Роман А. Устинов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский пр-т, 49, г. Москва, 125993, Россия
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

DOI: http://dx.doi.org/10.26583/bit.2017.4.08

Аннотация. На сегодняшний день речевые технологии являются одним из самых активно развивающихся секторов в мировой экономике. В связи с чем, вопросы обеспечения безопасности речевой информации (РИ) остаются весьма актуальными. В рамках данной работы рассмотрены системы защиты РИ для современной модели связи. Такая модель является мультимодальной и многопотоковой и подразумевает наличие большого числа абонентов, которые имеют возможность использовать несколько линий связи для организации своего взаимодействия. С учетом этого проведен детальный анализ угроз конфиденциальности, целостности и доступности РИ. Рассмотрены существующие методы противодействия данным угрозам. Показано, что имеющиеся методы не обеспечивают безопасность речевых сообщений (РС) в полной мере и существует ряд новых угроз в области обеспечения целостности и доступности РИ, для которых на текущий момент решения отсутствуют или находятся на стадии разработки. Предложены собственные подходы для противодействия таким угрозам. Для обеспечения целостности РС наиболее перспективными являются методы стеганографии, в частности применение аудиомаркеров позволит однозначно аутентифицировать личность говорящего на протяжении всего сеанса связи. Для противодействия угрозам доступности РИ в части, касающейся пропускной способности канала связи и ограниченных объемов хранилищ данных РС, необходимы усовершенствование существующих и разработка новых адаптивных алгоритмов сжатия речи. При чем такие алгоритмы должны сохранять заданный уровень речевой разборчивости.

Ключевые слова: защита речевой информации, угрозы информационной безопасности, речевая разборчивость, аудиомаркер, адаптивное алгоритмы сжатия речи

Для цитирования. **УСТИНОВ, Роман А.** ОСОБЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 73-81, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/279>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.08.

***Благодарности:** Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета 2017 года.

Roman A. Ustinov
Financial University under Government of the Russian Federation (Financial University),
Leningradsky Prospekt, 49, Moscow, 125993, Russia
e-mail: public-ura@yandex.ru, ORCID 0000-0002-8454-9951

Specific features of modern voice protection systems

DOI: http://dx.doi.org/10.26583/bit.2017.4.08

Abstract. Nowadays, speech technologies are among the most vibrant sectors of the world's economy. Of high importance is the problem of ensuring the security of speech information (SI). Here we discuss SI protection systems within a modern communication model. The model is multimodal, multithreaded, and implies a large number of subscribers interacting via several communication lines. With this in mind, we perform a detailed analysis of threats to the confidentiality, integrity and accessibility of SI. Existing methods of counteraction against these threats are discussed, and shown to be insufficient to ensure the safety of voice messages (VM) in full. Mean while, there are new threats to the integrity and accessibility of SI, the solutions for

which are either do not exist, or only being developed. We propose our original approach to counter these threats. Steganography methods are the most promising for ensuring the integrity of the VM. In particular, using audiomarkers allows one to reliably trace speaker'sidentity throughout the entire communication session. In order to counter the threats to SI availability due to the capacity of the communication channel and the limited volumes of VM data storage, it is necessary to improve existing adaptive speech compression algorithms, along with developing new ones. Furthermore, such algorithms must keep the specified level of speech intelligibility.
Keywords: protection of speech information, threats to information security, speech intelligibility, audiomarker, adaptive compression algorithms
For citation. **USTINOV, Roman A.** Specific features of modern voice protection systems. IT Security, [S.l.], v. 24, n. 4, p. 73-81, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/279>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.08.
***Acknowledgements:** The article is prepared on the basis of the results of studies carried out at the expense of budget funds under the state task of the Financial University of 2017.

Введение

Несмотря на высокие темпы развития телекоммуникационных технологий, человеческая речь продолжает оставаться одним из самых популярных способов общения между людьми. Так, аналитики Forbes отмечают, что рынок речевых технологий является одним из самых динамично развивающихся секторов экономики в мире. По их прогнозам, к 2022 году он увеличится до 12 млрд, в качестве основной движущей силы отмечаются постоянно растущие потребности в речевых технологиях в области безопасности, телекоммуникациях, колл-центрах и B2C (Business-to-consumer) секторе [1].

