УДК 004.891

к.т.н. **Джулій А.В.** (УЕП, м.Хмельницький)
к.т.н., доц. **Чорненький В.І.** (УЕП, м.Хмельницький)

DOI: https://doi.org/10.17721/2519-481X/2021/73-09

МЕТОД ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОТОКОЛУ РОЗПОДІЛЕННЯ КЛЮЧІВ БЕЗПЕЧНОЇ IP-ТЕЛЕФОНІЇ НА ОСНОВІ АЛГОРИТМУ ДІФФІ – ХЕЛМАНА

У роботі запропоновано метод підвищення ефективності протоколу розподілення ключів безпечної Ip-телефонії на основі алгоритму Діффі – Хелмана, 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.

Вирішує наступні задачі: надає можливість виявити активного нелегітимного кореспондента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного кореспондента IP - протоколів в каналах зв'язку Інтернет-телефонії при відсутності попередньо розподіленої секретної ключової інформації між кореспондентами, довіреного центру. Результати проведеного 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. Найбільш небезпечною атакою є атака типу «зустріч по середині» на IP -протоколи розподілу загальної секретної інформації. Завдання формування загальної секретної інформації в умовах проведення атаки типу «зустріч по середині» вторгнення нелегітимного кореспондента на сучасному етапу є актуальною. 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. Знаючи вразливості та рівень захищеності об'єкта, для якого необхідно провести захист, активний нелегітимний кореспондент може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об'єкта.

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.

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

Вступ. Поширення IP-телефонії через Internet мережі поставило під загрозу прибутки операторів телефонних мереж. Проте, оператори AT&T, British Telecomunications, Deutsche Telecom, починають надавати послуги Internet-телефонії. 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.

Поширенню IP-телефонії в Україні перешкоджає декілька факторів: недостатньо надійна інфраструктура Internet мереж каналів зв‘язку; організації, які забезпечують телефонні мережі послугами зв‘язку, не зацікавлені в розвитку IP-телефонії. Лише кілька провайдерів надають послуги IP-телефонії - Infocom, IP Telecom, Sovam Teleport.

Перевагою Internet-телефонії є низька вартість міжміських і міжнародних переговорів, дозволяє зменшити витрати на послуги передачі факсів і мультимедіа зв'язку, за рахунок шифрування і стиснення голосового потоку.

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 Імереж, а також криптографічного захисту даних для забезпечення безпечної Internet-телефонії. 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 трафіка.

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

Постановка задачі. 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 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. 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 зв’язку.

Наявність двох і більше каналів у одного абонента на сьогодні досить поширене явище. 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.

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.

Основна частина. Для забезпечення підвищення надійності та безпеки Інтернет мереж IP -телефонії 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. 1) і при цьому виявляти активного нелегітимного абонента.

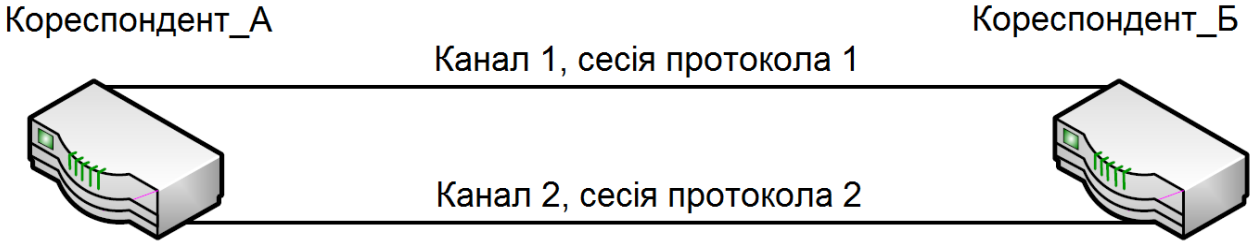

Рисунок 1 - Використання каналів зв'язку для обміну ключами

Для успішної реалізації роботи IP - протоколу ZRTP за декілька 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 TCP/UDP 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 мережі. Таким чином, реалізація перевірки роботи алгоритму обміну ключами Діффі-Хелмана по декільком каналах зв'язку в залежності від отриманих результатів 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. 2.

