УДК 004.357

Вестник УрФО № 3(29) / 2018, с. 5–12

Асяев Г. Д., Антясов И. С.

DOI: 10.14529/SECUR180301

ИСПОЛЬЗОВАНИЕ УЛЬТРАЗВУКОВЫХ КОЛЕБАНИЙ ДЛЯ РЕАЛИЗАЦИИ ТЕХНИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

В статье рассмотрены физические основы образования технического канала утечки информации с применением ультразвуковых колебаний. Описана уязвимость, позволяющая обратить наушники в микрофон на программном уровне. Представлена атака типа «Дельфин». Исследована применимость данной уязвимости для скрытой передачи информации с помощью ультразвуковых колебаний. Рассмотрены основные сценарии реализации данной атаки и выявлены основные методы противодействия.

Ключевые слова: *защита информации, ультразвук, передача данных, отношение сигнал/шум.*

Asyaev G. D., Antyasov I. S.

USING ULTRASONIC VIBRATIONS TO IMPLEMENT A TECHNICAL INFORMATION LEAKAGE CHANNEL

The article discusses the physical basis for the formation of a technical information leakage channel using ultrasonic vibrations. Describes the vulnerability that allows the headphones turn into a microphone at the program level. Introduced attack type "Dolphin". The applicability of this vulnerability to hidden information transmission using ultrasonic vibrations is investigated. The main scenarios for the implementation of this attack are considered and the main methods of countering are identified.

Keywords: *information protection, ultrasound, data transmission, signal-to-noise ratio.*

В настоящее время существует большое многообразие возможных сценариев похищения данных с ПК. Установка антивирусного программного обеспечения, разграничение доступа, увеличение границ контролируемой зоны, отключение ПК от сети Интернет – вот неполный перечь мер, необходимый для защиты информации. Однако даже при выполнении вышеперечисленных критериев два размещённых рядом компьютера, которые имеют либо

встроенные динамики, либо микрофон образуют технический канал утечки информации.

В качестве объекта разведки в рассматриваемом ТКУИ выступает информация ограниченного распространения, обрабатываемой на СВТ (компьютер или ноутбук). Актуальной средой распространения в данном случае является только воздушная. В качестве технического акустического средства разведки выступает микрофон или наушники, которые подключены непосредственно к самому объекту разведки и вспомогательный ПК или ноутбук, находящийся в одном помещении с объектом разведки.

Основными задачами исследования являются:

• Рассмотреть атаку типа «Дельфин»;

• Определить возможные сценарии проведения рассматриваемой атаки;

• Определить эффективность применения рассматриваемой уязвимости для скрытой передачи информации с помощью ультразвуковых волн;

• Рассмотреть программную и техническую спецификацию функции «jack retasking» для расширения вариантов атаки;

• Определить методы противодействия данной уязвимости.

Исследователи по кибербезопасности из Чжэцзянского университета доказали, что с помощью ультразвуковых колебаний можно скрытно передавать команды системам с функцией голосового помощника. Данная атака получила название «Дельфин». Алгоритм работы системы представлен на рисунке 1. Злоумышленник преобразует стандартные команды, произнесённые человеком в ультразвук. Система распознавания речи реагирует на эти колебания и выполняет соответствующие команды. Так как ультразвуковые колебания не слышны человеческому уху, то атакующий ничего не услышит, что повышает опасность реализации данной атаки [1].

С помощью данной атаки можно заставить систему открыть вредоносный сайт, загрузить шпионскую программу, позвонить кому-либо, либо включить диктофон и отправлять голосовую информацию через Интернет.

Выделяют 2 типа систем голосовых помощников:

• те, которые зависят от голоса говорящего;

• те, которые не зависят от голоса говорящего.

Для реализации атаки в первом случае злоумышленникам требуется запись голоса владельца данной системы для активации. Впоследствии уже можно с помощью ультразвуковых команд, промодулированных человеческим голосом передавать команды для выполнения.

