосової інформації та її модифікація чи підміна.

У разі необхідності в мережі IP-телефонії встановлення захищеного з'єднання проти атак типу «зустріч по середині» між двома кореспондентами учасниками сесії, в даному випадку можлива ситуація, коли 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 кореспондентам, центру сертифікації іншого абонента. Для встановлення захищеного з'єднання між абонентами учасниками сесії IP-телефонії виникає необхідність генерації та розподілу загальної секретної інформації (ключів) для реалізації з'єднання. Абоненти в даній ситуації можуть використовувати алгоритми симетричного або асиметричного шифрування. Недоліком алгоритмів симетричного шифрування є необхідність передачі секретного ключа відкритими каналами зв’язку . В нелегітимного абонента з’являється цілком вірогідна можливість перехоплення секретної інформації, що дозволяє 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 відкритими каналами зв’язку передана інформація не буде прочитана нелегітимним абонентом у 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, у абонентів учасників зв’язку не буде можливості переконатися, що несекретний ключ передається між ними без модифікації нелегітимним абонентом, як показано на рис. 1. Також до недоліків алгоритмів асиметричного щифрування слід віднести те, що відкритий і секретний ключі мають відносно великий розмір, що утрудняє їх передачу по Інтернет мережі між абонентами зв’язку.

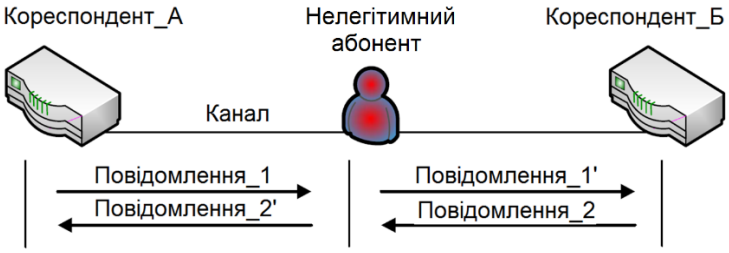

Рис. 1. Застосування атаки «зустріч по середині» при використанні асиметричного шифрування

Для підвищення безпеки генерації та обміну загальної секретної інформації пропонується використовувати наступні шляхи: підвищення безпеки передачі інформації за рахунок програмної перевірки автентифікаційного 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 автентифікаційного рядка абонентів з використанням ще одного каналу зв'язку, при цьому автентифікаційний 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 каналу IP-телефонії. Виникає необхідність в автоматизації процесу перевірки короткого автетифікаційного 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 протоколів IP-телефонії використана перевага легітимних абонентів по відношенню до нелегітимних, яка полягає в тому, що тільки легітимні абоненти учасники сесії мають доступ до отримання голосової інформації з двох і більше каналів 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 протоколів IP-телефонії розподілу загальної секретної інформації між абонентами сесії пропонується для підвищення захищеності, але даний протокол IP-телефонії не гарантує 100% достовірності. В якості оцінки модернізації протоколів IP-телефонії використовуються наступні критерії величин 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 $P_{У\_СК}$.

Протокол IP-телефонії ZRTP (криптографічний протокол узгодження ключів шифрування, використовуваний у системах передачі голосу по IP мережам) має в своєму розпорядженні механізм захисту активної атаки нелегітимним абонентом типу «зустріч по середині», виражений у вербальній перевірці короткого автентифікаційного рядка по голосовому каналу між абонентами сесії IP-телефонії. В даному випадку після успішного виконання протоколу IP-телефонії ZRTP і встановлення голосового каналу між абонентами сесії в топології типу клієнт-клієнт без сервера, абоненти отримують відповідне значення короткого автентифікаційного рядка - що представляє собою комбінацію символів обчислений-отриманий спеціалізованим алгоритмом. Один з абонентів учасників сесії вимовляє короткий автентифікаційний рядок голосовим каналом зв'язку IP-телефонії. Інший абонент який є також учасником сесії, звіряє короткий автентифікаційний рядок на своєму VoIP-моніторі зі значенням, отриманим по голосовому каналу. Якщо автентифікаційні 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 автентифікаційного рядка голосовим каналом зв'язку. Якщо автентифікаційні 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 автентифікація буде виконуватися за рахунок знання абонентом голосових характеристик іншого абонента учасника зв'язку, а також за рахунок немодифікованої передачі потоку даних по двох каналах зв'язку - голосовим каналом SRTP і каналом передачі даних.