Такое положение дел обусловлено тем, что речь является уникальным психолингвистическим процессом. Она обладает рядом признаков, присущим только ей: эффект присутствия, эмоциональная окраска, информационная избыточность и т.п.[2] Таким образом, задача защиты речевой (акустической) информации (РИ) на сегодняшний момент не потеряла своей актуальности, а в связи с постоянно развивающимися технологиями речевой обработки, а также средствами акустической (речевой) разведки приобретает все большее значение[3].

Модель многопотоковой мультимодальной системы связи

На современном этапе развития систем связи, традиционная модель голосовой связи, представленная на рисунке 1, значительно изменилась.

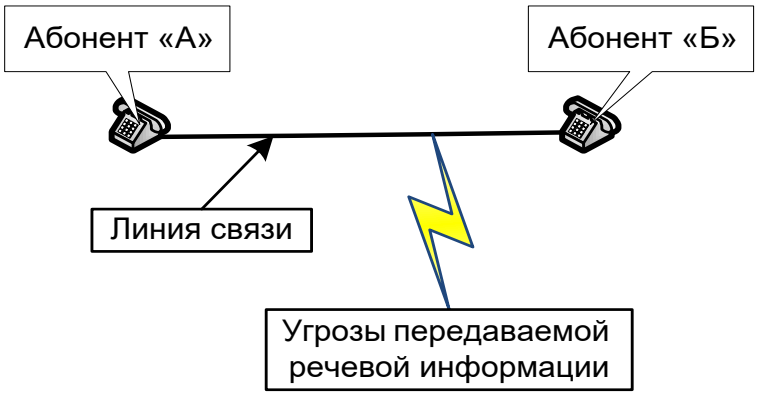

Рисунок 1 - Традиционная модель связи абонентов
(Fig. 1 - Traditional model of communication subscribers)

В настоящее время актуальная модель связи абонентов представляет собой мультимодальную многопотоковую систему, в которой участвует много абонентов и

может быть задействовано несколько линий связи. Такая модель представлена на рисунке 2.