Для реализации атаки по втором случае достаточно сразу посылать системе команды с помощью ультразвука. Так как было доказано, что система понимает фразы для активации произнесённые на другой частоте (в ультразвуковом диапазоне). Данная атака работает в диапазоне 21000-40000 Гц, а максимальное расстояние между ультразвуковым излучателем и устройством, поддерживающим систему распознавания голоса, при котором удалось успешно реализовать вышеописанный алгоритм составило 2 метра.

Однако ультразвуковые колебания можно использовать не только для передачи команд голосовым помощником, но и для скрытой передачи данных. С помощью вредоносного программного обеспечения, которое может быть внедрено, например, внутренним нарушителем, можно настроить беспроводную передачу защищаемых сведений между двумя компьютерами посредством акустиче-

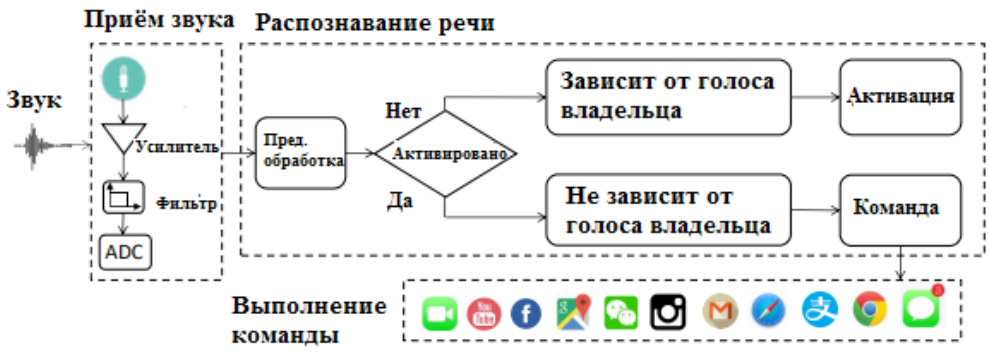


Рис. 1. Схема работы голосовых помощников

ских колебаний. В качестве акустических колебаний выступают ультразвуковые волны в диапазоне 17000-24000 Гц (данный диапазон частот выбран из функциональных возможностей динамиков и микрофонов). Так как ультразвук в большинстве случаев не способно воспринимать человеческое ухо, то рядовой пользователь никак не сможет на слух понять, что происходит утечка информации. Было проведено исследование в ходе которого происходила непрерывная запись в течение 5 часов всех шумов, циркулирующих в помещении, кроме того была открыта форточка откуда доносился индустриальный шум (рядом проходит оживлённая улица с большим количеством машин и людей).

Исходя из рисунка 2, видно, что речевая информация и индустриальные шумы, которые циркулируют в помещении, никаким образом не влияют на процесс записи и распознавания сигналов, которые ведутся при скрытой передачи с помощью ультразвуковых волн в силу отсутствия излучения в заданном диапазоне частот: 17000-20000 Гц, что повышает актуальность рассматриваемой угрозы.

Пусть в помещении имеются два компьютера (рис. 3). Компьютер А обрабатывает защищаемую информацию, оснащён внутренним динамиком и не имеет выход в Интернет. Компьютер В обрабатывает общедоступную информацию, оснащён микрофоном и имеет выход в сеть Интернет. С помощью заранее внедрённого вредоносного скрипта компьютер А преобразовывает информацию ограни-