Використанням сучасного програмно-апаратного забезпечення та відповідних технологій достатньо просто виконати синтез голосової інформації 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 автентифікаційного рядка. Переданої голосової інформації може бути достатньо для синтезу голосової інформації абонента для підміни одного набору символів на інші з метою модифікації автентифікаційного рядка в голосовому каналі. В цьому випадку перевірка автентифікаційного рядка пройде успішно навіть при наявності активної атаки нелегітимним абонентом типу «зустріч по середині» (рис. 2).

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 протоколу IP-телефонії ZRTP пропонується впровадження автоматизованої програмно-апаратної перевірки автентифікаційного рядка. При використанні декількох каналів зв'язку, відповідна перевірка надасть можливість виявити нелегітимного абонента.

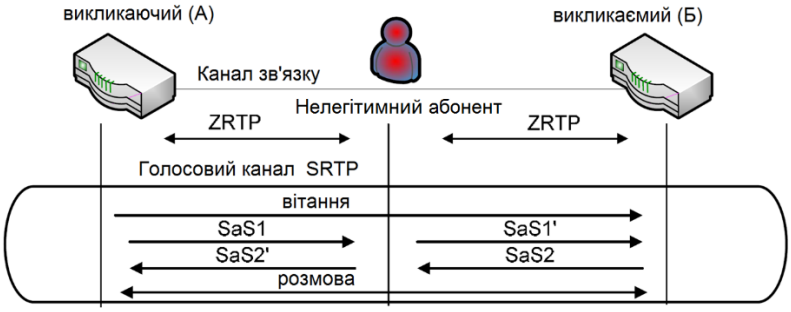

Рис. 2. Підміна автентифікаційного рядка в голосовому каналі зв'язку IP-телефонії

Інформація про IP-адресу, яка необхідна для організації захищеного каналу сесії, може бути отримана абонентами наступним чином: по телефону, при особистій зустрічі, по електронній пошті, іншими доступними засобами зв'язку. Інформація про IP-адресу не є секретною для нелегітимного абонента і може бути передана відкритими каналами зв'язку, на відміну від IP-адрес, загальна секретна інформація для алгоритмів симетричного шифрування є закритою і доступ до неї призведе для нелегітимного абонента до 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 іншим каналом зв'язку.

Перевагою підвищення безпеки потоку даних у вигляді програмної автоматизованої перевірки ідентифікаційного рядка є невисока складність розробки та реалізації програмними засобами IP-протоколу. Аутентифікаційний рядок передається в спеціалізоване програмне забезпечення за результатом виконання IP-протоколу ZRTP. В даному випадку достатньо передати автентифікаційний рядок абоненту по додатковому каналу зв'язку для виконання програмної автоматичної перевірки. Недолік – 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: 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 перевірки автентифікаційного рядка та виявлення активного нелегітимного абонента, який працює в одному з двох каналів зв'язку.

Алгоритм 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, використовують при цьому канал зв'язку IP_{A1}–IP_{B1}. Результатом роботи протокола ZRTP є отримання автентифікаційного рядка (рис. 3).

3. Абонент *A* відправляє свій автентифікаційний рядок SAS_A каналом зв'язку IP_{A2}–IP_{B2} абоненту *B*.

Абонент *B* отримує автентифікаційний рядок SAS_A'.

4. Абонент *B* відправляє свій автентифікаційний рядок SAS_B каналом зв'язку IP_{A2}–IP_{B2} абоненту *A*. Абонент *A* отримує SAS_B '.

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

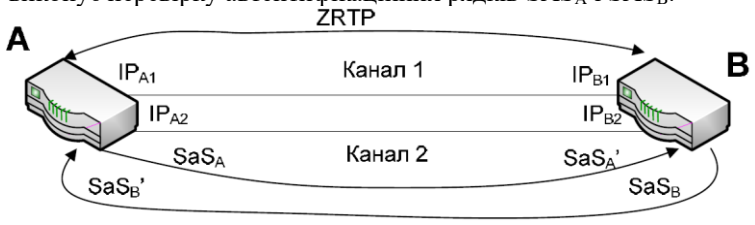

Рис. 3. Механізм програмної перевірки автентифікаційного рядка

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

7. Якщо значення автентифікаційних 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 автентифікаційних рядків SAS_A і SAS_B'. Якщо вони співпадають, то можна зробити висновок, що в мережі відсутній активний нелегітимний абонент в каналах зв'язку, або, що вірогідно також, присутній активний нелегітимний абонент одночасно в обох каналах зв'язку.