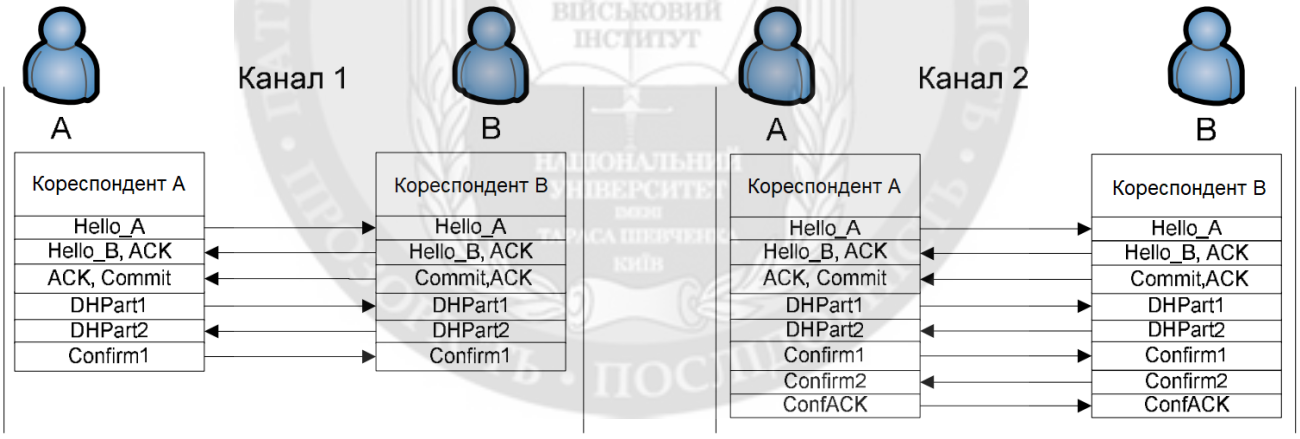

Рисунок 2- Взаємодія абонентів Інтернет мережі IP – телефонії при використанні модифікованого протоколу ZRTP

Розглянемо ймовірність захоплення обладнання оператора $P_{НСДЦ_{ЗАХОБЛ\_2}}$, яка визначає що нелегітимний абонент може виконувати активну атаку типу «зустріч по середині» в одному з двох каналів зв'язку Інтернет мережі IP -телефонії. 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 (виявлення атаки, успішної атаки «зустріч по середині», успішного розподілу секретної інформації): $P_{BA\_ЗС}$ $P_{УA\_ЗС}$ $P_{У\_СК}$. Активна атака називається успішної, якщо 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 компрометуючий 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 $P_{NO\_НА}$:

$$P_{NO\_НА} = 1 - P_{НСВА} \quad \text{тоді:} \quad P_{УК2} = P_{NO\_НА}{}^2 = (1 - P_{НСВА})^2.$$

Розглянемо варіант виявлення нелегітимного абонента з використанням трьох каналів зв'язку IP – телефонії. 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. 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.

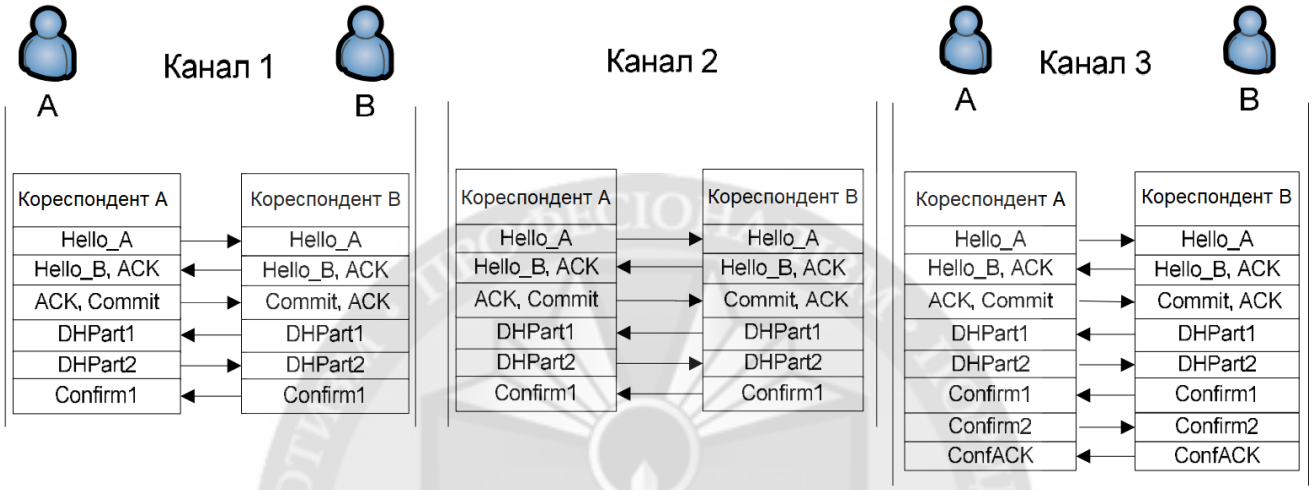

Рисунок 3 - Взаємодія кореспондентів при роботі одночасно по трьох каналах зв'язку

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 (З-ВНА); ВКНА: режим роботи з виключенням нелегітимного абонента (З-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.

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.

ЛІТЕРАТУРА:

1. Джулій, В.М. Модель нелегітимного абонента забезпечення безпеки IP-телефонії / О.С. Андрощук, В.М. Джулій, Ю.П. Кльоц, І.В. Муляр // Вимірювальна та обчислювальна техніка в технологічних процесах. – Хмельницький, 2020. – №2. – С. 38–45.