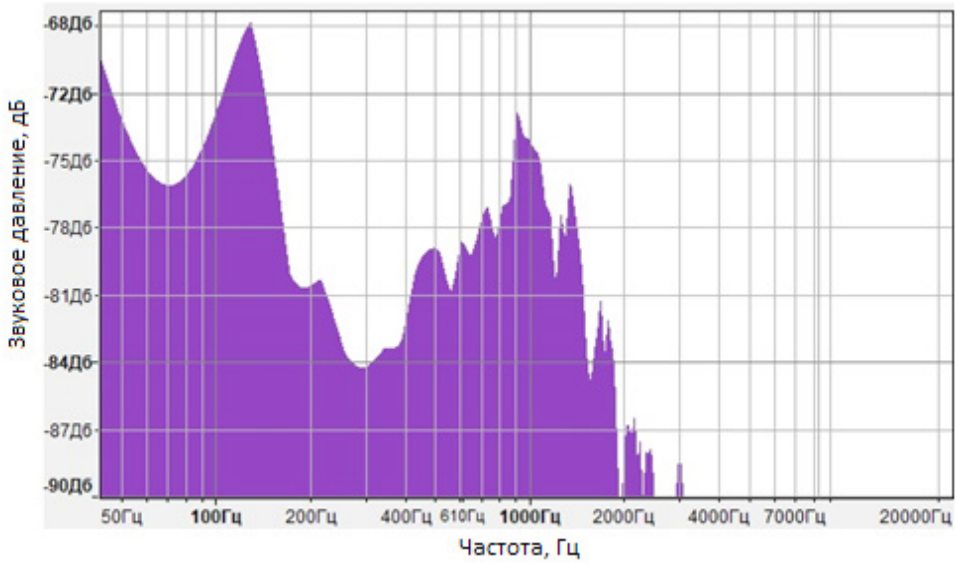


Рис. 2. АЧХ шума, циркулирующего в помещении в течении дня

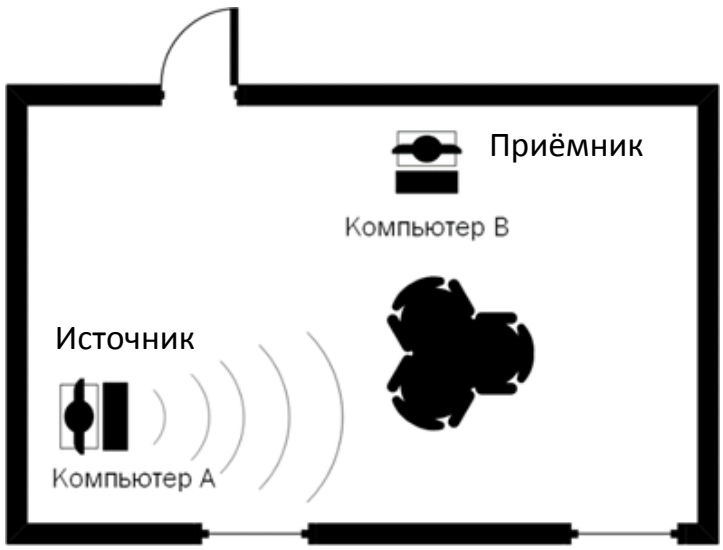
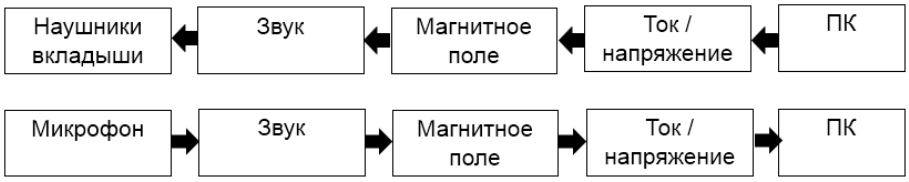


Рис. 3. Возможный сценарий атаки

ченного доступа в ультразвуковые колебания определённой частоты и излучает в эфир. Компьютер В с помощью микрофона прослушивает и записывает эфир в заданном диапазоне частот и, впоследствии, либо проводит демодуляцию полученных сигналов и получает исходные файлы, либо сразу передаёт данные в сеть Интернет.

Однако, принимать ультразвуковые колебания могут не только микрофоны, но и наушники. Стоит заметить, что микрофон и наушники на физическом уровне построены одинаково и отличаются лишь программной составляющей.



В чипах производителя звуковых карт Realtek есть функция под названием «jack retasking/ jack remapping», которая позволяет изменить функции/назначение порта на программном уровне. Эта особенность может использоваться в качестве реализации уязвимости для утечки речевой информации. Данное исследование было уже проведено автором в предыдущей статье. Злоумышленник может изменить назначение порта с выходного на входной без ведома пользователя и с помощью наушников записывать ультразвуковые колебания для последующей демодуляции и получения защищаемой информацией [2].

