

Устенко С.В., д.е.н., професор,
Остапович Т.В., аспірант,
ДВНЗ «Київський національний економічний
Університет імені Вадима Гетьмана»

Ustenko S., Dr., Prof.,
Ostapovych T., post-graduate
SHEE «Kyiv National Economic University
named after Vadym Hetman»

АНАЛІЗ ТА ВИКОРИСТАННЯ ТЕХНОЛОГІЙ VoIP-ТЕЛЕФОНІЇ В БАНКІВСЬКИХ СИСТЕМАХ

THE ANALYSIS AND USAGE THE TECHNOLOGIES OF VoIP-TELEPHONES AT THE BANKING SYSTEMS

Анотація. Стаття присвячена використанню технологій VoIP-телефонії у банківських системах. VoIP — дослівно розшифровується як голосовий дзвінок за допомогою Інтернет протоколу. В статті розглянуто найпоширеніші Інтернет протоколи, які використовуються для здійснення дзвінка, висвітлено їхні недоліки та переваги. На простому прикладі пояснено принцип роботи VoIP-телефонії та технологій, які необхідні для здійснення дзвінка софтверно, білінгову систему, та здійснено короткий огляд тих ризиків та небезпек, які виникають під час здійснення телефонного дзвінка в мережі Інтернет. Також здійснено спробу в межах виділеної теми описати ті технології, які можна використати для захисту телефонного дзвінка в мережі Інтернет, зокрема мова йде про шифрування та автентифікацію, встановлення з'єднання за допомогою ключів. Для цього було здійснено аналіз принципів побудови та технологій використання VoIP-телефонії. Зокрема описано порівняння такої технології, та способи її практичного використання в банківській системі, як реалізація принципу єдиного інформаційного вікна для спрощення роботи оператора терміналу, збільшення надійності використання даних, так як відпадає потреба копіювати інформацію в межах різних інформаційних систем, тобто наголос робиться на тому, що створюється єдина система з єдиним потоком трафіку і як наслідок виникає можливість збільшити безпеку використання інформації. Єдине інформаційне вікно дає можливість створити фільтрацію адрес робочих станцій, що в свою чергу виключає використання несанкціонованих точок доступу до самої системи та запобігає витоку інформації. Крім цього було розглянуто впровадження цілісної системи VoIP-телефонії на прикладі роботи Публічного акціонерного товариства «Державний ощадний банк України». Надано структурні схеми реалізації VoIP-телефонії в роботі банківської системи та реалізації єдиного інформаційного вікна. Ключові слова: VoIP-телефонія, банківські системи, база знань, SIP, RADIUS.

Annotation. The article is devoted to the use of VoIP telephony technologies in banking systems. VoIP — literally stands for Voice over Internet Protocol. The article deals with the most common Internet protocols used to make a call, their shortcomings and advantages are highlighted. The simple explanation of the principle of VoIP-telephony and technologies required for making a call to the

wholesaler, billing system, and a brief overview of the risks and dangers that arise when making a phone call on the Internet is explained. It also attempts to describe, within the topic, the technologies that can be used to protect a telephone call on the Internet, in particular, encryption and authentication, and the establishment of a connection using keys. For this purpose, an analysis of the principles of construction and technologies for the use of VoIP telephony was carried out. In particular, a comparison of such technology and methods of its practical use in the banking system, such as the implementation of the principle of a single information window for simplifying the operation of the terminal operator, and increasing the reliability of the use of data is described, since there is no need to copy information within the various information systems, that is, the emphasis is on that creating a single system with a single stream of traffic and as a consequence there is an opportunity to increase the security of the use of information. The only information window allows you to create filtering addresses of workstations, which makes it possible to exclude the use of unauthorized access points to the system itself, and to prevent the leakage of information. An example of the implementation of the whole VoIP telephony system was described, for example, Public Joint Stock Company "State Savings Bank of Ukraine". Structural schemes for the implementation of VoIP telephony on the example of the banking system, and the implementation of a single information window are provided.

Key words: VoIP telephony, banking systems, knowledge base, SIP, RADIUS.

Постановка проблеми: Ризики використання інформаційно-комунікаційних систем у банківських системах безпосередньо пов'язані з недоліками які притаманні системам VoIP і є достатньо серйозною проблемою.