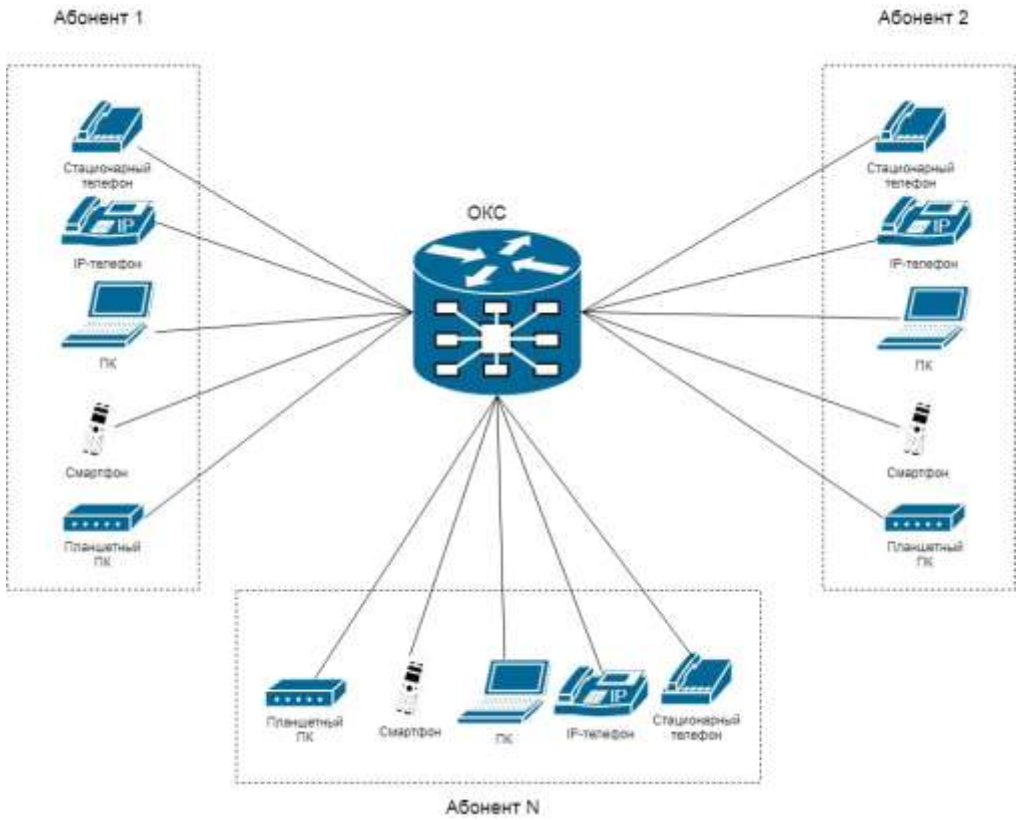

Рисунок 2 - Актуальная модель связи абонентов (много абонентов - много линий связи)

(Fig. 2 - Current model of subscribers (a lot of subscribers - a lot of lines))

Актуальные угрозы речевой информации при ее передаче по общедоступным каналам связи

Как и для любого другого вида информации защищенность РИ на практике рассматривается как совокупность трех основополагающих понятий: конфиденциальность, целостность, доступность [4].

Основными элементами описания угроз информационной безопасности являются:

- источник угрозы;
- среда распространения информативного сигнала;
- носитель защищаемой информации.

В качестве источников угроз безопасности РИ можно рассматривать злоумышленников (физические лица, юридические лица, криминальные, террористические группировки, разведывательные службы государств), осуществляющих перехват (съем) информации с использованием технических средств ее регистрации.

Среда распространения информативного сигнала (РИ) - это физическая среда, по которой информативный сигнал может распространяться и приниматься (регистрироваться) приемником.

Носителем защищаемой РИ являются акустические (речевые) сигналы.

С учетом вышеизложенного, рассмотрим современные угрозы РИ.

Угрозы конфиденциальности

Угрозы конфиденциальности направлены на получение несанкционированного доступа к РИ и напрямую связаны с угрозами свойственными каналам связи и аппаратно-программным средствам передачи голосовой информации. Это обусловлено тем, что во время передачи голосовой (звуковой) информации, она является наиболее доступной и менее защищённой для нарушителя, не обладающего специальными дорогими устройствами акустической (речевой) разведки на уровне специальных служб, но обладающего знаниями обо всех технологических процессах обработки такой информации.

Определим основные угрозы конфиденциальности РИ:

- применение подслушивающих устройств и видеосъемка с аудио сопровождением;
- обнаружение и анализ побочных электромагнитных излучений и наводок;
- перехват данных, передаваемых по каналам связи, и их последующий анализ для определения протоколов обмена, правил установления сеансов связи и авторизационных параметров пользователя с целью получения доступа к защищаемой РИ;
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, MAC-адрес, адрес в системе связи, аппаратный блок кодирования;
- внедрение аппаратных и/или программных "закладок", вирусного программного обеспечения, позволяющих преодолевать систему зашиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации.

Угрозы целостности

В общем смысле целостность защищаемой информации, во-первых, обеспечивает неизменность данных на предполагаемом этапе жизненного цикла обработки информации со стороны нелегитимных пользователей (статистическая целостность), а во-вторых, гарантирует то, что информация внутренне непротиворечива и отражает реальное положение вещей (динамическая целостность)[4].

К угрозам статической целостности относятся[5]:

- незаконное изменение информации, фальсификация информации (дезинформация);
- фальсификация автора сообщения, то есть нарушение аутентичности - гарантии того, что источником информации является именно тот, субъект, который заявлен как ее автор;
- нарушение аппелированности сообщения, то есть гарантия авторства сообщения - возможность доказать, что автором сообщения является именно заявленный субъект.

Угрозами динамической целостности является нарушение атомарности транзакций, внедрение нелегальных пакетов в информационный поток и т.д.

Угрозы доступности

Угрозы доступности РИ, в свою очередь, также обусловлены указанными особенностями построения каналов голосовой связи, однако дополнительно включают в себя вопросы помехозащищенности и пропускной способности.

