Кібернетична безпека

УДК 004.056.53; 004.056.55

Н.І. Алішов, С.В. Зінченко, А.Н. Алішов, Н.О. Сапунова

Інститут кібернетики імені В.М. Глушкова НАН України, Київ

ЗАСТОСУВАННЯ НЕРОЗКРИВНИХ ШИФРІВ ДЛЯ УБЕЗПЕЧЕННЯ VOIP-ТЕЛЕФОНІЇ

Статтю присвячено проблемам безпеки VOIP-телефонії. Розглянуто основні види загроз для VOIP-телефонії, заходи щодо їх усунення. Запропоновано програмно-апаратний комплекс захисту на базі використання нерозкривних шифрів, який працює в потоковому режимі.

***Ключові слова**: потокова інформація, VOIP-телефонія, захист інформації, нерозкривні шифри, протоколи передавання інформації, пристрій захисту інформації.*

Вступ

Проблеми безпеки мережевих голосових повідомлень за технологією VOIP мало чим відрізняються від проблем безпеки мережі в цілому [1 – 4]. Основну небезпеку становлять хакери, які, знаючи про уразливості системи, створюють атаки, що сприяють відмові систем, перехопленню особистих даних через користувальницьке ПЗ, наприклад X-lite, Skype, Ekiga та ін. Докладна технічна інформація про велику кількість протоколів VOIP також створює проблеми, пов'язані з маршрутизацією голосового трафіка через брандмауери і мережні адреси, які використовуються для з'єднання транзитних мереж. Граничні контролери застосовуються для захисту дзвінків. Інші методи вимагають завантаження допоміжних протоколів (STUN або Interactive Connectivity Establishment (ICE) тощо).

Зазвичай організації вдаються до різних заходів безпеки для захисту VOIP-трафіка − голосових повідомлень, що передаються по безпечним IP. Це досягається за рахунок застосування різних методик шифрування.

Багато користувальницьких систем VOIP не підтримують шифрування передачі голосових даних, надаючи у результаті можливість підслуховувати VOIP-виклики. У статті описуються технологія й апаратно-програмні засоби організації захисту передавання потокової мультимедійної інформації в реальному часі для VOIP-телефонії на базі розробленого в Інституті кібернетики НАНУ USB-пристрою шифрування [5].

Основні види загроз для VOIP-мереж

Перехоплення та маніпулювання даними. Найпоширеніша уразливість телефонних мереж, особливо небезпечна для IP-телефонії. У випадку застосування IP-телефонії зловмисникові не потрібен фізичний доступ до лінії передавання даних. Пристрій перехоплення, що знаходиться усередині корпоративної мережі, найімовірніше може бути виявлений, а от зовнішнє прослуховування відстежити практично неможливо. Крім того, перехоплені дані або голос можна передати далі у зміненому вигляді. У таких умовах весь незашифрований голосовий потік необхідно вважати небезпечним.

Підміна та злом користувальницьких даних. Відмова від використання або спрощення механізмів автентифікації й авторизації в IP-телефонії відкриває для зловмисника можливість несанкціоновано отримати доступ до системи, підмінивши дані про користувача своїми даними. Можливий також злом облікових даних користувачів за допомогою перебору або прослуховування незахищених каналів зв'язку. Подібна уразливість може бути використана, наприклад, для здійснення дорогих дзвінків за рахунок жертви або для прийому важливих для зловмисника дзвінків і їхнього записування з метою застосування даної інформації в корисливих цілях. У будь-кому випадку така «дірка» в безпеці здатна звести нанівець всю можливу вигоду від використання IP-телефонії.

Обмеження доступності. Одним з різновидів атак є «відмова в обслуговуванні» (Denial of Service, DoS). Ця атака націлена на перевищення граничного навантаження на систему великою кількістю коротких дзвінків або інформаційного непотребу. Якщо не організовано постійне відстежування ознак подібних атак і застосування пасивних засобів захисту, сервери IP-телефонії врешті-решт не справляться зі зрослим навантаженням і не зможуть обслуговувати підключених абонентів.

Інформаційна безпека VOIP-телефонії

Підхід до організації інформаційної безпеки, у тому числі VOIP-телефонії, має бути комплексним,

© Н.І. Алішов, С.В. Зінченко, А.Н. Алішов, Н.О. Сапунова

оскільки кожен спосіб захисту не тільки закриває свою частину інформаційного периметра, але й доповнює інші рішення. Тому пропонований комплекс реалізує захист двох частин − серверної та клієнтської.