9. Якщо значення автентифікаційних 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 надає 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 ймовірностей: $P_{УА\_ЗС}$ - 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», 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, атака називається успішною. 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 коду автентифікації 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 автентифікаційного рядка IP-телефонії не надає можливості визначити, на який саме канал зв'язку нелегітимний абонент буде виконувати активну атаку. 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.

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 автентифікаційного рядка. При використанні в цій ситуації декількох каналів зв'язку відповідна перевірка надає можливість виявити нелегітимного абонента.

IP-протокол з програмною перевіркою автентифікаційного 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.

References

1. José Estrada, Mayra Calva, Ana Rodríguez, Christian Tipantuña. Security of IP Telephony in Ecuador: Online Analysis. Enfoque UTE, V.7-N.2, Jun.2016, P.25-40.
2. Cherkasov D. Osnovy tekhnolohii VoIP ta IP-telefonii / Dmytro Cherkasov // Telekom voennaia sviaz. – 2017. – №2. S. 98-104.
3. VOIP security and best practices : For SIP Trunking and Branch Offices Applications. Sangoma Technologies, 2018. 54 r.
4. Hulechko M. S. Analiz potochnoho stanu dii v oblasti zakhyshchenoi IP- telefonii / M. S. Hulechko, V. M. Dzhulii, V. Yu. Titova // Zbirnyk naukovykh prats molodykh naukovtsiv i studentiv «Intelektualnyi potentsial – 2020». – Khmelnytskyi : PVNZ UEP, 2020. – Ch. 2. – S. 35–39.
5. Lytvynov V.V. Suchasnyi stan zakhystu informatsii v IR-telefonii / V.V. Lytvynov, V.V. Kazymyr, Ye.V. Ryndych // Matematychni mashyny i systemy. –2009. – № 2. – S. 76-84.
6. Filip Rezac; Jan Rozhon; Jakub Safarik; Miroslav Voznak; Zuzana Bajakova. Analysis of the IP telephony security issues using automatic neural network classifier. Published in: 2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM). Publisher: IEEE, 2016. R. 75-84.
7. Olifer, V.G. Bezopasnost kompyuternyh setej / V. G. Olifer, N. A. Olifer. - M. : Goryachaya liniya-Telekom, 2017. - 644 s.
8. Cisco IP Phone 7800 and 8800 Series Security Overview. Cisco public, 2017. 10 p.
9. Hazem El M Bakry, Ali Taki El E Deen and Ahmed Hussein El Tengy. Implementation of an Encryption Scheme for Voice Calls. International Journal of Computer Applications 144(2), June 2016. P. 1-4.
10. Kochubinskyi A. Alhorytm vstanovlennia spilnoho sekretnoho znachennia, shcho gruntuietsia na eliptychnykh kryvykh / Anatolii Kochubinskyi, Volodymyr Syniavskyi, Oleksandr Shatalov. // Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini. – 2014. –Vyp. 2 (28). – S. 54-64.
11. Zastosuvannia nerozkryvnykh shyfriv dlia ubezpechennia VOIP-telefonii / N.I. Alishov, S.V. Zinchenko, A.N. Alishov, N.O. Sapunova // Systemy upravlinnia, navihatsii ta zviazku. – 2017. – Vypusk 1(41). – S. 3-7.
12. Osnovy programmno-apparatnoj zashity informacii. / M. A. Borisov, I. V. Zavodcev, I. V. Chizhov. – M.: URSS: Librokom, 2013. – 370 s.
13. Shangin, V. F. Informacionnaya bezopasnost i zashita informacii / V.F. Shangin. - M. : DMK Press, 2017. - 702 s.
14. Dzhulii, V.M. Model nelehitymnoho abonenta zabezpechennia bezpeky IP-telefonii / O.S. Androshchuk, V.M. Dzhulii, Yu.P. Klots, I.V. Muliar // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. – Khmelnytskyi, 2020. – №2. – Pp. 38–45.