УДК 004.891

к.т.н., доц**. Джулій В.М.** (ХмНУ)
к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н. **Степаненко Є.О.** (ЗСУ)
к.пед.н., доц. **Толок І.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2021/72-06

ІМОВІРНІСНА МОДЕЛЬ НЕЛЕГІТИМНОГО КОРЕСПОНДЕНТА ДРУГОГО РІВНЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ IP-ТЕЛЕФОНІЇ

В роботі запропонована імовірнісна модель виявлення нелегітимного кореспондента другого рівня на основі алгоритму Діффі-Хелмана. 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. Модель нелегітимного кореспондента може використовуватися при оцінці методів контролю рівня захищенності потоку даних з пакетною комутацією в Інтернет-телефонії, що надасть можливість забезпечення надійності IP-телефонії та підвищення захищенності.

Запропонована модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників. Модель нелегітимного кореспондента другого рівня враховує нелегітимних кореспондентів які не мають відповідного рівня доступу до сервісів безпечної IP-телефонії. До нелегітимних кореспондентів можуть в даному випадку бути віднесені: сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури. Визначені цілі нелегітимних абонентів другого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії: захоплення обладнання оператора; захоплення монітору абонента. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних 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 відслідкування і заборона виконання атаки типу «зустріч по середині» за рахунок використання в Інтернет мережах IP - телефонії декількох паралельних незалежних каналів сеансів зв'язку.

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

Вступ. Забезпечення підвищення ефективності та безпеки всіх галузей на сьогодні є однією з ключових проблем, тому актуальним сьогодення є необхідність впровадження і розвитку сучасних інформаційних технологій. 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. Великі корпоративні компанії

найбільш інтенсивно використовують IP-телефонію на основі локальних мереж. 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. Internet-телефонія не використовує дороге устаткування на шляху передачі інформації пакетів з голосовим сигналом.

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 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, 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.

Поширенню IP-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.

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. Таким чином ключ шифрування в даній схемі може бути відкритим, при цьому без втрати стійкості зашифрованого повідомлення, ключ дешифрування одержувачем повинен триматися в секреті. 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 (рис.1).

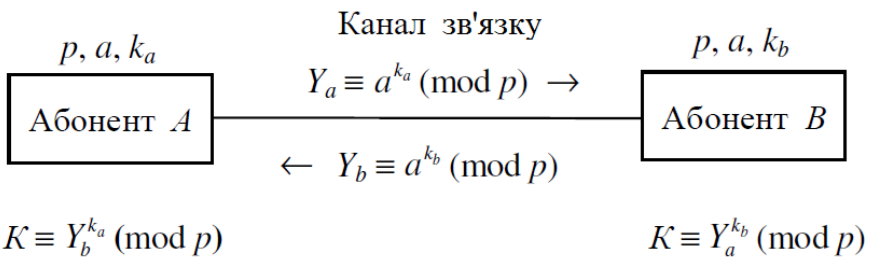

Рисунок 1 – Модель криптосистеми обміну ключами Діффі-Хеллмана

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. 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 кореспондента, яка буде враховувати атаку "зустріч посередині".

Основна частина. При розробці уточненої модель нелегітимного кореспондента більш доцільно розглядати зловмисників з точки зору рівня їх можливостей, а також наявності прав несанкціонованого доступу до інформації, одноразового чи постійного. Модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників. До першого рівня віднесемо нелегітимних операторів які мають відповідний рівень доступу до сервісів безпечної IP–телефонії [1]. До другого рівня віднесемо нелегітимних кореспондентів які не мають відповідного рівня доступу до сервісів безпечної IP - телефонії.

Нелегітимними кореспондентами (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 [1].

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

Визначимо цілі нелегітимних кореспондентів другого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP-телефонії: $Ц_{ЗАХОБЛ\_2}$ - захоплення обладнання оператора нелегітимним кореспондентом 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 кореспондентів розробимо модель другого рівня по кожній з перерахованих цілей.

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

Алгоритм дій нелегітимного кореспондента другого рівня наведено на рис. 2. Для виконання початку атаки, нелегітимний кореспондент другого рівня повинен визначитися на який сервіс IP-телефонії буде здійснювати активну атаку. Одним із можливих варіантів - отримання необхідної інформації, використання команди tracert, результатом виконання команди є проміжні вузли між нелегітимним кореспондентом і об’єктом атаки. Таким чином, з великою ймовірністю, можна вказати що ці вузли будуть задіяні в сеансі обміну пакетами даних між двома абонентами.