Аналіз досліджень і публікацій: Теоретичним і методологічним проблемам вивчення місця та ролі VoIP-телефонії у банківських системах присвячено багато праць [1–5]. Даній темі присвячено роботи науковців: Гольдштейн Б. С., Пінчук А. В., Суховицький А. Л. — "ІР-телефонія: Радіо і зв'язок", Глоба Л. С., Дяденко О. М., Чердинцева О. М. "Операторська платформа надання послуг"; Нопін С. В., Шахов В. Г. — "Аналіз захищеності абонентських систем ІР-телефонії від несанкціонованого доступу"; Дудикевич В.Б., Хорошко В.О., Микитин Г.В., Банах Р.І., Ребець А.І. — "Інформаційна модель безпеки технологій зв'язку.

Постановка завдання: На прикладі VoIP дослідити використання інформаційно-комунікаційних технологій у банківських системах.

Мета статті: аналіз і дослідження проблематики використання VoIP-телефонії у банківських системах.

Виклад основного матеріалу. Вступ. Використання мережі Інтернет у банківських системах не має обмежень, однак, проблема полягає лише в тому, який рівень захисту можна забезпечити за допомогою тієї чи іншої технології. У цій статті буде розглянуто систему передачі голосових повідомлень за допомогою мережі Інтернет або скорочено VoIP-телефонії, так як вона пов-

ністю витіснила з ринку всі інші подібні системи. Починаючи з 1993 року було відпрацьовано механізм, який використовується і сьогодні, зміни відбулися лише у способі використання та технологіях за допомогою яких було реалізовано це завдання. Сьогодні всі інші системи передачі голосових повідомлень уже не використовуються самі по собі, а є лише частиною, можна вже по праву сказати, світової системи VoIP.

VoIP (англ. voice over IP — голос через IP) — технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP. IP-телефонія — система зв'язку, в якій аналоговий звуковий сигнал абонента дискретизується (кодується в цифрову форму), компресується та пересилається цифровими каналами зв'язку до іншого абонента, де проводиться зворотна операція — декомпресія, декодування й відтворення аналогового сигналу [2]. Реалізована дана технологія за допомогою протоколів встановлення сесії та протоколів кодування і шифрування. До протоколів встановлення сесії можна віднести протоколи SIP і RADIUS.

SIP (англ. Session Initiation Protocol — протокол встановлення сесії) — протокол прикладного рівня, розроблений IETF MMUSIC Working Group і пропонує стандарт на спосіб установаки, зміни і завершення користувацького сеансу, що включає мультимедійні елементи, такі як відео або голос, миттєві повідомлення (instant messaging), он-лайн ігри та віртуальну реальність.

Протокол SIP почав розроблятися в 1996 році Хеннінгом Шульзрі (Henning Schulzrinne, Колумбійський університет) і Марком Хендлі (UCL). У листопаді 2000 року SIP був затверджений як сигнальний протокол проекту 3GPP і постійний елемент архітектури IMS [1].

RADIUS (англ. Remote Authentication Dial-In User Service) — протокол передачі даних, що використовується в комп'ютерних мережах для автентифікації, авторизації та обліку різноманітних сервісів (англ. authentication, authorization, accounting, AAA). RADIUS був розроблений Livingston Enterprises, Inc. в 1991 році, а потім був перенесений у стандарти IETF (англ. Internet Engineering Task Force).

RADIUS це клієнт-серверний протокол що працює на прикладному рівні, і може бути використовуватися як транспорт TCP та і UDP [3].

Дуже перспективним є використання в майбутньому протоколу Diameter. Він був створений з метою заміни та вдосконалення свого попередника, протоколу RADIUS.

За допомогою протоколу наступного покоління — *Diameter* можна виконувати нові команди та/або атрибутами, наприклад такими, що використовуються в протоколі EAP [4].

Найбільш частим є використання двох протоколів одночасно. Наприклад, встановлення сесії відбувається за допомогою SIP, а обрахунок вартості дзвінка за допомогою RADIUS. Таке поєднання дає можливість зменшити навантаження на сервер, так як буде використовуватися на половину менше пакетів для передачі даних. RADIUS має більше переваг у порівнянні з SIP, адже позбавлений недоліків, зокрема, таких як можливість здійснювати неоплачені дзвінки.