Существуют 4 возможных сценария реализации атаки. Исходные данные для всех ситуаций одинаковые:

• Имеется заражённый ПК, на котором обрабатывается защищаемая информация.

• Динамики (встроенные или переносные) излучают ультразвуковые колебания определённой частоты, формирующиеся путём перевода локальных файлов в неслышимый для человеческого уха сигнал.

1. Воздействие данного сигнала на ограждающие конструкции (окна), приводит к возникновению вибрационных колебаний промодулированных информативным сигналом. С помощью технических средств разведки возможна регистрация колебаний и дальнейшая расшифровка. Тем самым реализуется оптоэлектронный канал утечки информации.

2. В помещении имеется ещё один компьютер с подключённым к входному аудиогнезду микрофоном. С помощью данного записывающего устройства происходит регистрация акустических волн в заданном диапазоне частот, и отправка в сеть Интернет.

3. В помещении имеется ещё один компьютер с подключёнными к выходному аудиогнезду динамиками или наушниками. С помощью функции jack retasking злоумышленник переназначает выходной порт во входной выполняет все те же действия как в п. 2.

4. В помещении может находиться электронное устройство негласного получения информации, которое прослушивает эфир и при наличии акустических волн в заданном диапазоне частот записывает и отправляет данные по радиоканалу [3].

Для экспериментального исследования рассмотренной уязвимости были сгенерированы колебания с частотой 19000 Гц, которые излучались через встроенные динамики ноутбука HP 250 G6. Уровень громкости был выставлен на максимальный (64 дБ). Данные излучения были записаны на различном расстоянии с помощью стандартного средства звукозаписи Windows. В ходе проведения эксперимента в качестве приемной части ультразвуковых колебаний было исследовано звуковое оборудование, представленное в табл. 1.

Таблица 1

Экспериментальное оборудование

	Микрофон	**Наушники-вкладыши**	**Накладные наушники**
Название	OKLICK MP-M009B	PHILIPS SHE3550BK	PHILIPS SHL5000/00
Диапазон	50 – 23000 Гц	20 – 19000 Гц	9 – 24000 Гц
Чувствительность	58 дБ	95 дБ	104 дБ
Импеданс	—	32 Ом	24 Ом

Основными задачами исследования является определение применимости на практике данной уязвимости, а также определение максимальной дальности скрытой передачи информации при помощи ультразвуковых волн.

стотная характеристика ультразвукового сигнала записанного с помощью микрофона на расстоянии 1 метр.

Исходя из представленной выше таблицы видно, что данный канал утечки информации является актуальным и применимым на практике.