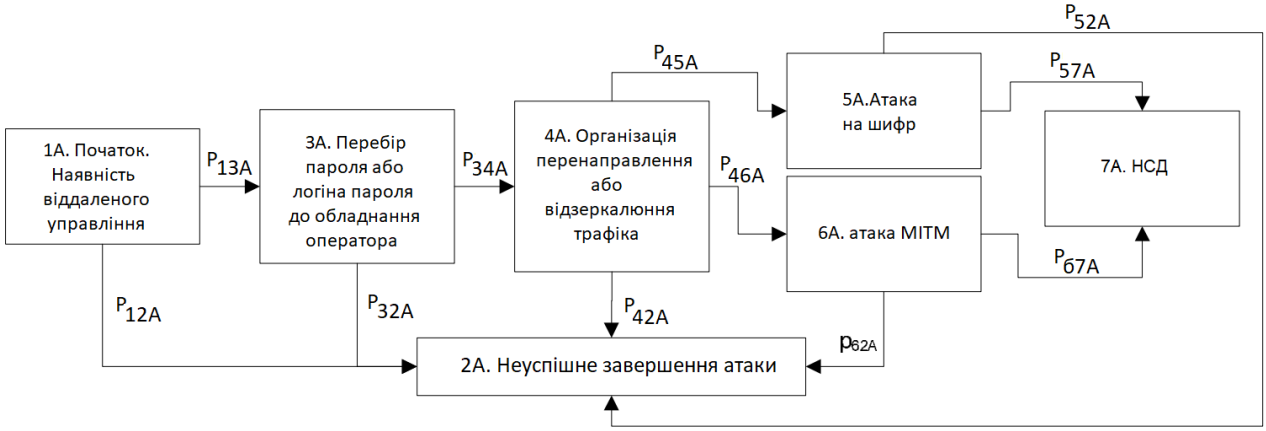

Рисунок 2 - Алгоритм дій при виконанні захоплення обладнання оператора нелегітимним кореспондентом другого рівня

Після вибору сервіса IP-телефонії – атаки, нелегітимним кореспондентом буде спроба захопити управління даним 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 кореспондента з використанням списків доступу ACL. Імовірності: p_{12} -ймовірність проведення активної атаки при наявності віддаленого відключення до сервісів IP-телефонії з боку нелегітимного кореспондента, або у оператора встановлені ACL; p_{13} - ймовірність проведення активної атаки при наявності віддаленого підключення до сервісів IP – телефонії, подія, зворотна p_{12}.

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

$$p_{34_{ЗАХОБЛ\_2}} = f(l,t,d,c), \quad (1)$$

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 кореспондента; c - швидкість каналу зв'язку Інтернет мережі IP - телефонії, під час виконання атаки.

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

У разі успішного захоплення нелегітимним кореспондентом віддаленого управління сервісами IP – телефонії, зловмисник може отримати несанкціонований доступ до потоку даних IP – телефонії використовуючи при цьому один з двох наступних шляхів: може виконати перебір пароля до переданого по Інтернет мережі медіа трафіка і виконувати прослуховування потоку даних IP - технології, або виконати атаку на механізм програмного розподілу загальної секретної інформації і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації. Однак, успішне виконання розглянутих атак нелегітимним кореспондентом 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 кореспондента через своє обладнання.

Імовірність успішної атаки нелегітимним кореспондентом на медіа трафік з метою отримання НСД до потоку даних можна визначити за наступною формулою:

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

Під активною атакою нелегітимним кореспондентом, мається на увазі, зміна маршруту потоку даних передачі пакетів мультимедійних файлів, що дозволять нелегітимному абоненту пропускати трафік кореспондента через своє обладнання.

