

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ, АВТОМАТИЗАЦІЯ ТА ОБЧИСЛЮВАЛЬНА ТЕХНІКА В ТЕХНОЛОГІЧНИХ ПРОЦЕСАХ

УДК 004.891

DOI: 10.31891/2219-9365-2020-66-2-7

АНДРОЩУК О. С., ДЖУЛІЙ В. М.,
КЛЮЦЬ Ю. П., МУЛЯР І. В.
Хмельницький національний університет

МОДЕЛЬ НЕЛЕГІТИМНОГО АБОНЕНТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІР-ТЕЛЕФОНІЇ

У роботі запропонована імовірна модель виявлення нелегітимного абонента на основі алгоритму Діффі-Хелмана. Вирішує наступні задачі: надає можливість виявити активного нелегітимного абонента, який використовує програмне забезпечення синтезу голосу; визначити активного нелегітимного абонента ІР-протоколів в каналах зв'язку Інтернет-телефонії при відсутності попередньо розподіленої секретної ключової інформації між кореспондентами, довіреного центру. Модель нелегітимного абонента може використовуватися при оцінці методів контролю рівня захищеності потоку даних з пакетною комутацією в Інтернет-телефонії, що надасть можливість забезпечення надійності ІР-телефонії та підвищення захищеності.

Ключові слова: імовірна модель, нелегітимний абонент, інформаційна взаємодія, криптографічний захист, канали зв'язку.

ANDROSHCHUK O., DZHULIY V.,
KLOTS Y., MULYAR I.
Khmelnytsky National University

MODEL OF ILLEGAL SUBSCRIBER OF IP-TELEPHONY SECURITY PROVISION

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

An analysis of possible active successful attacks (threats) and a study to identify their possible sources. Knowing the vulnerabilities and security level of the object for which protection is required, an active illegitimate subscriber can perform a combination of attacks, which can lead to unauthorized access to the data of the object.

Based on the analysis of algorithms of behavior of illegitimate subscribers, a model of the violator is proposed, which will take into account the level of capabilities of violators. The model of an illegitimate subscriber takes into account illegitimate operators who have the appropriate level of access to secure IP-telephony services: employees of this organization; software developers or suppliers of technical means, employees who provide improvement, maintenance, repair of means at the object on which protection of information resources is necessary. The purposes of illegitimate subscribers at carrying out active attack for the purpose of receiving unauthorized access to a stream of data of IP-telephony are defined. The ultimate goal of each active attack is to gain unauthorized access to the IP telephony data stream.

The illegitimate subscriber model can be used to evaluate methods of controlling the level of security of packet-switched data streams in Internet telephony, which provide the ability to ensure the reliability of IP telephony and increase security.

Keywords: probabilistic model, illegitimate subscriber, information interaction, cryptographic protection, communication channels.

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

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

Постановка задачі. Проведені дослідження показують існування декілька моделей нелегітимного абонента в IP-телефонії в Інтернет мережах. Імовірнісна модель нелегітимного абонента показує які дії та з використанням якого інструменту проводить нелегітимний абонент атаки при експлуатації захищеної IP-телефонії в Інтернет мережах. Імовірнісна модель нелегітимного абонента проводить аналіз та враховує різновиди атак, а також враховує особливості та характер атак на операційну систему Windows, з врахуванням використання операційною системою засобів захисту. Імовірнісна модель нелегітимного абонента не враховує програмний розподіл загальної секретної інформації (закритих ключів), з використанням IP – протоколів рознесення ключів IP-телефонії в Інтернет мережах[3]. Розглянута імовірнісна модель використовує попередній розподіл секретної інформації, тобто завчасна установка секрету учасниками сеансу. При застосуванні імовірнісної моделі нелегітимного абонента для здійснення атаки, задача якої отримання несанкціонованого доступу до голосової інформації IP-технології в Інтернет мережах, вирішується тільки задача дешифрування переданого потоку даних при цьому використовується «атака в лоб» (метод перебору), вірогідність успішного завершення даної атаки достатньо низька при правильному виборі ключів сесії. Таким чином модифікація пакетів інформації можлива в разі успішної атаки, результатом якої є підбір пароля для реалізації процесу дешифрування перехоплених потоків даних.