Убезпеченню сервера буде сприяти організація запобіжних заходів, зокрема таких традиційних:

Застосування політики складних паролів. Одержання облікових даних методом перебору (bruteforce) вимагає значних витрат часу й обчислювальних ресурсів, ускладнення паролів дозволить зробити даний метод атак недоцільним.

Відключення гостьових дзвінків. Дозвіл на здійснення вихідних дзвінків надається тільки користувачам системи, це унеможливить спроби подзвонити ззовні без попередньої авторизації.

Обмеження напрямків дзвінків, доступних абонентам, застосування схеми «заборонено все, крім дозволеного». Зловмисник, якому вдалося отримати облікові дані користувача системи, зможе реалізувати дзвінки тільки по певних напрямках. Це дозволить уникнути несанкціонованого здійснення дорогих міжнародних дзвінків.

Відключення відповіді про неправильний пароль. За замовчуванням VOIP-сервер видає одну помилку про неправильний пароль для існуючого й іншу для неіснуючого VOIP-клієнтів. Зловмисник, скориставшись якоюсь з безлічі програм для підбирання паролів, зможе перевірити всі короткі номери й збирати паролі лише до існуючих акаунтів, які дали відповідь «неправильний пароль».

Регулярні перевірки системи на предмет спроб злому, контроль параметрів. Організація системи моніторингу стану системи дозволить поліпшити якість IP-телефонії та визначити типові для даної конфігурації параметри. Відхилення цих параметрів від отриманих типових значень свідчить про проблеми з устаткуванням, каналами зв'язку або наявність спроб вторгнення зловмисників.

Використання систем блокування доступу після невдалих спроб реєстрації. Переглядаючи періодично звіти системи з метою виявлення спроб злому, можна виділити й заблокувати IP-адреси нападників, що дозволить скоротити непотрібний SIP-трафік і захиститися від множинних спроб злому.

Застосування міжмережних екранів. Міжмережний екран пропускає вихідний трафік від сервера телефонії до SIP-провайдера та фільтрує вхідний за певними правилами. Доцільно закривати на міжмережному екрані всі мережеві порти для IP-телефонії, крім необхідних для її коректної роботи й адміністрування. Цей метод захисту застосовується на VOIP-сервері, щоб захистити його від внутрішніх атак. У такому разі сервер телефонії буде доступний із зовнішніх мереж тільки по певних службових портах, підключення до яких має виконуватися із застосуванням шифрування.

Убезпечення VOIP-даних. Для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної або комерційної інформації в руки зловмисника необхідно захистити передані відкритими каналами зв'язку дані від перехоплення та прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, цю проблему можна розділити на дві складові − захист службових даних IP-телефонії (SIP-протокол) і захист голосового трафіка (RTP-протокол) (рис. 1).

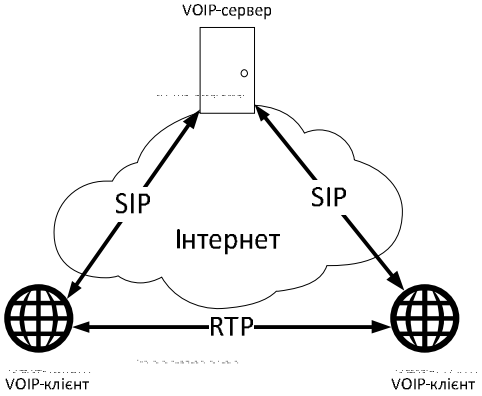

Рис. 1. Схема організації VOIP-телефонії

Протоколи передавання потокової інформації. На даний час існують безліч стандартних міжнародних протоколів, призначених для передавання потокової інформації в комп'ютерних мережах. Крім того, багато відомих фірм пропонують програмні застосування, які є надбудовами над цими протоколами для передавання мультимедійної потокової інформації в комп'ютерних мережах. Тому розробку власних протоколів не можна вважати актуальною задачею. Завдання авторів полягало в тому, щоб інтегрувати розроблені програмні засоби для пристрою шифрування з існуючими протоколами та застосуваннями (рис. 2, 3, табл. 1). Таке завдання не є тривіальним і вимагає високого професіоналізму, оскільки ці системи не призначені для «чужорідних» пристроїв.