Абсолютним стандартом кодування голосу впродовж минулих років є система H.264. Енкодер H.264 виконує процеси прогнозування, перетворення і кодування для створення стисненого потоку біт у форматі H.264. Декодер H.264 виконує відповідний процес декодування, зворотнього перетворення і реконструкції для відтворення відеопослідовності [5].

Перш ніж перейти до опису технологій, які допоможуть зробити VoIP безпечнішим, а значить придатним до використання в банківських системах необхідно детальніше ознайомитися з принципом побудови таких систем.

Принцип побудови VoIP. Вся система VoIP побудована на основі протоколів транспортного рівня TCP і UDP. Це протоколи транспортного рівня, які здійснюють зв'язок між машиною — відправником пакетів і машиною -адресатом.

Прикладний рівень — це додатки типу клієнт-сервер, що базуються на протоколах нижніх рівнів. На відміну від протоколів транспортного, фізичного та канального рівня, протоколи прикладного рівня займаються деталями конкретного додатка і «не цікавляться» способами передачі даних по мережі. Серед основних додатків TCP/IP, наявних практично в кожній його реалізації використовується протокол емуляції терміналу Telnet, протокол передачі файлів FTP, протокол електронної пошти SMTP, протокол управління мережею SNMP, що використовується в системі World Wide Web (WWW) протокол передачі гіпертексту HTTP та ін.

Оскільки в Інтернеті деталі фізичних з'єднань приховані від додатків, прикладний рівень зовсім «не дбає» про те, що клієнт працює в мережі Ethernet, а сервер підключений до мережі Token Ring. Між кінцевими системами може бути кілька десятків маршрутизаторів і безліч проміжних фізичних мереж різних типів, але додаток буде сприймати цей конгломерат як єдину фізичну

мережу. Це і обумовлює основну логіку і привабливість технології Інтернет і протоколу IP.

На базі протоколу IP будується не тільки мережа Інтернет, а й будь-які інші мережі передачі даних (локальні, корпоративні), які можуть мати або не мати вихід на глобальну мережу Інтернет. Універсальність і гнучкість мереж на базі протоколу IP дає можливість застосовувати їх не тільки для передачі даних, а й іншої мультимедійної інформації. Нещодавно IP-мережі стали використовувати для передачі мовних повідомлень. Без технології протоколу IP сьогодні складно уявити діяльність будь-якої банківської системи, а тим більше роботу VoIP [6].

Обов'язковим є наявність у системі так званого VoIP-шлюзу, який буде приймати та передавати інформацію у вигляді пакетів фізично поєднуючи абонентів. Прикладом може бути Freeswitch, який має відкритий програмний код і розповсюджується на умовах вільної ліцензії. Також важливою складовою є білінгова платформа, яка здійснює розрахунок вартості дзвінка та складає маршрут дзвінка. Саме в білінговій платформі є перспектива використовувати штучний інтелект і нейронні мережі, адже процес побудови маршруту з кожним роком стає все складнішим з'являється все більше операторів зв'язку та можливостей обрати вартість та якість голосового повідомлення.

Вищезазначену проблему можна вирішити за допомогою *баз знань*, яка буде оновлюватися в режимі реального часу. Для того щоб зрозуміти складність побудови білінгової платформи, потрібно описати принцип її роботи.

У кожного дзвінка є дві частини: їх називають оригінатор і термінатор. Оригінатор створює новий дзвінок, а термінатор його приймає. Дзвінки здійснюються між двома людьми, які користуються послугами операторів VoIP-телефонії, кожен дзвінок має свою вартість, тобто є ціна, яку сплачує користувач, який має бажання зателефонувати, вартість дзвінків йому встановлює його оператор. Для того, щоб дзвінок успішно відбувся, потрібно мати кінцевого користувача, який має можливість прийняти дзвінок, він може бути абонентом тієї самої мережі або бути абонентом іншої мережі тоді повна вартість збільшується, адже за послугу термінатора потрібно платити. Таким чином, чим дешевшою є вартість послуг термінатора, тим більший прибуток отримає оператор зв'язку. Саме на цьому етапі потрібно зосередити свою увагу під час створення бази знань та використання систем штучного інтелекту. Крім того, потрібно враховувати що людина не може здійснювати такий вибір в реальних сучасних умовах, а