К подобного рода угрозам относятся [6]:

- физическое воздействие на вычислительную систему (ВС) или отдельные ее части с целью вывода ВС из строя, уничтожения, нарушения регламентированного порядка функционирования;

- физическое воздействие на подсистемы обеспечения функционирования ВС (электропитания, охлаждения и т.п.);
- изменение режимов работы устройств или программ;
- различные методы ведения радиоэлектронной борьбы и/или информационного воздействия (создание активных радиопомех на частотах работы устройств системы и т.п.);
- внедрение аппаратных и/или программных "закладок", вирусного программного обеспечения с целью дезорганизации функционирования ВС;
- угрозы типа отказ в обслуживании (Denial of Service - DoS) - атака на ВС с целью довести её до отказа, то есть создание таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым ВС ресурсам, либо этот доступ затруднён.

Методы обеспечения безопасности речевой информации

Оборонительный аспект создаваемых с помощью информационных технологий средств обеспечения информационной безопасности РИ в открытых, общедоступных каналах связи (ОКС), требует от разработчика комплексного подхода к решению проблемы защиты речевых сообщений (РС). То есть построение систем защиты РИ должно проводиться с учетом всех возможных угроз, и исходя из предположения, что злоумышленник (ЗЛ) обладает всем необходимым арсеналом знаний и технического оборудования для осуществления несанкционированного доступа к РИ в ОКС.

На рисунке 3 представлены методы защиты РИ от угроз конфиденциальности, целостности и доступности. Рассмотрим каждый из представленных методов более подробно.

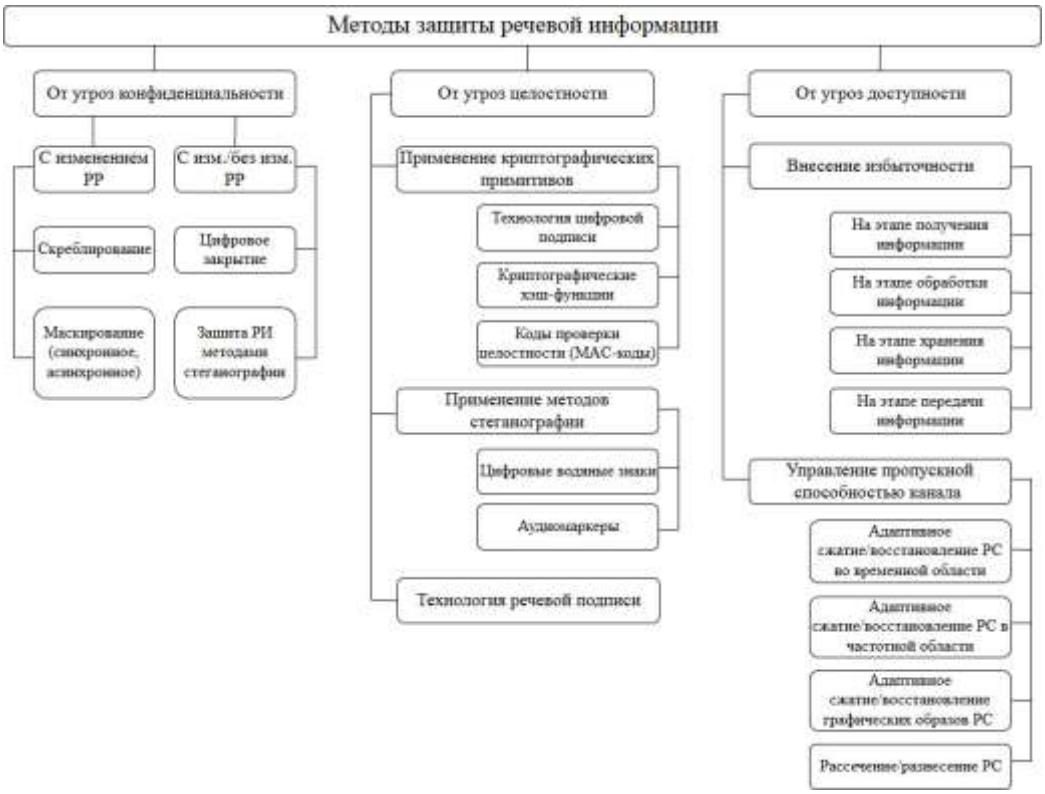

Рисунок 3 - Методы защиты речевой информации
(Fig. 3 - Methods of protection of speech information)

Методы защиты речевой информации от угроз нарушения конфиденциальности

На сегодняшний день существует большое количество различных методов, обеспечивающих безопасность РИ при ее передаче по ОКС. Данные методы основываются на преобразованиях речевых сигналов, изменяющих характеристики РС, затрудняя их разборчивость и узнаваемость для ЗЛ.