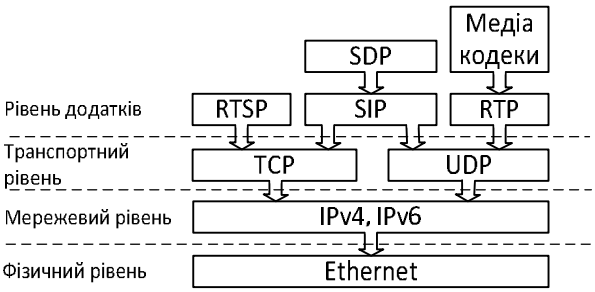

Рис. 2. Місце протоколів VOIP-телефонії у стеці протоколів TCP/IP

Протоколи, що застосовуються у VOIP-телефонії:

Таблиця 1

Базові мультимедіа-кодеки, що використовуються у VOIP-телефонії

Назва	Тип	Опис	Швидкість передачі даних (Кбіт)	Частота дискретизації (кГц)
G.711	аудіо	Імпульсно-кодова модуляція (ІКМ)	64	8
G.711.1	аудіо	Імпульсно-кодова модуляція (ІКМ)	80-96 Кбіт	8
G.721	аудіо	Адаптивна диференціальна імпульсно-кодова модуляція (ADPCM)	32	8
G.722	аудіо	7 кГц аудіо-кодування в межах 64 Кбіт /с	64	16
G.722.1	аудіо	Кодування на 24 і 32 Кбіт/с для гучного зв'язку в системах з малими втратами кадрів	24/32	16
GSM 06.10	аудіо	-	13	8
Speex	аудіо	-	8, 16, 32	2.15-24.6
Ilbc	аудіо	-	8	13.3
THEORA	відео	Стиснення з втратами	-	-
H.264	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	від 64 Кбіт/с до 960000 Мбіт/с	-
H.263	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	192 Кбіт/с	-
H.261	відео	MPEG-4 AVC/H.264, стиснення з втратами та без втрат	від 40 Кбіт/с до 2 Мбіт/с	-

– **SIP** (Session Initiation Protocol) − протокол ініціювання сеансів, є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференц- і телефонних з'єднань, розподілу мультимедійної інформації. Користувачі можуть брати участь в існуючих сеансах зв'язку, запрошувати інших користувачів і бути запрошеними ними до нового сеансу зв'язку. Запрошення можуть бути адресовані певному користувачеві, групі користувачів або всім користувачам.

– **SDP** (Session Description Protocol) − протокол прикладного рівня, призначений для опису сесії передавання потокових даних, включаючи VOIP-телефонію, Інтернет-радіо, програми мультимедіа. Сесія SDP може реалізовувати кілька потоків даних. У протоколі SDP в даний час визначені аудіо, відео, дані, управління і застосування (потокові), подібні до MIME-типів електронної пошти в Інтернет-адресах. Повідомлення SDP, що передається від одного вузла іншому, може вказувати:

- адреси місця призначення, які можуть бути адресами мультикастингу для медіапотоків;
- номери UDP-портів для відправника й одержувача;
- медіа-формати (наприклад, кодеки, описувані профілем), які можуть застосовуватися під час сесії;
- час старту й зупинки. Використовується в разі широкомовних сесій, наприклад, телевізійних або радіопрограм. Можна внести час початку, завершення і часи повторів сесії.

– **RTP** (Real-time Transport Protocol) – працює на прикладному рівні і є основним протоколом для передавання даних у реальному масштабі часу. Протокол RTP переносить у своєму заголовку дані, необхідні для відновлення аудіо або відео в приймальному вузлі, а також дані про тип кодування інформації (JPEG, MPEG і т.п.). У заголовку даного протоколу, зокрема, передаються часова мітка і номер пакета. Ці параметри дозволяють при мінімальних затримках визначити порядок і момент декодування кожного пакета, а також інтерполювати втрачені пакети.