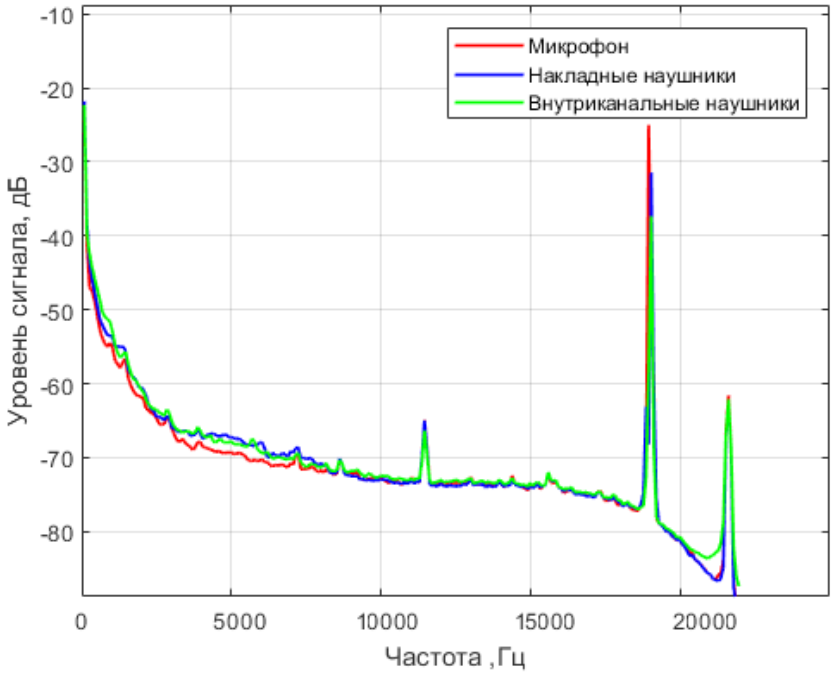


Рис. 4. Средний уровень сигнала на расстоянии 1 метр при записи через микрофон, накладные наушники, наушники-вкладыши

Исходя из рисунка 4, можно заметить, что более высоким качеством записи обладают накладные наушники по сравнению с наушниками-вкладышами. Разница в уровне сигнала от накладных наушников по сравнению с микрофоном составляет всего около 6 дБ. На рисунке 5 представлена амплитудно-ча-

Важным параметром при передаче различных сообщений является шаг частоты. Чем меньше этот шаг, тем больший объём информации можно будет передать. Стоит отметить, что при увеличении расстояния передачи увеличивается погрешность передачи частоты (рис. 6).

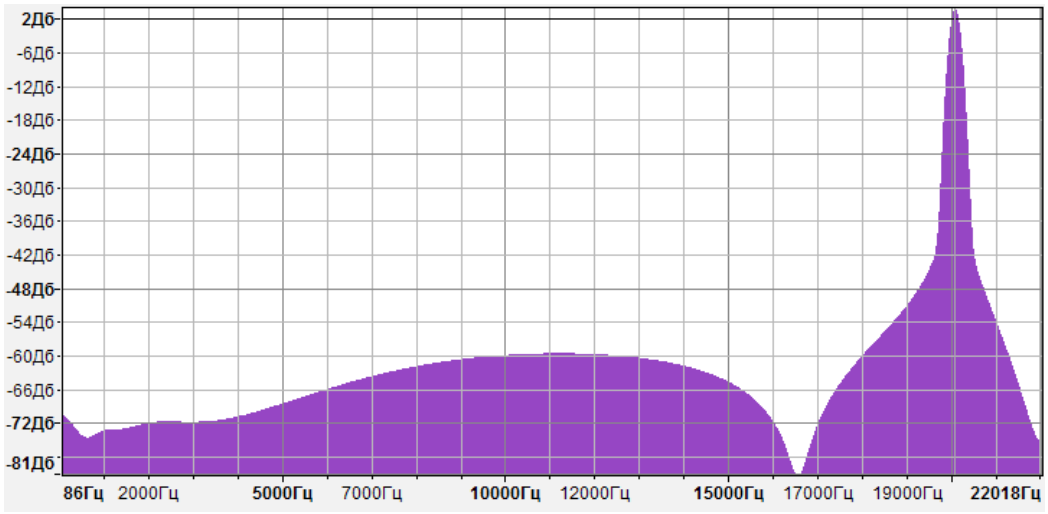


Рис. 5. АЧХ ультразвукового сигнала, сгенерированного на частоте 20200 Гц, записанная с помощью микрофона

Таблица 2

Зависимость расстояния от уровня сигнала

	Микрофон	Накладные наушники	Наушники вкладыши
1 метр	-25 дБ	-31 дБ	-38 дБ
3 метра	-30 дБ	-38 дБ	-46 дБ
5 метров	-40 дБ	-50 дБ	-68 дБ