2. Бабаш, А.В. Криптографические методы защиты информации: учебник для студетнов вузов / А. В. Бабаш, Є. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

3. Борисов, М.А. Основы для программно-аппаратной защиты информации: учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., переработаное и доп. - М. : ЛЕНАНД, 2016. - 416 с.

4. Васильева, И. И. Криптографические методы защиты информации: практикум и учебник для академ. бакалавриата / И. И. Васильева. - Санкт-Петерб. гос. эконом. университет. - М. : Юрайт, 2017. - 349 с.

5. Нестеров, С.А. Основы информационной безопасности: учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

6. Олифер, В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия-Телеком, 2017. - 644 с.

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

8. Касперский, Е. В. «Компьютерное зловредство» / Е. В. Касперский. – Санкт-петербург: Питер, 2009. – 208 с.

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

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

11. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.

REFERENCES:

1. 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.

2. Babash, A.V. and Baranova, Ye. K. (2016), “Kryptohrafycheskye metodы zashchytы ynformatsyy : uchebnyk dlia studetnov vuzov” / M. : KNORUS, 190 p.

3. Borysov, M.A., Zavodtsev, Y.V. and Chyzhov Y.V.(2016), “Osnovы dlia prohrammno-apparatnoi zashchytы ynformatsyy : ucheb. posobye dlia vuzov” / M. : LENAND, 416 p.

4. Vasyleva, Y.Y. (2017),_”Kryptohrafycheskye metodы zashchytы ynformatsyy : praktykum y uchebnyk dlia akadem. Bakalavryata” / M. : Yurait, 349 p.

5. Nesterov, S.A. (2017), “Osnovы ynformatsyonnoi bezopasnosty : uchebnyk” / SPb. : Lan, 423 p.

6. Olyfer, V.H. and Olyfer, N. A. (2017), “Bezopasnost kompiuternыkh setei” / M. : Horiachaia lynyia-Telekom, 644 p.

7.. Borisov, M. A., Zavodcev, I. V. and CHizhov, I. V. (2013), ”Osnovy programmno-apparatnoj zashchity informacii” / M.: URSS: Librokom,. 370 p.

8. Kasperskij, E. V. (2009), ”Komp'yuternoe zlovredstvo”, Sankt-peterburg: Piter,. 208 p.

9. Partyka, T. L. and Popov, I. I. (2011), ”Informacionnaya bezopasnost' uchebnoe posobie” / M.: FORUM, 432 p.

10. Serdyuk, V. A. (2011), ”Organizaciya i tekhnologii zashchity informacii ” / M.: Izdatel'skij dom Gosudarstvennogo universiteta – Vysshej shkoly ekonomiki,. 571 p.

11. SHan'gin, V. F. (2017), ”Ynformatsyonnaia bezopasnost y zashchyta ynformatsyy” / M.: DMK Press, 702 p.

PhD Dzhulij A.V., PhD Chornenky V.I.

METHOD OF IMPROVING THE EFFICIENCY OF THE SAFE IR-TELEPHONY KEY DISTRIBUTION PROCEDURE BASED ON THE DIFFY-HELMAN ALGORITHM

The paper proposes a method to improve the efficiency of the secure IP-telephony key distribution protocol based on the Diffie-Hellman algorithm, which differs from the existing method for detecting an illegitimate subscriber by introducing an automated software and hardware verification of the authentication string. If several communication channels are used in this case, an appropriate check will reveal an illegitimate subscriber. Solves the following tasks: makes it possible to identify an active illegitimate correspondent using voice synthesis software; to identify an active illegitimate correspondent of IP - protocols in the communication channels of Internet telephony in the absence of previously distributed secret key information between the correspondents of the trusted center. The results of the study allow us to indicate that the most well-known IP-protocols for the distribution of general secret information need to be improved in two directions: increasing the information security of IP-telephony and improving the main indicators of IP-protocols of Internet networks. The most dangerous attack is a meeting-in-the-middle attack on IP protocols for the distribution of shared secret information. The task of forming general secret information in the context of a "meeting in the middle" attack of an illegitimate correspondent's invasion is relevant at the present stage. One of the methods to improve the security of the IP protocol for the formation of general secret information is to monitor and prohibit the execution of an attack of the "meeting in the middle" type due to the use of several parallel independent channels of communication sessions in the Internet IP - telephony networks. Knowing the vulnerability and the level of protection of the object for which it is necessary to carry out protection, an active illegitimate correspondent can perform a combination of attacks that can lead to gaining unauthorized access to the object's data.

A method for identifying an active illegitimate IP subscriber is proposed - protocols for the distribution of shared secret information based on the Diffie-Hellman key exchange algorithm, the feature of the method is the use of several open communication channels. Provides a decrease in the likelihood of a successful "meeting in the middle" attack by an active illegitimate subscriber, as well as the presence of a mechanism for identifying an active attacker in the communication channel in the absence of previously distributed shared secret information. The method imposes restrictions on the communication channels used, in the sense that the communication channels must be independent.

Key words: illegitimate correspondent, information interaction, Internet telephony, cryptographic protection, communication channels, key distribution.