– **RTCP** (Real-time Control Protocol) – заснований на періодичній передачі пакетів управління всім учасникам сеансу зв'язку при використанні того ж механізму розподілу, що і протокол RTP. Протокол нижчого рівня повинен забезпечити мультиплексування інформаційних і керуючих пакетів, наприклад, з використанням різних номерів портів UDP. Протокол RTCP виконує чотири основні функції:

- забезпечення зворотного зв'язку для оцінювання якості розподілу даних,
- синхронізація звукового та відеосигналу,
- передача параметрів, необхідних для розрахунку частоти відправлення пакетів,
- управління сеансом зв’язку.

На рис. 3 наведено спрощену схему взаємодії клієнта з мультимедійним сервером через базові протоколи передачі потокової інформації.

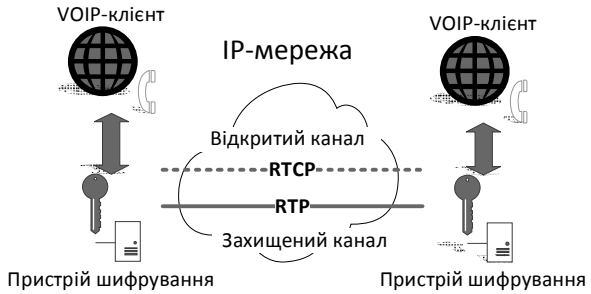

Рис. 3. Схема взаємодії клієнтів IP-мережі

Як видно з рис. 3, відкритий канал організовано з використанням протоколів RTSP і RTCP. Перший керує передачею потокової інформації в реальному масштабі часу, другий контролює зміни в мережі для надання інформації RTP-протоколу.

Захищений канал базується на використанні RTP-протоколу. Як зазначалося, існує безліч застосувань, що забезпечують взаємодію клієнтів через відкритий канал (наприклад, застосування XLITE, EKIGA і т.п.). Тому основним завданням при виконанні роботи було створення не тільки інтерфейсу взаємодії з цими застосуваннями для організації передавання відкритих даних, але й способу використання інтерфейсу протоколу RTP для інтеграції з розробленим пристроєм шифрування переданих потокових мультимедійних даних у реальному масштабі часу. У даній реалізації для цієї мети використовуються проксі-сервери, хоча можливі й інші варіанти. Вважаємо, що наразі представлений варіант є найбільш ефективним.

Комплекс захисту VOIP-телефонії

З погляду системної інтеграції розроблений комплекс складається з двох підсистем: програмної підсистеми, що забезпечує інтерфейс з мережевим протоколом, й апаратної підсистеми, яка реалізує запропонований алгоритм шифрування потоків інформації на базі нерозкривних шифрів. Узагальнену схему взаємодії цих підсистем показано на рис. 4.

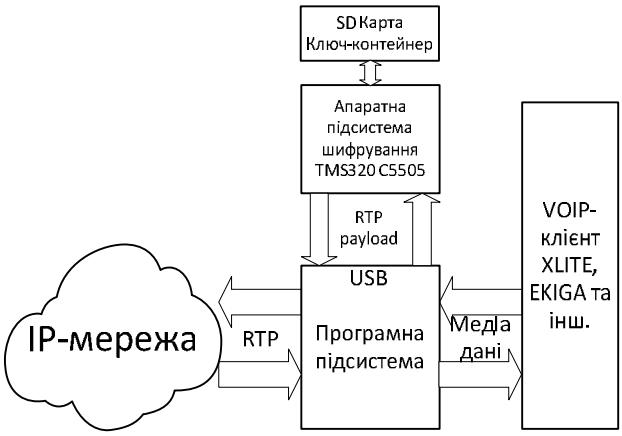

Рис. 4. Загальний схема роботи пристрою захисту

Пропонована система захисту працює в потоковому режимі, тобто зашифровані дані, що передаються каналом зв'язку, розшифровуються в прикінцевому пристрої й далі обробляються іншими застосуваннями або апаратними пристроями. Тому реалізований режим функціонування системи захисту не припускає збереження переданих даних у зашифрованому вигляді.

Програмна підсистема. Програмна підсистема надає необхідний набір API-функцій для сторонніх застосувань, а також реалізує розроблений функціонал.

Апаратна підсистема. Для застосувань апаратна підсистема представляється у вигляді набору функцій, які викликаються при виклику заданих API-функцій із програмної підсистеми. Така реалізація дозволяє гнучко модифікувати різні підпрограми без необхідності повторного перепрограмування всього пристрою. Крім цього з'являється можливість додавати в апаратну частину нові реалізації алгоритмів генерації псевдовипадкових чисел, протоколів узгодження, спеціалізованих функцій обробки різного контенту та ін.