Основным показателем защищенности РИ от угроз конфиденциальности является речевая разборчивость (РР) - отношение количества принятых слушателем (артикулянтом) элементов речи к общему количество переданных элементов речи. В зависимости от способов изменения РР различают методы защиты РИ с изменением или без изменения РР.

К методам с изменением РР относятся: *маскирование, аналоговое скремблирование (преобразование)*.

Под *маскированием* понимается синтез спектра маскированного речевого сигнала, путем внесения амплитудно-частотного искажения, обеспечивающий максимальную скрытность передачи сигнала при наилучшем качестве восстановленной речи. Различают синхронное (требуется наличие блока (схемы) синхронизации) и асинхронное маскирование РИ.

Под *скремблированием* понимается изменение характеристик исходного речевого сигнала таким образом, чтобы преобразованный (защищенный) сигнал был неразборчив и неузнаваем, но занимал такую же полосу частот спектра, как и исходный открытый речевой сигнал [7, 8].

Цифровое закрытие РИ и защита РИ методами стеганографии могут применяться как методы с изменением, так и без изменения РР. Это обусловлено тем, что использование указанных методов условно можно разбить на два эта.

В случае цифрового закрытия - это преобразование речевого сигнала (без изменения или с изменением РР) в цифровую форму и применение криптографических алгоритмов.

В случае использования стеганографических методов - это предварительная обработка речевого сигнала (в цифровой или аналоговой форме с изменением/без изменения РР) и последующее внедрение в стегоконтейнер. Стоит отметить, что данный метод позволяет обеспечить не только конфиденциальность передаваемого РС, но и скрыть сам факт передачи. Среди наиболее распространенных вариантов использования стеганографии для обеспечения безопасности РИ могут использоваться[5]:

- скрытная передача РИ в информационных сообщениях иного вида (видео, изображение, текст);
- скрытная передача РИ в другом речевом сигнале.

Методы защиты речевой информации от угроз нарушения целостности

На практике задачи обеспечения целостности информации решаются путем применения различных криптографических примитивов[4]:

- технология цифровой подписи;
- криптографические хэш-функции;
- коды проверки подлинности (MAC-коды).

В дополнение к указанным способам защиты РС от угроз целостности могут применяться[9, 10]:

- стеганографические методы (выявление признаков незаконного копирования аудио и видеозаписей может осуществляться по цифровым водяным знакам и др.);
- технология речевой подписи (повышение защищенности документооборота).

Однако для РИ появляются новые угрозы нарушения целостности, обусловленные интенсивным развитием речевых технологий и методов повышения качества обработки речевого сигнала.

Так, в августе 2017 года на ежегодной конференции и выставке в области компьютерной графики и интерактивных технологий SIGGRAPH 2017 специалистами из Вашингтонского университета были продемонстрированы возможности нейросетевых технологий по синтезу реалистичного видео с использованием аудиозаписей. Им удалось сформировать высокореалистичное фейковое видео с Бараком Обамой. Для этого потребовалось всего лишь 14 часов, в течении которых нейросеть обучалась правильной синхронизации движений губ и речевого потока на образцах выступлений бывшего президента США, находящихся в свободном доступе.

Еще одним ярким примером может служить возросшее число случаев телефонных "пранков" и мошенничеств, когда при помощи технологий синтеза человеческой речи ЗЛ выдают себя за других людей.

Таким образом, возникает задача подтверждения подлинности источника РС на всем интервале ведения разговора, в том числе и при организации видеоконференцсвязи. Одним из решений данной проблемы может служить внедрение аудиомаркеров (некоторый аналог цифровых водяных знаков) в речевой поток для однозначной аутентификации личности говорящего [11, 12].

Методы защиты речевой информации от угроз нарушения доступности

Угрозы доступности РИ обусловлены уязвимостями каналов связи, поэтому нейтрализация указанных угроз достигается путем введения той или иной избыточности. На текущий момент существует достаточное количество апробированных решений в этой области, некоторые из которых отражены на рисунке 4 [4].