При цьому ймовірності відображають: p_{45} - ймовірність, що нелегітимний кореспондент почав виконувати підбір пароля до переданого по Інтернет мережі медіа трафіка; p_{46} - ймовірність, що нелегітимний кореспондент почав виконувати атаку на механізм програмного розподілу загальної секретної інформації на IP - телефонію. Імовірність p_{57} - означає успішну атаку нелегітимного кореспондента на підбір пароля до переданого по Інтернет мережі медіа трафіка. В даному випадку нелегітимному кореспонденту стає доступно виконувати прослуховування потоку даних IP - технології, або виконати атаку на механізм програмного розподілу загальної секретної інформації і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації. Імовірність p_{52} відображає неуспішне закінчення атаки нелегітимного кореспондента на підбір пароля до переданого по Інтернет мережі медіа трафіка по підбору пароля за обмежений час. $T_{ЗЛВ\_АКТ}$ - час протягом якого дані актуальні – залежить від призначення даних. $T_{ЗЛВ\_ПРЛ}$ - час, необхідний на підбір пароля, залежить від рівня технічних потужностей нелегітимного кореспондента - $ЗЛВ_{ПТ}$, які застосовуються для захисту мультимедійних файлів криптографічних примітивів і криптоалгоритмів - $ЗЛВ_{КР}$, довжини ключа - $ЗЛВ_L$, а також від ускладнюючих елементів - $ЗЛВ_Д$.

$$p_{57}=f\left(T_{ЗЛВ\_АКТ}, T_{ЗЛВ\_ПРЛ}\right)=f\left(T_{ЗЛВ\_АКТ}, ЗЛВ_{ПТ}, ЗЛВ_{КР}, ЗЛВ_L, ЗЛВ_Д\right) \quad (2)$$

$$p_{52}=1-p_{57} \quad (3)$$

Імовірність p_{67} визначає успішну атаку на механізм програмного розподілу загальної секретної інформації і при цьому виконувати дешифрування трафіка з використанням отриманої секретної інформації на механізм розподілу ключів. Під атакою в даній ситуації будемо розуміти вторгнення нелегітимного кореспондента в канал зв'язку потоку даних IP-телефонії в момент обміну секретною інформацією між абонентами сесії IP - телефонії. Таким чином, це дозволить нелегітимному кореспонденту виробити два секретних ключа – для обміну інформацією з кожним кореспондентом незалежно один від одного. Тим самим, 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 потужностей використовуваних нелегітимним кореспондентом програмно-апаратних та технічних засобів 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 кореспондентом необхідна розробка відповідного програмного забезпечення. Імовірність p_{62} відображає неуспішне виконання активної атаки типу «зустріч по середині» нелегітимним кореспондентом і визначається як:

$$p_{62}=1-p_{67}. \quad (4)$$

Для проведення дослідження та аналізу алгоритму поведінки дій нелегітимного кореспондента при виконання активної атаки типу «зустріч по середині» використовується відповідний математичний апарат теорії імовірнісних графів, дозволяє оцінити даний алгоритм та визначити середній час необхідний для успішного виконання і ймовірність успішного завершення проведеної атаки. На рис. 3 представлений імовірнісний граф який описує алгоритм поведінки дій нелегітимного кореспондента 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 утворююча функція. У наведеному імовірнісному графі виділена гілка, яка відповідає успішному виконанню атаки метою якої є отримання НСД до потоку даних IP - телефонії і складена утворююча функція $H(x)$ цієї гілки. Для імовірнісного графа показаного на рис. 3 представлені $P_{НСД} = H(x=1)$:

$$P_{НСДЦ} = p_{13}p_{34}\left(p_{45}p_{57} + p_{46}p_{67}\right), \tag{5}$$

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

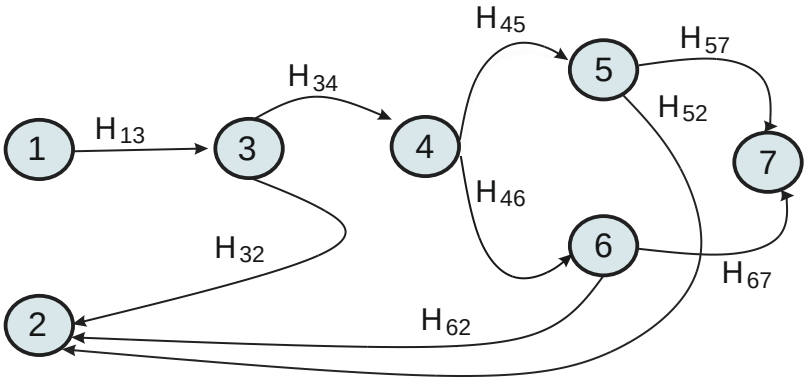

Рисунок 3 - Імовірнісний граф дій при виконанні захоплення обладнання оператора нелегітимним кореспондентом другого рівня