Модель нелегітимного абонента наведена та описана в стандарті по питанням технічного та експортного контролю [1, 2]. У запропонованому стандарті наведений опис загальної моделі нелегітимного абонента. Описана в стандарті модель не враховує також особливостей роботи в Інтернет мережах захищеної IP-телефонії. Технологія IP-телефонії має в своєму розпорядженні в застосуванні IP – протоколи, які призначені для підвищення ефективності та забезпечення безпеки IP-телефонії, сюди можна віднести захист сигналізації, розподіл загальної секретної інформації між учасниками сеансу зв'язку, захист голосової інформації, при цьому не наведено інформації про здійснення атак на IP-протоколи IP-телефонії. В проведеному аналізі робіт [7] рекомендуються загальні вимоги, які ждуть бути запропонованими до мережі IP-телефонії в Інтернет мережах, також наводиться опис загальних характеристик та виконуваних дій при здійсненні атак на мережу IP-телефонії. Рівень описаних атак відповідає діям середньостатистичного хакера при проведенні атак на сервіси IP-телефонії. На основі проведеного дослідження та аналізу відповідних робіт можна зробити наступний висновок: в розглянутих роботах не наводиться декомпозиція IP-протоколів Інтернет мереж безпечної IP-телефонії на відповідні складові, також не наведено опис успішних атак на IP-протоколи Інтернет мереж які безпосередньо використовуються в безпечній IP-телефонії. В розглянутих роботах [6] використовуються та описуються загальні підходи та принципи забезпечення підвищення надійності та захисту сервісів IP-телефонії, а також загальні підходи та принципи можливих дій нелегітимного абонента при атаках на сервіси IP-телефонії. В роботах не приділяється належної уваги атакам на протоколи розподілу загальної секретної інформації між учасниками сеансу зв'язку, захисту голосової інформації, при цьому не приводиться інформації про здійснення атак на IP-протоколи використовуваних в IP-телефонії. Таким чином виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях нелегітимного абонента, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP-протоколів Інтернет-мереж, які використовуються безпечною IP-телефонією, запропонована модель має враховувати вказані особливості.

Основна частина. Моделі які описані в розглянутих роботах [1, 3] не дозволяють визначити імовірність успішної атаки на отримання несанкціонованого доступу до потоку даних в мережі захищеної IP-телефонії, яка працює в режимі за схемою точка – точка, також не надають механізмів виявлення та захисту від атак типу «зустріч по середині», розглянуті моделі не враховують даний тип атак. В запропоновану модель нелегітимного абонента необхідно включити додаткові механізми, такі як: виявлення імовірності успішної атаки на отримання несанкціонованого доступу до потоку даних захищеної IP-телефонії, яка працює в режимі за схемою точка – точка; також механізми виявлення та захисту від атак типу «зустріч по середині». Виникнення загроз в Інтернет мережах безпеки голосової інформації в IP-телефонії може проявитися в результаті виникнення додаткового каналу потоку інформації в Інтернет мережах між нелегітимним абонентом (джерелом загрози) і кореспондентом носієм інформації, при цьому необхідно створення відповідних умов, які сприяють для виникнення порушення захищеності та безпеки голосової інформації. Наскільки актуальна загроза порушення захищеності та безпеки голосової інформації буде оцінюватися, також, типом джерела загрози – рівнем атаки, рівнем захищеності джерела голосової інформації та наявністю вразливостей, а також рівнем захищеності середовища поширення голосового інформаційного сигналу.

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

Рівень впливу на закриті інформацію, яку необхідно захистити, визначається можливостями джерела загроз, наскільки джерело загроз володіє інформацією про сервіси захисту IP-телефонії, також рівень впливу на закриті інформацію визначається рівнем механізмів якими володіє джерело загроз. Джерело загроз, яке

здійснює дії (атаку) або займається підготовкою до дій (атаки) результатом яких є отримання несанкціонованого доступу до інформації з подальшим впливом на закриту інформацію є зловмисником інформаційної безпеки. В якості нелегітимного абонента будемо визначати фізичну особу, яка випадково чи не випадково здійснює дії (атаки) в своїх інтересах чи в інтересах даної організації, чи в інтересах інших організацій (можливо іноземних організацій) результатом яких є порушення захищеності та безпеки інформаційних ресурсів при її обробці програмно-апаратними, технічними та іншими сервісами в інформаційних системах.

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

Таким чином нелегітимними операторами (перший рівень) можуть в даному випадку можуть виступати: працівники даної організації; розробники програмного забезпечення або постачальники технічних засобів, працівники які забезпечують удосконалення, супровід, ремонт засобів на об'єкті, на якому необхідний захист інформаційних ресурсів. До нелегітимних абонентів (другий рівень) можуть в даному випадку бути віднесені: сторонні особи; особи іноземних держав; представники іноземних розвідувальних служб; терористичні і кримінальні структури.