Рисунок 4 - Структура системы защиты от угроз нарушения доступности (Fig. 4 - The structure of the system of protection against threats of violation of availability)

Но несмотря на широкий спектр существующих методов противодействия угрозам нарушения доступности, для систем защиты РИ есть ряд специфических задач, в области которых решения отсутствуют, либо находятся на стадии разработки.

Весьма актуальной представляется задача накопления и хранения архивов РИ, возникшая в результате принятия 6 июля 2016 г. федеральных законов № 374-ФЗ и

№ 375-ФЗ ("пакет Яровой"), которые в том числе обязывают операторов связи хранить звонки абонентов за определенный период.

Кроме того, существует традиционная задача управления пропускной способностью канала связи в условиях активного информационно-технического воздействия ЗЛ.

Решение данных задач подразумевает разработку новых и усовершенствование существующих адаптивных методов сжатия РИ с сохранением максимального уровня РР в условиях ограниченного объема хранилища данных или в условиях низкой пропускной способности канала связи [13, 14].

Заключение

Несмотря на бурное развитие информационных технологий, РИ до сих пор занимает значительную часть в общем объеме предаваемой информации даже в условиях изменившейся модели связи абонентов. С учетом этого изменился и приоритет традиционных угроз безопасности РИ, появились новые угрозы.

Можно считать, что наиболее защищенной РИ остается от угроз нарушения конфиденциальности. Такое положение дел обусловлено тем, что традиционно конфиденциальность считается наиболее значимым свойством безопасности информации. Для обеспечения защиты РС от несанкционированного доступа разработан и применяется широкий спектр как программных, так и программно-аппаратных средств защиты, основанных на реализации одного или комбинации нескольких методов защиты РИ: маскирование, скремблирование, цифровое закрытие или стеганография.

Однако с учетом постоянно развивающихся речевых технологий растет и значимость обеспечения безопасности РИ от угроз нарушения целостности и доступности. Данные вопросы требуют более внимательного и комплексного подхода для своего решения.

Для защиты РС от угроз нарушения целостности весьма перспективными видятся методы стеганографии. Например, для подтверждения личности участников переговоров в ОКС можно использовать технологию встраивания аудиомаркеров в РС.

Для противодействия угрозам доступности РИнеобходима разработка и исследование новых методов адаптивного сжатия речи с сохранением заданного уровня РР и повышения пропускной способности ОКС, в том числе на основе образного анализа-синтеза речевого сигнала.

СПИСОК ЛИТЕРАТУРЫ:

1 Федорин М. Они нас слышат: куда развиваются речевые технологии? "Forbes Russia". URL: http://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (дата обращения: 11.09.2017).

2 Устинов Р.А. Проблема обеспечения информационной безопасности при передаче аудиовизуальных данных по общедоступным каналам связи. Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 3. URL: http://technomag.bmstu.ru/doc/168981.html (дата обращения: 13.09.2017).

3 Дворянкин С.В., Козлачков С.Б., Харченко Л.А. Оценка защищенности речевой информации с учетом современных технологий шумоочистки. Вопросы защиты информации № 2. 2007. с. 18-21.

4 Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс. URL: http://ss-sks.narod.ru/is/lit01.pdf (дата обращения: 15.09.2017).

5 Пузыренко А.Ю, Конахович Г.Ф. Компьютерная стеганография. Теория и практика. К.: "МК-Пресс", 2006. 288 с.

6 Park P.VoIP Threat Taxonomy Cisco Press. URL: http://www.ciscopress.com/articles/article.asp?p=1245881 (дата обращения: 21.09.2017).

7 Дворянкин С.В. Компьютерные технологии защиты речевых сообщений в каналах электросвязи. Учебное пособие. М.: РИО МТУСИ, 1999. 52 с.

8 Дворянкин С.В., Мишуков А.А. Маскирование речевой информации: перспективные методы и средства. "Спецтехника и связь" № 3. 2009. с. 46-51.

9 Дворянкин С.В., Минаев В.А. Возможности скрытой передачи информации по общедоступным каналам речевой связи. Тезисы докладов 7-й Международной конференции "Информатизация правоохранительных систем". М: Академия управления МВД РФ, 1997. ч. 2. с. 78-79.