З урахуванням зростаючої необхідності в передаванні потокової мультимедійної інформації в комп'ютерних мережах пристрій (рис. 5, 6) був створений на базі процесора серії TMS320 C5505 для цифрової обробки сигналів, що забезпечило необхідну продуктивність.

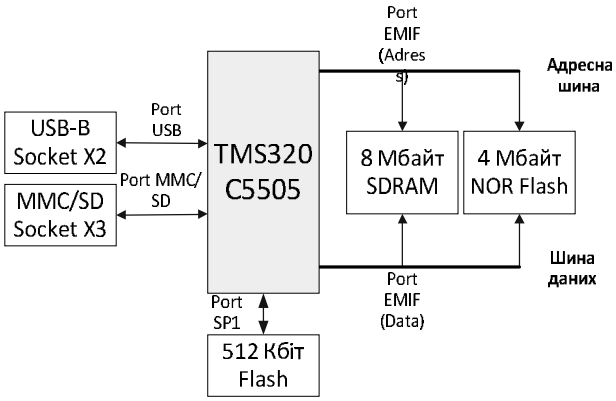

Рис. 5. Блок-схема
розробленого пристрою шифрування

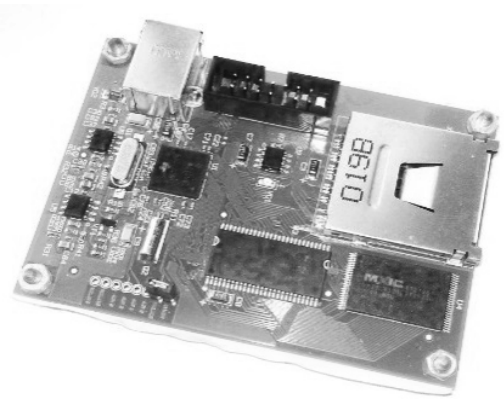

Рис. 6. Загальний вигляд пристрою шифрування

Алгоритм передавання зашифрованої потокової інформації в реальному часі. Суть розробленого алгоритму шифрування полягає в такому. У масив пам'яті на базі SD-картки записуються істинно випадкові числа (шум лісу, шум автомобільного двигуна й т.п.), з яких зорганізується спеціальний масив (він і буде секретним ключем). Береться байт мультимедійного файлу, який треба зашифрувати, у секретному ключі розшукується його адреса й ця адреса передається по мережі. На приймальній стороні є такий самий масив істинно випадкових чисел (секретний ключ), де відповідно до прийнятої адреси розшукується значення байта, яке стане байтом зашифрованої послідовності. Даний алгоритм є гранично криптостійким. Існує безліч варіантів його реалізації. Наприклад, вибира-

ється один із кращих алгоритмів генерації псевдовипадкових чисел з певними параметрами («зерно»). Передавальна сторона на базі істинно випадкових чисел (відповідно до описаного алгоритму) відправляє приймальній стороні «зерно». Приймальна сторона, використовуючи ці параметри, на льоту генерує відповідні псевдовипадкові числа й із цих чисел вибирає байти переданої мультимедійної інформації. У такому випадку обсяг вихідного масиву чисел може бути значно меншим.

Схему спрощеного варіанта пропонованого алгоритму шифрування наведено на рис. 7.