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

Враховуючи те, що передача голосової інформації в Інтернет мережах безпечної IP-телефонії здійснюється з використанням загального доступу, а монітори VoIP практично доступні будь-якій сторонній особі, як і легальний доступ до Інтернет-мереж – таким чином на основі сказаного можливо зробити висновок про актуальність виникнення загроз віддаленого доступу і можливості їх реалізації нелегітимними абонентами, як першого так і другого рівнів.

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

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

Отже виникає необхідність розробки моделі нелегітимного абонента яка буде враховувати дії нелегітимного абонента, які були не враховані в розглянутих роботах, в існуючих моделях, в першу чергу виникає необхідність прийняти до уваги декомпозиція IP – протоколів Інтернет мереж, які використовуються безпечною IP-телефонії, модель повинна враховувати вказані особливості, мати механізми виявлення та захисту від атак типу «зустріч по середині». Для врахування в моделі вказаних недоліків розглянемо схему взаємодії кореспондентів захищеної IP-телефонії клієнт–клієнт, при відсутності попереднього програмного розподілення загального секретного матеріалу (закритого ключа сесії), і також розглянемо можливі варіанти дій нелегітимного абонента в схемі клієнт–клієнт (див. рис. 1).

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

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

При здійсненні активної атаки нелегітимним абонентом необхідно враховувати можливий рівень прав порушника, так порушник може знаходитися в одній підмережі з об'єктом на який направлена атака, в даному випадку може мати достатньо прав для виконання успішної атаки, в іншому випадку порушник

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

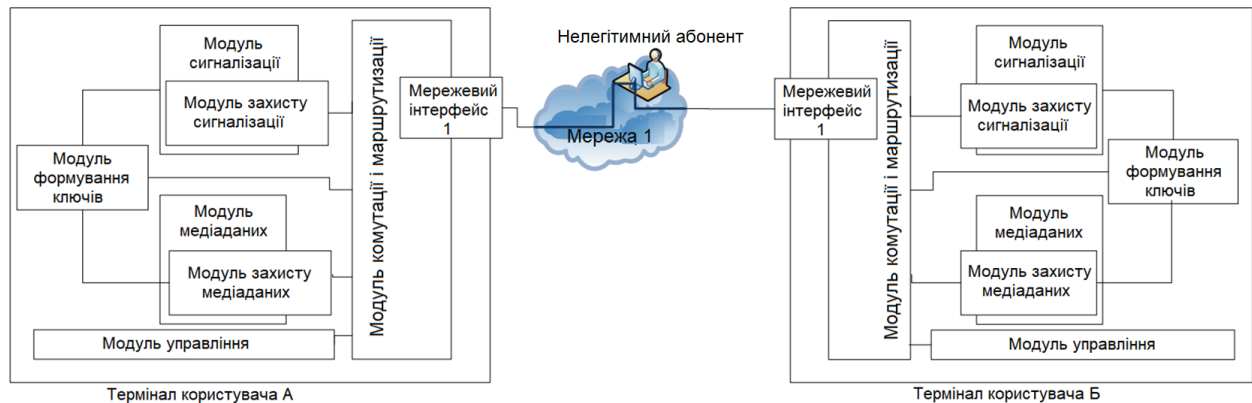


Рис. 1. Схема встановлення з'єднання в сценарії клієнт-клієнт

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

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

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

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

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

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

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

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

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

У випадку коли нелегітимний абонент не має достатнього рівня доступу на обладнання оператора, може спробувати отримати доступ, виконуючи атаку на перебір паролів для отримання більш високого рівня доступу до сервісів IP-телефонії. Алгоритм дій нелегітимного абонента першого рівня наведено на рис. 2. Імовірність $p_{18,34,40,67}$ характеризує ймовірність, що у нелегітимного абонента першого рівня на початку виконання активної атаки є доступ відповідного рівня достатній для проведення подальших дій з метою отримання несанкціонованого доступу до потоку даних IP-телефонії. Імовірність $p_{18,34,40,67}$ може бути визначена, наступним чином:

$$p_{18,34,40,67} = \begin{cases} 1, \text{якщо нелегітимний абонент має достатній рівень доступу;} \\ 0, \text{якщо нелегітимний абонент не має достатній рівень доступу.} \end{cases}$$

Імовірність $p_{19,34,40,67}$ відображає ймовірність події, у випадку коли нелегітимний абонент підключив своє необхідне обладнання в мережі оператора IP-телефонії на вузол, через який є доступ до даних (медіа-трафіку).