Розглянемо модель нелегітимного кореспондента, 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 кореспондента наведено на рис. 4. На основі отриманих результатів, можливих дій нелегітимним кореспондентом, більш детально розглянуті атаки які може виконати зловмисник, в залежності від доступу до шлюзу чи персонального комп'ютера кореспондента. При доступу до шлюзу нелегітимного кореспондента найбільш вірогідною є проведення активної атаки з проксінга всього трафіка з використанням обладнання зловмисником. Атака виконується за схемою, представленою на рис. 4, на схемі показані IPI, IP2 - шлюзи кореспондента, а S_H - сервер нелегітимного кореспондента з встановленим на ньому спеціалізованого програмного забезпечення.

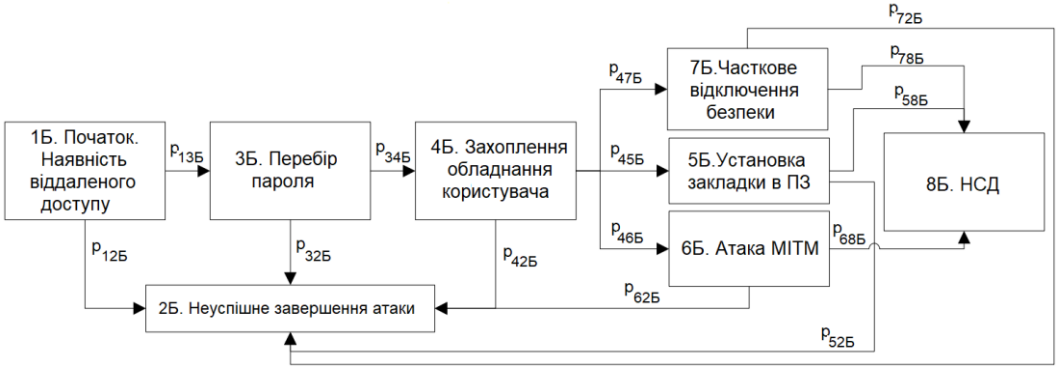

Рисунок 4 - Алгоритм дій при виконанні захоплення монітора кореспондента нелегітимним кореспондентом другого рівня

Для успішного проведення даної атаки нелегітимному абоненту необхідно отримати в першу чергу доступ до монітора кореспондента, захопити управління VoIP монітором і встановити відповідне спеціалізоване програмне забезпечення та виконати дії по його налаштуванню. Наприклад, якщо у кореспондента на VoIP моніторі, в режимі точка-точка, в відповідному запису в телефонній книжці шлюзу зберігаються IP-адреса IP – телефонії, то нелегітимний кореспондент в стані підмінити IP - адресу на VoIP моніторі кореспондента *Б* в записнику на VoIP моніторі кореспондента *А* на свою - IP-адресу, в результаті виконаних дій дзвінки з телефону кореспондента *А* будуть приходити на сервер нелегітимного кореспондента - S_H. Таким чином в даній ситуації - сервер нелегітимного кореспондента буде виконувати взаємозв'язок через IP - протоколи IP – телефонії між власним сервером і кореспондентом *Б* від імені іншого абонента мережі IP- телефонії - кореспондента *А*. IP-протоколи безпеки Інтернет мережі також будуть виконуватися IP – технологією між кореспондентами *Б* і сервером нелегітимного кореспондента. В результаті виконаних дій нелегітимний кореспондент отримує доступ до всього потоку даних (інформації), яка буде передаватися між кореспондентами *А* і *Б*, у відкритому доступі і при необхідності може модифікуватися нелегітимним кореспондентом а також прослуховуватися. Перенаправлення потоку даних IP- телефонії від кореспондента *А* на сервер нелегітимного кореспондента S_H можна здійснювати не тільки за рахунок підміни IP - адреси на VoIP моніторі, а також і за рахунок зміни налаштувань на шлюзі кореспондента *А*, встановивши адресу сервера нелегітимного кореспондента S_H в якості проксі-сервера або в якості основного сервера Інтернет мережі IP-телефонії.

Рисунок 5 - Атака з проксінг при виконанні захоплення монітора
а) виконання розподілу загальної секретної інформації,
б) встановлений захищений канал голосової інформації

При використанні VoIP монітора нелегітимним кореспондентом на якому встановлений програмний шлюз IP-телефонії найбільш вірогідним здійсненням активної атаки є: атака з проксінг всього потоку даних медіа трафіка 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 голосову 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 кореспондента S_H для подальшої відповідної обробки. Окрім цього, для доступу до потоку голосової інформації, яка передається на сервер нелегітимного кореспондента 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.