10 Дворянкин С.В., Минаев В.А. Технология речевой подписи. Открытые системы. - М.1997. № 5 (25). с. 68-71.
11 Дворянкин С.В., Дворянкин Н.С. Способ установления подлинности речевых сообщений, передаваемых по каналам сотовой связи. Спецтехника и связь. 2015. № 4. с. 32-39.
12 Scheips D. Voice recognition - benefits and challenges of this biometric application for access control SourceSecurity.com. URL: https://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html (дата обращения: 21.09.2017).
13 Sun L., Mkwawa IH., Jammeh E., Ifeachor E. Speech Compression Springer International Publishing AG. URL: https://link.springer.com/chapter/10.1007%2F978-1-4471-4905-7_2 (дата обращения: 21.09.2017).
14 Дворянкин С.В., Калужин Р.В. Адаптивное сжатие аудиоинформации в системах защиты и обработки. "Системы безопасности", № 6(48), 2002. с. 94-96.

REFERENCES:

[1] Fedorin M. Oni nas slyishat: kuda razvivayutsya rechevyie tehnologii ? "Forbes Russia". URL: http://www.forbes.ru/tekhnologii/331035-oni-nas-slyshat-kuda-razvivayutsya-rechevye-tekhnologii (accessed: 11.09.2017).
[2] Ustinov R.A. Problema obespecheniya informatsionnoy bezopasnosti pri peredache audiovizualnyih dannyih po obschedostupnyim kanalam svyazi. Nauka i obrazovanie. MGTU im. N.E. Baumana. Elektron. zhurn. 2011. no 3 URL: http://technomag.bmstu.ru/doc/168981.html (accessed: 13.09.2017).
[3] Dvoryankin S.V., Kozlachkov S.B., Harchenko L.A. Estimation of security of voice information with the modern technology of noise-cancellation. Voprosyi zaschityi informatsii no 2. 2007.pp. 18-21. (In Russian).
[4] Tsirlov V.L. Osnovyi informatsionnoy bezopasnosti avtomatizirovannyih sistem. Kratkiy kurs. URL: http://ss-sks.narod.ru/is/lit01.pdf (accessed: 15.09.2017).
[5] Puzyirenko A.Yu, Konahovich G.F. Computer steganography. Teoriya i praktika. K.: "MK-Press", 2006. 288 p.
[6] Park P. VoIP Threat Taxonomy Cisco Press. URL: http://www.ciscopress.com/articles/article.asp?p=1245881 (accessed 21.09.2017).
[7] Dvoryankin S.V. Computer protection technology voice messages in telecommunication channels. Uchebnoe posobie. M.: RIO MTUSI, 1999. 52 p.(In Russian).
[8] Dvoryankin S.V., Mishukov A.A. Masking of speech information: advanced methods and tools. "Spetstehnika i svyaz" no 3. 2009. pp. 46-51 (In Russian).
[9] Dvoryankin S.V., Minaev V.A. The possibility of hidden transmission of information through public channels voice communications. Tezisyi dokladov 7-y Mezhdunarodnoy konferentsii "Informatizatsiya pravoohranitelnyih sistem". M: Akademiya upravleniya MVD RF, 1997. vol. 2. pp. 78-79. (In Russian).
[10] Dvoryankin S.V., Minaev V.A. Technology voice signature. Otkryityie sistemyi. - M.1997. no 5 (25). pp. 68-71. (In Russian).
[11] Dvoryankin S.V., Dvoryankin N.S. The method of establishing the authenticity of voice messages transmitted over cellular channels. Spetstehnika i svyaz. 2015. no 4. pp. 32-39. (In Russian).
[12] Scheips D. Voice recognition - benefits and challenges of this biometric application for access control SourceSecurity.com. URL: https://www.sourcesecurity.com/news/articles/co-3108-ga.4100.html (accessed: 21.09.2017).
[13] Sun L., Mkwawa IH., Jammeh E., Ifeachor E. Speech Compression Springer International Publishing AG. URL: https://link.springer.com/chapter/10.1007%2F978-1-4471-4905-7_2 (accessed: 21.09.2017).
[14] Dvoryankin S.V., Kaluzhin R.V. Adaptive compression of audio in security systems and processing. "Sistemyi bezopasnosti", no. 6(48), 2002. pp. 94-96.

Поступила в редакцию - 19 июня 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – June 19, 2017. The final version – November 01, 2017.