використання програмної логіки не враховує тих обставин, які є важливими для прийняття рішення. Також цікавим буде процес навчання на основі моніторингу статистичної інформації, адже за місяць оператори зв'язку накопичують сотні гігабайт інформації про здійснені дзвінки в яких записано тривалість, вартість та інші параметри кожного опрацьованого дзвінка. Даний процес може здійснюватися в форматі CDR (CALL DETAIL RECORD) або напяму в базу, якщо використовується RADIUS протокол. RADIUS дає можливість попередньо визначити вартість та можливість тривалість дзвінка, що значно спрощує випадки виявлення шахрайства. Дана інформація є дуже важливою для аналізу, але людина в силу своїх можливостей просто фізично не здатна здійснити обробку такого значного обсягу інформації, тому наявність елементів системи штучного інтелекту, для створення якого потрібно мати базу знань і здійснення процесу навчання моделі, буде дуже доречним. Після процесу опрацювання такої інформації з'являється можливість дати відповідь на питання, як користувачі використовують VoIP-телефонію, які тарифні плани можна їм запропонувати в майбутньому тощо [7].

Типи загроз для VoIP. Питання безпеки зв'язку завжди було одним з важливих у мережах телекомунікацій. В даний час у зв'язку з бурхливим розвитком глобальних комп'ютерних мереж і, в тому числі мереж Інтернет-телефонії, забезпечення безпеки передачі інформації стає ще більш актуальним. Розробка заходів у галузі безпеки повинна проводитися на основі аналізу ризиків, визначення критично важливих ресурсів системи і можливих загроз. Існує кілька основних типів загроз, які становлять найбільшу небезпеку в мережах VoIP-телефонії:

- *підміна даних про користувача* означає, що один користувач мережі видає себе за іншого. При цьому виникає вірогідність несанкціонованого доступу до важливих функцій системи. Використання механізмів аутентифікації та авторизації в мережі підвищує впевненість у тому, що користувач, з яким встановлюється зв'язок, не є підставною особою, і що йому можна надати санкціонований доступ;

- *підслуховування.* Під час передачі даних про користувачів (користувальницьких ідентифікаторів і паролів) або приватних конфіденційних даних по незахищених каналах ці дані можна підслухати і згодом зловживати ними. Методи шифрування даних знижують вірогідність цієї загрози;

- *маніпулювання даними.* Дані, які передаються по каналах зв'язку, в принципі можна змінити. У багатьох методах шифру-

вання використовується технологія захисту цілісності даних, що запобігає їх несанкціонованій зміні;

- *відмова від обслуговування* (Denial of Service — DoS) є різновидом хакерської атаки, в результаті якої важливі системи стають недоступними. Це досягається шляхом переповнення системи непотрібним трафіком, на обробку якого йдуть всі ресурси системної пам'яті і процесора. Система зв'язку повинна мати відповідні ресурси для розпізнавання подібних атак і обмеження їх впливу на мережу;

- найрозвиненішою формою шахрайства в Інтернеті, без сумніву, є *фішинг*. Типовими інструментами фішингу є mail (поштові повідомлення, що використовують методи соціальної інженерії), спеціально розроблені web-сайти.

Базовими елементами у сфері безпеки є *аутентифікація, цілісність і активна перевірка*. Аутентифікація покликана запобігти загрозі знеособлення і несанкціонованого доступу до ресурсів та даних. Хоча авторизація не завжди включає до свого складу аутентифікацію, але найчастіше одне обов'язково має на увазі інше. Цілісність забезпечує захист від підслуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність переданої інформації. Активна перевірка означає перевірку правильності реалізації елементів технології безпеки і допомагає виявляти несанкціоноване проникнення в мережу і атаки типу DoS [8].

Способи подолання загроз для VoIP-телефонії. Основою будь-якого захищеного зв'язку є криптографія. *Криптографією* називається технологія складання і розшифрування закодованих повідомлень. Крім того, криптографія є важливою складовою для механізмів аутентифікації, цілісності і конфіденційності. Аутентифікація є засобом підтвердження особи відправника або одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, за якої дані не може зрозуміти ніхто, крім їх відправника і одержувача. Зазвичай криптографічні механізми існують у вигляді алгоритму (математичної функції) і секретної величини (ключа), алгоритми відомі, а в секреті необхідно тримати тільки криптографічні ключі. Причому чим більше бітів у такому ключі, тим менше він вразливий.