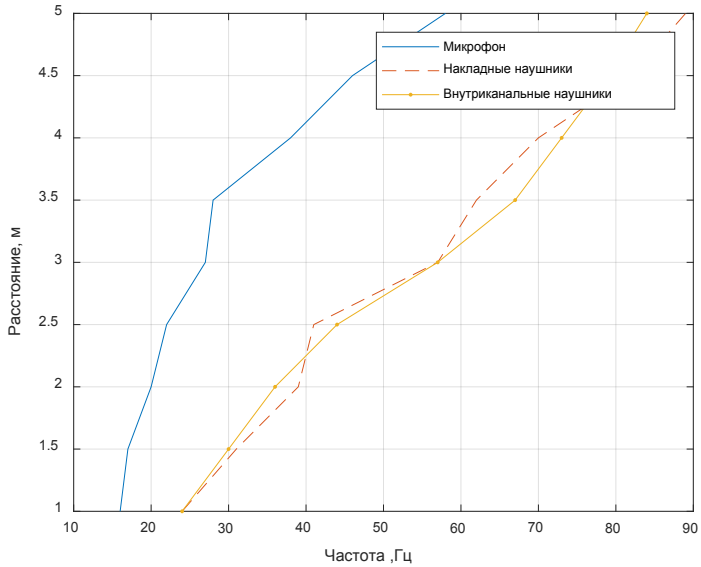


Рис. 6. Зависимость расстояния передачи от погрешности передачи частоты

Так при передаче ультразвуковых колебаний на расстоянии 1 метр средняя погрешность для микрофона составила ± 16 Гц, на расстоянии 3 метра ± 27 Гц, на расстоянии 5 метров ± 58 Гц. Экспериментальным путём было выявлено, что оптимальным шагом частоты, при котором достигается уверенное распознавание сигналов является 150 Гц. Данное числовое значение обеспечивает формирование полноценного алфавита. Таким образом, описанный технический канал утечки информации «Дельфин» является актуальным для большинства типовых офисных ситуаций, а вышеприведённые исследования доказали эффективность его реализации на практике.

Для противодействия данной атаке можно выделить 4 метода защиты:

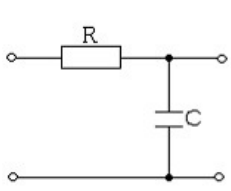
1. *Технический.* Доработка системы, регистрирующей акустические колебания, интегрирующей цепочкой, которая выполняет роль фильтра низких частот [4]. Следует ограничивать частотный диапазон до 20000 Гц.

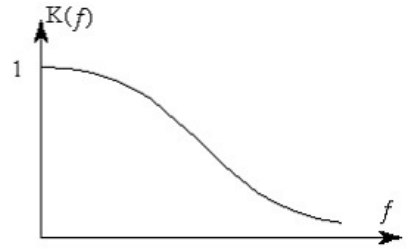
Рассчитаем значения сопротивления и ёмкости, при которых обеспечивается частота среза 20000 Гц. В качестве общего сопротивления возьмём 5 кОм. Входное напряжение = 1 В, а выходное = 0,7 В.

1) Определим входное напряжение Xc= $\frac{U_{вых} * R_{общ}}{U_{вх}} = \frac{0{,}7 * 5000}{1} = 3500$ Ом;

2) Определим сопротивление резистора *R=Робщ-Xc=5000-3500=1500 Ом;*

3) Определим ёмкость конденсатора: $X_c = \frac{1}{2\pi f c}$. Выразим ёмкость $C = \frac{1}{2\pi f X_c} = \frac{1}{2*3.14*20000*3500} = 2.23$ нФ;





4)Проверим частоту среза:

$$F_{ср} = \frac{1}{2\pi X_C C} = \frac{1}{2*3.14*3500*2.23*10^{-9}} \approx 20000 \text{ Гц}$$

Таким образом для построения фильтра низких частот, который будет ограничивать все частоты выше 20000 Гц, следует применить резистор сопротивлением 1.5 кОм (например, CF-50), а конденсатор ёмкостью 0.22 мкФ (например, К10-17А Н50). Данные значения конденсатора и резистора являются достаточно распространёнными и доступными в продаже, что повышает практическую реализацию данного метода.