Таким чином, для успішного проведення активної атаки нелегітимним кореспондентом, 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, також рівня потужності спеціалізованого програмного забезпечення та механізмів взлому нелегітимного кореспондента. Таким чином імовірність успішного проведення атаки представимо наступним чином:

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

У випадку наявності сервісів захищеної IP-телефонії віддаленого управління, нелегітимному кореспонденту для успішного проведення активної атаки необхідно з використанням спеціалізованого програмного забезпечення підібрати пароль для авторизації на VoIP моніторі кореспондента. При цьому вводиться допущення, що IP-адреса об'єкта активної атаки відома нелегітимному кореспонденту і отримана заздалегідь. Підбір пароля залежить від IP – протоколу, рівня захищеності IP-телефонії віддаленого управління, на який виконується активна атака нелегітимного кореспондента. 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:

$$p_{45_{ЗАХМОН\_2}} = f\left(l, T, D, C\right), \tag{6}$$

де l - довжина 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 кореспондента; C - швидкість каналу зв'язку Інтернет мережі IP - телефонії, під час виконання атаки.

У разі успішного перебору пароля і отримання доступу до VoIP монітору кореспондента, захоплення нелегітимним кореспондентом віддаленого управління сервісами IP – телефонії, зловмисник може отримати НСД до потоку даних IP – телефонії використовуючи при цьому один з двох наступних шляхів: установка закладки в спеціалізоване програмне забезпечення кореспондента, модифікація програмного забезпечення VoIP монітора; коригування налаштувань VoIP монітора кореспондента; здійснення атаки типу «зустріч по середині» на всі протоколів захищеної IP-телефонії. Можливість проведення відповідної атаки визначається рівнем забезпечення програмно – апаратними, технічними засобами та механізмами нелегітимного кореспондента, а також наявністю в нелегітимного кореспондента спеціалізованих інструментів і засобів.

Сутність першої атаки нелегітимним кореспондентом полягає в захопленні голосової інформації в обхід IP - протоколів IP-телефонії: в відключенні IP - протоколів Інтернет мережі захищеної IP-телефонії; в зміні режимів роботи IP - протоколів Інтернет мережі захищеної IP-телефонії, для виконання нелегітимним кореспондентом прослуховування голосової інформації (медіа трафіка). Сутність другої і третьої атаки полягає в корегуванні налаштувань VoIP монітора кореспондента IP-телефонії для реалізації атаки типу «зустріч по середині», при якій весь потік даних IP - протоколів Інтернет мережі захищеної IP-телефонії проходять через нелегітимного кореспондента, 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 кореспондент, виконує сценарій з'єднання по черзі з кожним з кореспондентів, при цьому використовує IP - протоколи безпеки Інтернет мережі захищеної IP-телефонії, відповідно до представленої схеми (рис. 6).

Вибравши один з варіантів здійснення атаки, нелегітимний абонент, після успішного завершення, в змозі отримати несанкціонований доступ до потоку даних IP - телефонії. Однак, при цьому існує ймовірність неуспішного виконання вибраного варіанта здійснення атаки, яка в даному випадку буде відображається ймовірностями p_{72} і p_{62} відповідно.

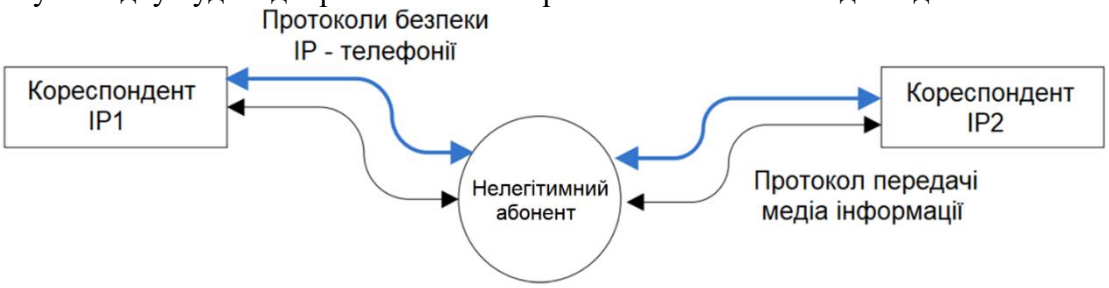

Рисунок 6 - Реалізація атаки «зустріч посередині»
для IP - протоколів забезпечення безпеки VoIP-моніторів

Наприклад, атака типу "модифікація налаштувань VoIP-монітора кореспондента" може також закінчитися не успішно, 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 нелегітимним кореспондентом, побудований відповідний імовірнісний граф (рис. 7).