$$p_{19,34,40,67} = \begin{cases} 1, \text{якщо нелегітимний абонент зміг встановити своє обладнання} \\ \text{на вузлі оператора;} \\ 0, \text{якщо нелегітимний абонент не зміг встановити своє обладнання} \\ \text{на вузлі оператора.} \end{cases}$$

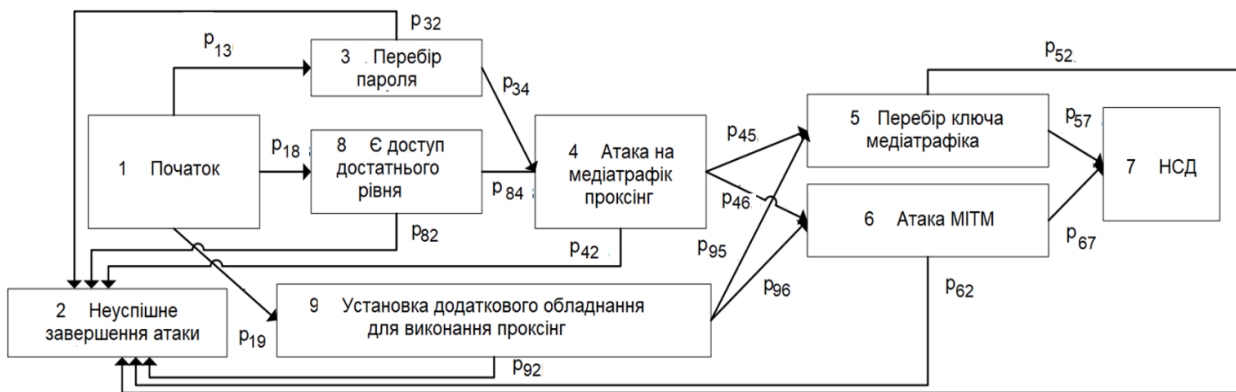


Рис. 2. Алгоритм дій при виконанні захоплення обладнання оператора нелегітимним абонентом

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

На основі отриманих результатів, які отримані проведенням аналізом, можливих дій нелегітимного абонента побудований відповідний ймовірнісний граф, представлений на рис. 3. У наведеному ймовірнісному 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 ймовірнісного графа показано на рис. 3 представлені $P_{НСД}$.

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

$$P_{НСДЦ,34,40,67} = ((p_{13}p_{34} + p_{18}p_{84})p_{45} + p_{19} + p_{95})p_{57} + ((p_{13}p_{34} + p_{18}p_{84})p_{46} + p_{19} + p_{96})p_{67},$$

де p_{ij} – ймовірність переходу з вершини i графа у вершину j .

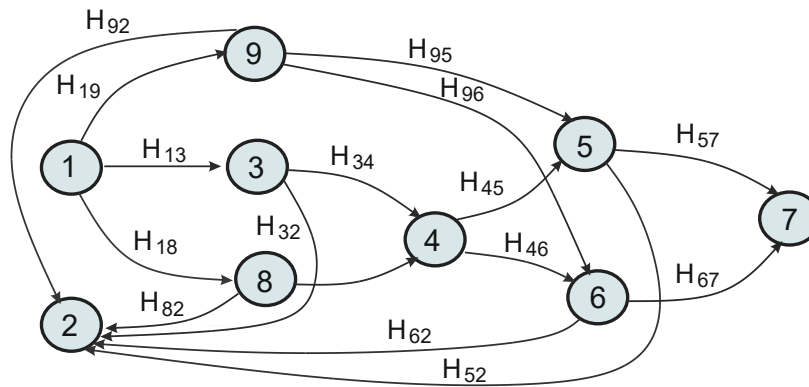


Рис. 3. Імовірнісний граф захоплення обладнання оператора нелегітимним абонентом першого рівня

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

$$P_{\text{ЗАХ_НСДЦ_ЗАХОБЛ}} = 1 - P_{\text{НСДЦ_ЗАХОБЛ}} = 1 - ((p_{13}p_{34} + p_{18}p_{84})p_{45} + p_{19} + p_{95})p_{57} + ((p_{13}p_{34} + p_{18}p_{84})p_{46} + p_{19} + p_{96})p_{67},$$