Структура шифрованого VoIP виклику. Дзвінок складається з сигнальної і media частин, кожна з яких може бути зашифрована окремо з застосуванням спеціальних методів-протоколів. Для шифрування сигнальної інформації застосовується SSL/TLS, для шифрування «голоси» ZRTP і SRTP протоколи.

SSL/TLS — грубо кажучи, аналог HTTPS для звичайного SIP. Протокол дозволяє клієнту переконатися, що він спілкується з потрібним сервером за умови, що клієнт довіряє наданим сервером сертифікатам.

SRTP і ZRTP — це два різних способи шифрувати потоку. Принципова відмінність між ними в тому, що обмін ключами для SRTP відбувається на етапі сигналізації (на першій сигнальній стадії встановлення виклику). А для ZRTP — безпосередньо на початку обміну пакетами (у другій, «медійній» частині) за спеціальним протоколом, який базується на методі криптографії Діффі — Хеллмана.

Важливо те, що для SRTP обов'язковою умовою надійності шифрування дзвінка є одночасне використання SSL/TLS + SRTP, інакше зломиснику не складе труднощів отримати ключі (які будуть передані по шифрованому SIP) і прослухати розмову. Для ZRTP це не важливо, потік буде надійно зашифрований не залежно від того, шифрується сигналізація чи ні. Протокол також вміє визначати наявність «man in the middle» (у тому числі серверів послуг) між клієнтами, які спілкуються. Це дозволяє бути впевненим у тому, що розмову неможливо прослухати, принаймні з точки зору прослуховування мережі/середовища передачі даних.

Також важливим моментом є використання аутентифікації. Під аутентифікацією розуміється визначення користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, брандмауера і т. д.) і його місця розташування в мережі з подальшою авторизацією користувачів і кінцевих пристроїв. Найпростішим способом аутентифікації є використання паролів, але для підтримки високого рівня безпеки паролі доводиться часто змінювати. Методи використання одноразових паролів застосовуються досить часто. Серед них можна відзначити методи аутентифікації за протоколом S/Key або за допомогою спеціальних апаратних засобів (token password authentication). Механізм аутентифікації за протоколом Point-to-Point Protocol (PPP) часто застосовується в середовищі модемного доступу і включає використання протоколів Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) і Extensible Authentication Protocol (EAP). Розробка протоколу EAP усе ще триває, але вже зараз вона дає можливість більш гнучкого використання існуючих протоколів і тільки з'являються технології аутентифікації в каналах PPP. TACACS + і Remote Access Dial-In User Service (RADIUS) — це протоколи, які підтримують масштабовані pi-

шення в області аутентифікації. Протокол Kerberos (Цербер) використовується в обмежених областях для підтримки єдиної точки входу в мережу. Система одноразових паролів S/Key, визначена в RFC 1760, представляє собою систему генерування одноразових паролів на основі стандартів MD4 і MD5. Вона призначена для боротьби з «повторними атаками», коли хакер підслуховує канал, виділяє з трафіку ідентифікатор користувача і його пароль та надалі використовує їх для несанкціонованого доступу. Система S/Key заснована на технології клієнт-сервер, де клієнтом зазвичай є персональний комп'ютер, а сервером — сервер аутентифікації. Спочатку і клієнта, і сервер потрібно налаштувати на єдину паролівну фразу і рахунок ітерації. Клієнт починає обмін S/Key, відправляючи серверу пакет ініціалізації, а сервер у відповідь відправляє порядковий номер і випадкове число, так зване «зерно» (seed). Після цього клієнт генерує одноразовий пароль. Для цього клієнт передає одноразовий пароль на сервер, де він і перевіряється. Для перевірки аутентифікації система одноразово пропускає отриманий одноразовий пароль через захищену хеш-функцію. Якщо результат цієї операції збігається з попереднім паролем, що зберігається у файлі, результат аутентифікації вважається позитивним, а новий пароль зберігається для подальшого використання. Аутентифікація за допомогою апаратних засобів працює за однією з двох альтернативних схем: — за схемою запит-відповідь; — за схемою аутентифікації з синхронізацією за часом. У схемі запит-відповідь користувач підключається до сервера аутентифікації, який, у свою чергу, пропонує ввести персональний ідентифікаційний номер (PIN) або користувальницький ідентифікатор (user ID). Користувач передає PIN або user ID на сервер, який потім робить «запит» (передає випадкове число, яке з'являється на екрані користувача). Користувач вводить це число в спеціальний апаратний пристрій, схожий на кредитну картку, де число запити шифрується за допомогою користувацького шифрувального ключа. Результат шифрування відображається на екрані. Користувач відправляє цей результат на сервер аутентифікації. У той час як користувач підраховує цей результат, сервер аутентифікації розраховує цей же результат самостійно, використовуючи для цього базу даних, де зберігаються всі користувацькі ключі. Отримавши відповідь від користувача, сервер порівнює його з результатом власних обчислень. Якщо обидва результати збігаються, користувач отримує доступ до мережі. Якщо результати виявляються різними, доступ до мережі не надається. При використанні схеми з синхронізацією за часом на