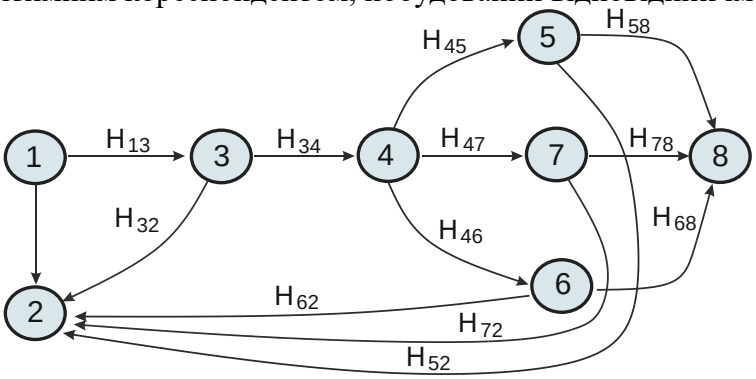

Рисунок 7 - Імовірнісний граф дій при виконанні захоплення VoIP-монітора нелегітимним кореспондентом другого рівня

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. 7 представлені $P_{НСД} = H(x=1)$:

$$P_{НСДЦ_{ЗАХМОН\_2}} = p_{13}p_{34}\left(p_{45}p_{58} + p_{46}p_{68} + p_{47}p_{78}\right), \quad (7)$$

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

Для кожного з розглянутих імовірнісних графів дій нелегітимним кореспондентом наведені $P_{НСД}$ [1]:

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

$$+\left(\left(p_{13}p_{34} + p_{18}p_{84}\right)p_{46} + p_{19} + p_{96}\right)p_{67}$$

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

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

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

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

$$P_{НСД} = \max\left\{P_{НСДЦ_{ЗАХОБЛ\_1}}, P_{НСДЦ_{ЗАХМОН\_1}}, P_{НСДЦ_{ЗАХОБЛ\_2}}, P_{НСДЦ_{ЗАХМОН\_2}}\right\}. \quad (8)$$

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, в даному випадку сам абонент є найбільш зацікавленою особою в приділенні більшої уваги для підвищення безпеки IP – телефонії і при цьому зниження $P_{НСД}$. Кореспонденти 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 нелегітимним кореспондентом можна виділити декілька часткових моделей нелегітимного абонента.

Також необхідно враховувати, що імовірності $p_{57\_ЗАХОБЛ\_1}$, $p_{57\_ЗАХОБЛ\_2}$ залежать від застосовуваного симетричного алгоритму шифрування [1].

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 кореспондента. Можна ввести припущення, 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:

$$P_{НСД} = \max\left\{P_{НСДЦ\_ЗАХОБЛ\_1}, P_{НСДЦ\_ЗАХОБЛ\_2}\right\}, \quad (9)$$

$$P_{НСДЦ_{ЗАХОБЛ\_2}} = p_{13\_ЗАХОБЛ\_2}p_{34\_ЗАХОБЛ\_2}p_{46\_ЗАХОБЛ\_2}p_{67\_ЗАХОБЛ\_2}\sqrt{b^2 - 4ac}, \quad (10)$$

$$P_{НСДЦ_{ЗАХОБЛ\_1}} = \left(\left(p_{13}p_{34} + p_{18}p_{84}\right)\cdot\cdot p_{46} + p_{19} + p_{96}\right)\cdot p_{67}. \quad (11)$$

Для дослідження імовірнісно-часових характеристик необхідно розглянути протоколи розподілу загальної секретної інформації захищеної IP-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; 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 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 табл. 1. 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. 1 не відповідає четвертій вимогі, 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 вимогі з таблиці 1, так як повідомлення 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.