де p_{13} – ймовірність вибору активної атаки перебір пароля для доступу нелегітимного абонента до обладнання оператора IP-телефонії; p_{18} – ймовірність наявності в нелегітимного абонента успішного доступу достатнього рівня на обладнання оператора IP-телефонії; p_{19} – ймовірність наявності в нелегітимного абонента можливості установки необхідного обладнання для успішного виконання атаки; p_{34} – ймовірність для нелегітимного абонента успішного завершення атаки по перебору пароля для доступу до обладнання оператора IP – телефонії Інтернет мереж; p_{45} – ймовірність вибору атаки нелегітимним абонентом «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{46} – ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{57} – ймовірність успішного завершення нелегітимним абонентом активної атаки «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{67} – ймовірність успішного завершення атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів); p_{95} – ймовірність вибору атаки нелегітимним абонентом «злом шифру» для проведення дешифрування захищеного потоку даних IP-телефонії; p_{96} – ймовірність вибору атаки нелегітимним абонентом на механізм програмного розподілу секретної інформації (ключів) між учасниками сесії.

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

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

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

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

Література

1. Про науково-технічну інформацію : Закон України з 25.06.1993 № 3322-XII. Дата оновлення: 19.04.2014. URL: <http://zakon5.rada.gov.ua/laws/main/3322-12> (дата звернення: 02.09.2020).
2. Про захист інформації в інформаційно-телекомунікаційних системах : з Закону України від 05.07.1994 № 80/94-ВР. Дата оновлення: 04.07.2020. URL: <http://zakon5.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 02.09.2020).
3. Бабаш, А.В. Криптографические методы защиты информации : учебник для студетнов вузов / А. В. Бабаш, С. К. Баранова. - М. : КНОРУС, 2016. - 190 с.
4. 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.
5. Васильева, И. И. Криптографические методы защиты информации : практикум и учебник для академ. бакалавриата / И. И. Васильева. - Санкт-Петербург. гос. эконом. университет . - М. : Юрайт, 2017. - 349 с.
6. Нестеров, С.А. Основы информационной безопасности : учебник / С. А. Нестеров. - СПб. : Лань, 2017. - 423 с.
7. Олифер, В.Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия-Телеком, 2017. - 644 с.
8. Kim Peter. The Hacker Playbook 3: Practical Guide To Penetration Testing / Securety planet LLC 2018 359 p.
9. Шаньгин, В. Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М. : ДМК Пресс, 2017. - 702 с.

References

1. Pro naukovo-tehnichnu informatsiyu : Zakon Ukrayiny vid [About scientific and technical information : Law of Ukraine from] 25.06.1993 № 3322-XII. Data onovlennya: 19.04.2014. URL: <http://zakon5.rada.gov.ua/laws/main/3322-12> (data zvernennya: 02.09.2020).
2. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynnykh systemakh : Zakon Ukrayiny vid [On information protection in information and telecommunication systems : Law of Ukraine from] 05.07.1994 № 80/94-VR. Data onovlennya: 04.07.2020. URL: <http://zakon5.rada.gov.ua/laws/show/80/94-вр> (data zvernennya: 02.09.2020).
3. Babash, A.V. Kriptograficheskiye metody zashchyty ynformatsyy : uchebnyk dlia studetnov vuzov / A. V. Babash, Ye. K. Baranova. - M. : KNORUS, 2016. - 190 s.
4. Borysov, M.A. Osnovy dlia prohrammno-apparatnoi zashchyty ynformatsyy : ucheb. posobyie dlia vuzov / M. A. Borysov, Y. V. Zavodtsev, Y. V. Chyzhov. - 4-e yzd., pererabotanoie y dop. - M. : LENAND, 2016. - 416 s.
5. Vasyleva, Y. Y. Kriptograficheskiye metody zashchyty ynformatsyy : praktykum y uchebnyk dlia akadem. bakalavryata / Y. Y. Vasyleva. - Sankt-Peterb. hos. ekonom. unyversytet . - M. : Yurait, 2017. - 349 s.
6. Nesterov, S.A. Osnovy ynformatsyonnoi bezopasnosty : uchebnyk / S. A. Nesterov. - SPb. : Lan, 2017. - 423 s.
7. Olyfer, V.H. Bezopasnost kompiuternyykh setei / V. H. Olyfer, N. A. Olyfer. - M. : Horiachaia lynyia-Telekom, 2017. - 644 s.
8. Kim Peter. The Hacker Playbook 3: Practical Guide To Penetration Testing / Securety planet LLC 2018 359 p.
9. Shanhyn, V. F. Ynformatsyonnaia bezopasnost y zashchyta ynformatsyy / V.F. Shanhyn. - M. : DMK Press, 2017. - 702 s.

Надійшла / Paper received: 07.07.2020

Надрукована / Paper Printed : 02.12.2020