апаратному пристрої користувача і на сервері працює секретний алгоритм, який через певні синхронізовані проміжки часу генерує ідентичні паролі і замінює старі паролі на нові. Користувач підключається до сервера аутентифікації, який запитує у користувача код доступу. Після цього користувач вводить свій PIN в апаратний картковий пристрій, і в результаті на екран виводиться деяка величина, яка являє собою одноразовий пароль. Цей пароль і відправляється на сервер. Сервер порівнює його з паролем, який був обчислений на самому сервері. Якщо паролі збігаються, користувач отримує доступ до мережі [8].

У випадку, якщо дзвінок надходить за іншою технологією, наприклад PSTN чи GSM, то сигнал проходить через IP-шлюз, який перетворює цифровий (VoIP) сигнал в аналоговий. Для передавання голосу через IP-мережу відбувається процедура стискання сигналу спеціальною програмою-кодеком. Це здійснюється для збільшення швидкості передавання даних відповідно для підвищення якості зв'язку. Рівень безпеки передавання мовної інформації підвищує процедура шифрування даних. Зв'язок між двома VoIP-терміналами можливий лише за умови сумісних кодеків [9].

1. Використання технології VoIP у банківських системах. Розглянемо приклад впровадження VoIP телефонії у банківській системі. Контакт-центр банку може бути початково організований на Asterisk і додаткових системах для вихідних обдзвонів, віндикування та розсилки SMS. Використання кількох програм буде апріорі незручним і забиратиме багато часу. Заявки з сайту будуть приходити на електронну пошту, переноситися вручну в базу та обдзвонюватися. Великий відсоток заявок буде втрачатися через людський фактор. Підготовка бази для вихідного обдзвону на основі вивантажених з банківської системи даних буде займати кілька годин роботи аналітиків і повинна бути виконана завчасно. До того ж, база швидко буде ставати не актуальною через відсутність синхронізації з банківською системою. Система вихідного обдзвону дозволяє імпортувати заявки лише в один статичний список.

2. VoIP + Cisco Packet Tracer. Використання окремої системи для віндикування також ускладнює роботу операторів (рис.1), яким доводилось вивчати кілька різних програм для контакт-центру і постійно переходити між ними та поштовою програмою в процесі роботи.

Для організації кожного процесу контакт-центру постійно будуть залучатися аналітики, IT-спеціалісти та програмісти. Різні програмні рішення для кожного процесу не забезпечують стабі-

льності роботи контакт-центру та не будуть інтегровані між собою і з банківською системою.

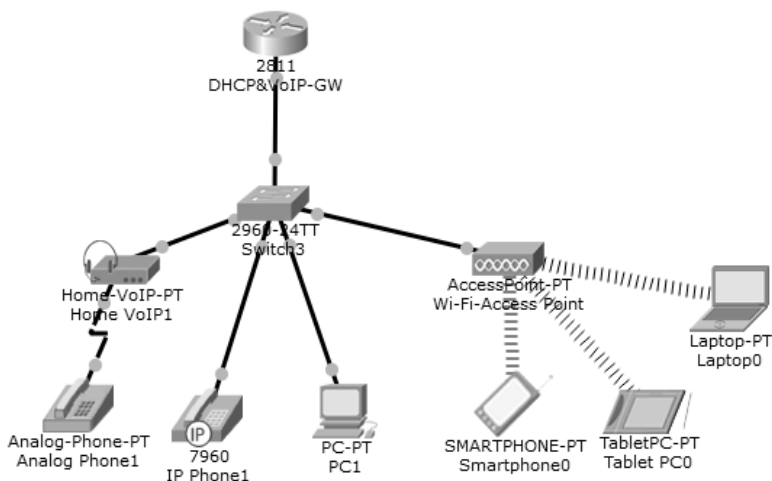


Рис. 1. VoIP + Cisco Packet Tracer

З використанням криптографічного захисту VoIP-телефонії потреба у спрощенні процесів обдзвону завдяки використанню багатофункціональної системи з інтегрованим модулем VoIP єдиного програмного забезпечення, дозволяють отримати детальну статистику за всіма типами звернень і збільшують ефективність роботи системи.