Таблиця 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

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 вимогі $K_1 = 0$ 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 вимогі, 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. 1, можна дати рекомендації по вибору IP протоколів: протоколи ZRTP і DTLS, рекомендовані - мають найбільше значення $Q_{ПРК}$. Оцінка імовірнісно-часових характеристик виконується для вказаних IP –протоколів. 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.

Висновки. Запропонована модель нелегітимного кореспондента буде враховувати рівень можливостей зловмисників. Модель нелегітимного кореспондента другого рівня враховує нелегітимних кореспондентів які не мають відповідного рівня доступу до сервісів безпечної IP-телефонії. До нелегітимних кореспондентів можуть, в даному випадку, бути віднесені:

сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури.

Визначені цілі нелегітимних абонентів другого рівня при проведенні активної атаки з метою отримання несанкціонованого доступу до потоку даних IP - телефонії: $Ц_{ЗАХОБЛ}$ - захоплення обладнання оператора; $Ц_{ЗАХМОН}$ - захоплення монітора абонента. Кінцевою метою кожної активної атаки є отримання несанкціонованого доступу до потоку даних 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.

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 «атака 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.

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 нелегітимний кореспондент може виконувати комбінацію атак, яка може привести до отримання несанкціонованого доступу до даних об’єкта.

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.

12. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин. - М.: ДМК Пресс, 2012. – 576 с.

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

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

15. Рыжиков, Ю.И. Имитационное моделирование. Теория и технология. / Ю.И. Рыжиков - СПб: КОРОНА принт, 2015. - 384 с.

16. Советов, Б. Я. Моделирование систем : учебник для бакалавров / Б. Я. Советов, С. А. Яковлев. — 7-е изд. — М. : Издательство Юрайт, 2015. — 343 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.

12. SHan'gin, V.F. (2012), ”Zashchita informacii v komp'yuternyh sistemah i setyah.” / M.: DMK Press,. 576 p.

13. Goldshteyn, B.S. and Kucheryavy, A.E. (2014), ”Seti svyazi post-NGN”/ [Post-NGN communication networks] , SPb.:BHV-Peterburg, 160p.: il.

14. Olifer, V. G. and Olifer, N. A. (2017), ”Kompyuternyie seti. Printsipyi, tehnologii, protokolyi ” / [Computer networks. Principles, technologies, protocols], SPb.: Piter, 992p.

15. Ryizhikov, Yu.I. (2015), ”Imitatsionnoe modelirovanie. Teoriya i tehnologiya.” / [Imitation modeling. Theory and technology], SPb: KORONA print, 384p.

16. Sovetov, B. Ya. and Yakovlev, S.A. (2015), ”Modelirovanie sistem : uchebnik dlya bakalavrov” / [System modeling: a textbook for bachelors] ,7-e izd. M. : Izdatelstvo Yurayt, 343p.

PhD Dzhulij V.M., PhD Mulyar I.V., PhD Stepanenko Ye.O., PhD Tolok I.V.

PROBABILITY MODEL OF THE SECOND LEVEL CORRESPONDENT OF IP-TELEPHONY SECURITY

The paper proposes a probabilistic model for identifying an illegitimate second-level correspondent based on the Diffie-Hellman algorithm. Solves the following tasks: allows you to identify an active illegitimate correspondent who uses 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, the entrusted center. The model of an illegitimate correspondent can be used to assess methods for monitoring the security level of a packet-switched data stream in Internet telephony, which will ensure the reliability of IP telephony and increase security.

The proposed model of an illegitimate correspondent will take into account the level of the attackers' capabilities. The second-level illegitimate correspondent model takes into account illegitimate correspondents who do not have an appropriate level of access to secure IP-telephony services. In this case,

illegitimate correspondents may include: unauthorized persons; persons of foreign states; representatives of foreign intelligence services; terrorist and criminal structures.

The goals of illegitimate second-level subscribers in carrying out an active attack in order to obtain unauthorized access to the data stream of IP - telephony are determined: seizure of the operator's equipment; capture of the subscriber monitor. The ultimate goal of every active attack is to gain unauthorized access to the IP telephony data stream.

The results of the analysis and research make it possible 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.

One of the methods to improve the security of the IP protocol for the formation of shared secret information is to monitor and prohibit the execution of a meeting-in-the-middle attack through the use of several parallel independent channels of communication sessions in the Internet IP-telephony networks.

Key words: probabilistic model, illegitimate correspondent, information interaction, Internet telephony, cryptographic protection, communication channels.