2. *Организационный.* Запрет в организациях использования наушников, микрофонов, а также динамиков без предусилителей [5]. Во избежание переназначения портов, следует извлекать наушники из аудиогнезда, когда они не используются по назначению. Данный метод является одним из самых эффективных и наименее затратным.

3. *Программный.* Отключение звукового оборудования в настройках BIOS. Это может предотвратить вредоносный доступ аудиокодека из операционной системы. Однако, использование данной конфигурации является приемлемым методом только для организаций, так как отключение звукового оборудования ведёт к невозможности прослушивания аудиозаписи и ведения конференц-переговоров. Использование сертифицированных средств защиты информации от несанкционированного доступа [5].

4. *Использование ультразвукового подавителя в помещении.* Достоинством является бесшумный режим работы, не влияющий на психологическое состояние человека, однако данный метод является самым финансово затратным.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Литература

1. Catalin Cimpanu., Hackers can use ultrasounds to take control of Alexa, Siri, Cortana, others, [Электронный ресурс] // https://www.bleepingcomputer.com/news/security/hackers-can-use-ultrasounds-to-take-control-of-alexa-siri-cortana-others/. (Дата обращения 15.08.2018).

2. Asyaev G.D., Antyasov I.S. Using headphones to implement a technical channel for the leakage of voice information // 2018 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) / 2018, P. 229-232.

3. Макаров Ю.К., Хорев А.А. Методы защиты речевой информаци и оценки их эффективности // Защита информации. – Конфидент.: 2001. - № 4, С. 22-33.

4. Сапожков М.А. Акустика // Справочник. – М.: Радио и связь 1998. – С. 186-192.

5. Фучко М.М., Широких А.В., Захаров А.А., Несговоров Е.С., Оленников Е.А. Аудиовыход как скрытый канал утечки данных: технологии создания и методы защиты //Вестник УрФО. Безопасность в информационной сфере. – Челябинск: Изд. Центр ЮУрГУ, 2016. - № 3(21) С. 26-30.

References

1. Catalin Cimpanu., Hackers can use ultrasounds to take control of Alexa, Siri, Cortana, others, [Elektronnyy resurs] // https://www.bleepingcomputer.com/news/security/hackers-can-use-ultrasounds-to-take-control-of-alexa-siri-cortana-others/. (Data obrashcheniya 15.08.2018).

2. Asyaev G.D., Antyasov I.S. Using headphones to implement a technical channel for the leakage of voice information // 2018 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT) / 2018, P. 229-232.

3. Makarov YU.K., Khorev A.A. Metody zashchity rechevoy informatsi i otsenki ikh effektivnosti // Zashchita informatsii. – Konfident.: 2001. - № 4, S. 22-33.

4. Sapozhkov M.A. Akustika // Spravochnik. – M.: Radio i svyaz' 1998. – S. 186-192.

5. Fuchko M.M., Shirokikh A.V., Zakharov A.A., Nesgovorov Ye.S., Olennikov Ye.A. Audiovykhod kak skrytyy kanal utechki dannykh: tekhnologii sozdaniya i metody zashchity //Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. – Chelyabinsk: Izd. Tsentr YUUrGU, 2016. - № 3(21) S. 26-30.

АСЯЕВ Григорий Дмитриевич, студент высшей школы электроники и компьютерных наук кафедры "Защита информации" Южно-Уральского Государственного Университета. Россия, 454080, г.Челябинск, проспект Ленина, д.76. E-mail: asyaev1996@mail.ru

ASYAEV Grigoriy, Higher School of Electronics and Computer student of the Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: asyaev1996@mail.ru

АНТЯСОВ Иван Сергеевич, руководитель, старший преподаватель кафедры "Защита информации научный " Южно-Уральского Государственного Университета. Россия, 454080, г. Челябинск, проспект Ленина, д.76. E-mail: antiasovis@susu.ru.

ANTYASOV Ivan, research manager, senior teacher Department of Science "Information security" of the South Ural State University. Russia, 454080, Chelyabinsk, Lenin Avenue, 76. E-mail: antiasovis@susu.ru.