Основні завдання дослідження: 1) впровадження динамічної системи маршрутизації, та зміна логіки обробки звернень клієнтів; 2) створення централізованої системи розсилки SMS, автодозвону та інформування; 3) впровадження фільтрів на основі інтеграції з банківською системою, тож відпадає потреба у експорті списків і використання пошти.

Прикладом реалізації подібного завдання є АТ «Ощадбанк». Основа всієї системи IP-телефонії банку — це кластер керування, який допускає подальше нарощування; він працює з програмним забезпеченням Cisco CallManager. Застосування техніки кластеризації за теперішніх масштабів мережі IP-телефонії АТ «Ощадбанк» спрямоване на підвищення надійності методом резервування.

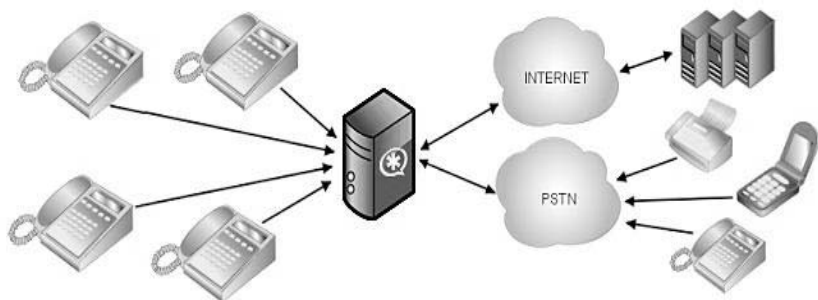


Рис.2. VoIP + IP/VC 3540

Однієї з функціональних можливостей мережі IP-телефонії банку є проведення конференцій, які можна реалізувати як з використанням CallManager так і/або за допомогою сервера конференцій (СК) IP/VC 3540. Програмне забезпечення CallManager містить програмні модулі, котрі відповідають за суто програмну реалізацію операцій змішування медіапотоків з використанням кодека G.711, необхідних для організації конференційного режиму зв'язку. Сервер конференцій IP/VC 3540 — це модульний пристрій, котрий забезпечує змішування медіапотоків за допомогою апаратних засобів СК. Крім того, IP/VC 3540 розширює функціональні можливості проведення конференцій порівняно з CallManager.

Висновки.

1) Проведено аналіз і досліджено можливості використання технологій VoIP-телефонії у банківських системах.

2) Використання технологій VoIP-телефонії у банківських системах вирішують такі завдання:

- проведення аудіоконференцій як з працівниками центрального апарату, так і з працівниками обласних управлінь банку, при цьому кількість учасників конференції суттєво збільшується;
- контроль стану (кількість учасників, їхні номери телефонів, час входу та виходу з конференції) можливості керувати проведенням аудіоконференції в режимі реального часу;
- захист доступу до аудіоконференції за допомогою застосування паролів і спеціалізованих систем захисту;
- утримування абонентів (мультиканальні можливості передачі даних), запобігання випадкам переадресування та перехоплення викликів;

- здійснення ефективного використання єдиного інформаційного вікна для підвищення ефективності роботи менеджера;
- передавання інформації про структуру та розмір депозитного портфеля за допомогою надійних засобів зв'язку VoIP-телефонії.