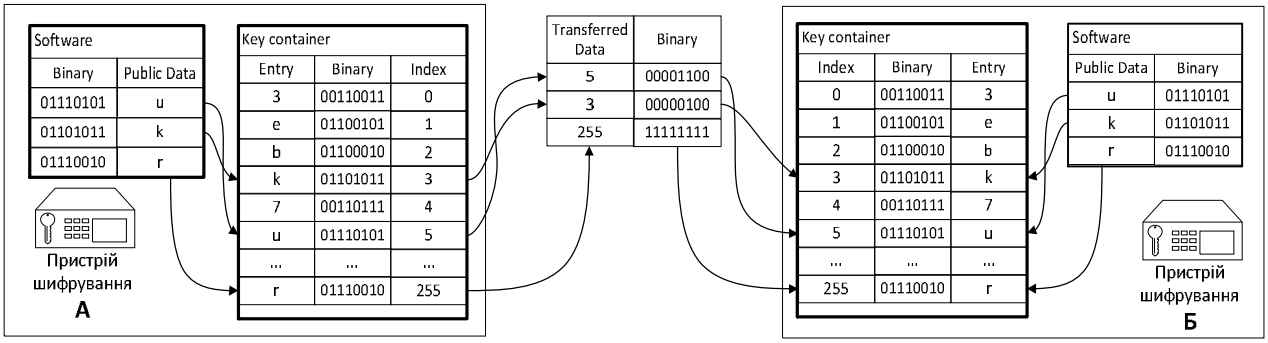

Рис. 7. Спрощений алгоритм передавання зашифрованої потокової інформації в реальному часі

Висновки

Отже, створення програмно-апаратних комплексів захисту на базі використання нерозкривних шифрів є перспективним напрямком досліджень в області інформаційної безпеки. Оскільки даний клас шифрів володіє доведеною криптостійкістю й відповідно не може бути зламаний, це дозволяє використовувати гарантовану криптостійкість. Особливою перевагою описаного комплексу захисту є робота в потоковому режимі, що дозволяє застосовувати його у VOIP-телефонії, в системах аудіо-, відеотрансляції, а також у різних розподілених системах з підвищеними вимогами до параметрів використовуваних каналів зв'язку. Наразі розроблений апаратно-програмний комплекс проходить експериментальне дослідження в настільних комп'ютерах, локально-корпоративній мережі комп'ютерів, а також у глобальній мережі Інтернет.

Список літератури

1. Method of shared data access in distributed computer networks / [Nycolaychuk Y.M., Humenniy P.V., Alishov N.I., Hladyuk V.M.]// Journal of Qafgaz University (Baku): Mathematics and Computer Science. – 2013. – V 1, N 1. – P. 17−23.

2. Computer technologies in information security/ [Valery Zadiraka, Yaroslav Nykolaichuk, Nadir Alishov, Ivan Albanskyi, Boris Bredelev et al.]. − Ternopil: Kart-Blansh, 2015. − 387 p.

3. Goto A. Safe and Secure Ubiquitous Communication/ A. Goto // Intern. workshop on network security and wireless communications 27 Jan 2005. – Accessed to: http://www.it.ecei.tohoku.ac.jp/~kato/workshop2005/NTT-goto-slides.pdf.

4. Network Security: Know It All / [J. Joshi, S. Bagchi, B.S. Davie et al.]. – Burlington: Morgan Kaufmann, 2008. – 368 p.

5. Технология системной интеграции аппаратно-программных средств защиты потоковой информации на базе нераскрываемых шифров [Алишов Н.И., Алишов А.Н., Бойко А.Я. и др.] // Системи обробки інформації: зб. наук. праць. – Х.: Харківський університет Повітряних Сил імені Івана Кожедуба, 2016. – Вип. 3 (140). – С. 7-10.

Надійшла до редколегії 2.02.2017

Рецензент: д-р техн. наук, проф. В.М. Опанасенко, Інститут кібернетики імені В.М. Глушкова НАН України, Київ.

ПРИМЕНЕНИЕ НЕРАСКРЫВАЕМЫХ ШИФРОВ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В VOIP-ТЕЛЕФОНИИ

Н.И. Алишов, С.В. Зинченко, А.Н. Алишов, Н.А. Сапунова

Статья посвящена проблемам безопасности VOIP-телефонии. Рассмотрены основные виды угроз для VOIP-телефонии, мероприятия по их устранению. Предложен программно-аппаратный комплекс защиты на основе использования нераскрываемых шифров, который работает в потоковом режиме.

***Ключевые слова**: потоковая информация, VoIP-телефония, защита информации, нераскрываемые шифры, протоколы передачи информации, устройство защиты информации.*

APPLICATION OF UNBREAKABLE ENCRYPTION TO ENSURE SECURITY IN VOIP TELEPHONY

N.I. Alishov, S.V. Zintchenko, A.N. Alishov, N.A. Sapunova

The article is devoted to security VOIP telephony issues. Considered the main types of threats to VOIP telephony and activities to eliminate them. Proposed a VOIP protection system based on using unbreakable cipher. It includes hardware and software that operates in streaming mode.

***Keywords:** streaming, VOIP telephony, data protection, unbreakable cipher, data protocols, data security device.*