Література

1. Протокол встановлення сесії. Електронний ресурс. [Режим доступу:] https://uk.wikipedia.org/wiki/Session_Initiation_Protocol
2. Голос через IP. Електронний ресурс. [Режим доступу:] <https://uk.wikipedia.org/wiki/VoIP>
3. Протокол передачі даних RADIUS. Електронний ресурс. [Режим доступу:]
4. Протокол передачі даних Diameter. Електронний ресурс. [Режим доступу:] <https://uk.wikipedia.org/wiki/Diameter>
5. Енкодер H.264. Електронний ресурс. [Режим доступу:] <https://uk.wikipedia.org/wiki/H.264>
6. Гольдштейн Б. С., Пінчук А. В., Суховицький А. Л. IP-телефонія: Радіо і зв'язок, 2008. Ст. 395-399.
7. Операторська платформа надання послуг: Електронне навчальне видання. Конспект лекцій / Л. С. Глоба, О.М. Дяденко, В.Ф. Чердинцева. — К.: НН ІТС НТУУ «КПІ», 2013. — 191 с.
8. Нопін С. В., Шахов В. Г. Аналіз захищеності абонентських систем IP-телефонії від несанкціонованого доступу // Інформаційні технології. 2008. №11. Ст. 67–74.
9. Дудикевич В.Б., Хорошко В.О., Микитин Г.В., Банах Р.І., Ребець А.І. Інформаційна модель безпеки технологій зв'язку // Інформатика та математичні методи в моделюванні. 2014. Том 4, № 2 С. 137–148.

References

1. Protokol vstanovlennia sesii. Elektronnyi resurs. [Rezhym dostupu:] https://uk.wikipedia.org/wiki/Session_Initiation_Protocol
2. Holos cherez IP. Elektronnyi resurs. [Rezhym dostupu:] <https://uk.wikipedia.org/wiki/VoIP>
3. Protokol peredachi danykh RADIUS. Elektronnyi resurs. [Rezhym dostupu:]
4. Protokol peredachi danykh Diameter. Elektronnyi resurs. [Rezhym dostupu:] <https://uk.wikipedia.org/wiki/Diameter>
5. Enkoder H.264. Elektronnyi resurs. [Rezhym dostupu:] <https://uk.wikipedia.org/wiki/H.264>
6. Holdshtein B. S., Pinchuk A. V., Sukhovytskyi A. L. IP-telefoniia: Radio i v'iazok, 2008. St. 395–399.

7. Operatorska platforma nadання posluh: Elektronne navchalne vydannia. Konspekt leksii / L. S. Hloba, O.M. Diadenko, V.F. Cherdyntseva. — K.: NN ITS NTUU «KPI», 2013. — 191 s.

8. Nopin S. V., Shakhov V. H. Analiz zakhyshchenosti abonentskykh system IP-telefonii vid nesanktsionovanoho dostupu // Informatsiini tekhnologii. 2008. №11. St. 67–74.

9. Dudykevych V.B., Khoroshko V.O., Mykityn H.V., Banakh R.I., Rebets A.I. Informatsiina model bezpeky tekhnologii zviazku // Informatyka ta matematychnimetody v modeliuvanni. 2014. Tom 4, № 2 St. 137–148.

Статтю подано до редакції 22.10.2018 р.

УДК336.02:330.43

О. Л. Шапошник, аспірантка кафедри вищої математики,
ДВНЗ «Київський національний економічний
університет ім. Вадима Гетьмана»

Shaposhnyk Helen, PhD Student of the Advanced
Mathematics Department
SHEE «Kyiv National Economic University
named after Vadym Hetman»

МОДЕЛЮВАННЯ ВПЛИВУ ЗМІН ГРОШОВО-КРЕДИТНОЇ ПОЛІТИКИ НА РІВЕНЬ ФІНАНСОВОЇ БЕЗПЕКИ ДЕРЖАВИ

MODELING THE INFLUENCE OF CHANGES IN THE MONEY-CREDIT POLICY ON THE STATE OF FINANCIAL SAFETY LEVEL

Анотація. У роботі визначено складові фінансової безпеки: банківська безпека, безпека небанківського фінансового сектора, боргова безпека, валютна безпека, бюджетна безпека та грошово-кредитна безпека. Обґрунтовано, що для побудови регресійних моделей, що описують дієвість інструментів грошово-кредитної політики в контексті забезпечення фінансової безпеки екзогенною змінною виступатиме показник інфляції як індекс споживчих цін.

Побудовано модель індексу споживчих цін на основі щомісячних даних. За допомогою надбудови Аналіз даних у MSExcel побудовано кореляційну матрицю та проаналізовано парні коефіцієнти кореляції між всіма парами змінних моделі.

Доведено, що значення парних коефіцієнтів кореляції між незалежними змінними є невисокими, що є свідченням відсутності мультиколінеарності. Відсутність мультиколінеарності перевіряється за допомогою критерію Хі-квадрат.