УДК 004.451

Вестник УрФО № 3(33) / 2019, с. 5–11

**Беляев Д. О., Волчков Д. Н., Поршнев С. В.**

DOI: 10.14529/secur190301

# *О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА КАК УСТРОЙСТВА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К РЕЧЕВОЙ ИНФОРМАЦИИ*

*Статья посвящена исследованию возможности перехвата потенциаль-ным злоумышленником акустической речевой информации с использованием микрофонов, встроенных или подключенных к ПЭВМ, функционирующих под управлением операционных систем Windows 7, Windows 10 и Ubuntu 16.04, а также передачи данной информации по локальной вычислительной сети. Изучены особенности функционирования устройств звукозаписи и тех-нологии обработки звуковых сигналов, используемые в ПЭВМ, и пути проникновения в операционную среду, также описаны действия, обеспечиваю-щие захват звука с микрофона и передачу аудиоинформации по локальной вычислительной сети.*

***Ключевые слова:*** *акустический речевой сигнал; ПЭВМ; звуковая кар-та; канал утечки речевой информации; программное обеспечение.*

**Belyaev D. O., Volchkov D. N., Porshnev S. V.**

# *ON THE POSSIBILITY OF USING A PERSONAL COMPUTER AS THE DEVICE UNAUTHORIZED ACCESS TO SPEECH INFORMATION*

*The article is devoted to the study of the possibility of interception by a potential attacker of acoustic speech information using MIC-rophones, built-in or connected to a PC, operating systems running Windows 7, Windows 10 and Ub-untu 16.04, as well as the transfer of this information on the local area network. The peculiarities of the functioning of recording devices, and technologies about the creation of audible signals used in personal computer, and pathways in the operating environment, also describes the steps that can capture audio from a microphone and transmitting audio information over a local area network*

***Keywords:*** *acoustic speech signal; a personal computer; sound card; chan-nel of leak of the speech information; software.*

**Введение**

Практически каждая современная ПЭВМ, используемая для обработки, хранения и передачи информации, снабжена звуковой картой – платой рас-ширения, которая используется для регистрации, воспроизведения и обра-ботки звуковых сигналов [1]. Звуковые карты обеспечивают полный дуп-лексный режим (Full Duplex), т.е. позволяют одновременно принимать (запи-сывать) и передавать (воспроизводить) аудиоинформацию [2]. В этой связи была высказана гипотеза о том, что данные устройства, потенциально, могут использоваться, как основа образования канала утечки информации акусти-ческой речевой информации [7] без использования специально разработан-ных для решения подобных задач технических устройств (например, при размещении ПЭВМ, оснащенной звуковой картой и имеющей выход в вычислительные сети, в помещениях для ведения конфиденциальных перегово-ров). В статье приводятся экспериментальные результаты, подтверждающие сформулированную выше гипотезу.

**Методика проведения исследования**

Для реализации процесса перехвата речевого сообщения штатными средствами ПЭВМ и его передачи по локальной компьютерной сети исполь-зовался программно-аппаратный комплекс, состоящий из 2-х ПЭВМ, на од-ной из которых осуществлялся захват аудиосигнала со встроенных устройств звукозаписи и его передача через локальную вычислительную сеть на вторую ПЭВМ, где принятая аудиоинформация преобразовывалась в звуковой сигнал, воспроизводимый через динамики второй ПЭВМ.

Для исследования возможности получения акустической речевой ин-формации, ее передачи и воспроизведения на кроссплатформенном языке программирования Java в демонстрационных целях было разработано спе-циальное программное обеспечение. Выбор данного программного обеспе-чения обеспечил компиляцию исполняемых модулей разработанного ПО, работающих как под управлением ОС Windows 7 и 10, так и ОС Ubuntu 16.04.

В рамках проведения исследовательской работы использовался пакет Javax.sound. sampled, который обеспечивал возможность захвата, обработки и воспроизведения аудиоданных [3]. Отметим, что для задания формата аудиозаписи в пакете Javax.sound.sampled имеются два типа конструкторов, использующих переменные [3], описание которых приведено в таблице 1.

Первый конструктор позволяет выбрать один из реализованных в биб-лиотеке Javax. sound.sampled форматов кодирования звука: ALAW (сжатие звука по алгоритму a-Law – алгоритму преобразования 16-битных PCM-сигналов в нелинейный 8-битный формат [6]); PCM_FLOAT (PCM-кодирование с плавающей запятой); PCM_SIGNED (знаковое представление PCM-сигнала в 16-битном формате); PCM_ UNSIGNED (беззнаковое пред-ставление PCM-сигнала в 8-битном формате); ULAW (сжатие звука по алго-ритму μ-Law – алгоритму преобразования 16-битных PCM-сигналов в нели-нейный 8-битный формат, отличие от a-Law – методы кодирования и деко-дирования [6]).

Второй конструктор использует по умолчанию метод кодирования PCM (Pulse-code modulation) [5] – импульсно-кодовую модуляцию оцифро-ванного звукового сигнала, полученного на выходе линейного 16-битового АЦП.

Анализ функционала ОС Windows 7 и 10 показал, что для дистанцион-ного включения микрофона и управлениями такими его параметрами, как «Подавление шума» и «Подавление эхо», могут использоваться утилиты командной строки SubInACL.exe и SetACL.exe [4], позволяющие получить в полный доступ к разделу реестра HKEY_LOCAL_MACHINE, от-

*Таблица 1*

**Переменные конструктора**

| Название переменной | Тип переменной |
|---|---|
| **encoding** (техника кодирования звука) | protected **AudioFormat.Encoding** |
| **sampleRate** (количество кадров в секунду, частота дискретизации) | protected float |
| **sampleSizeInBits** (количество бит для кодировки каждого кадра, разрядность) | protected int |
| **channels** (количество каналов) | protected int |
| **frameSize** (количество байт, для записи каждого кадра) | protected int |
| **frameRate** (количество кадров, записанных в секунду) | protected float |
| **bigEndian** (параметр, указывающий на то, как хранятся аудиоданные для одной выборки, с прямым или обратным порядком байт) | protected boolean |

вечающему за запись звука, и всем его подразделам, отвечающим за подавление шума и подавление эхо. Элементы управления настройкой звука реализованы в виде подкласса FloatControl, обеспечивающий управление диапазоном значений с плавающей точкой, класса Control. С помощью данного подкласса можно настроить элемент управления MASTER_GAIN, который является элементом управления общего уровня усиления на линии, если звуковая карта поддер-живает данный элемент управления. Также в ходе исследования были опре-делены функции ОС, позволяющие производить скрытую настройку пара-метров конфиденциальности микрофона.

В ОС Ubuntu 16.04 для регулирования большого количества парамет-ров работы со звуком используется встроенный аппарат микширования Al-samixer для Advanced Linux Sound Architecture (ALSA).

Передача аудиосигнала от одного компьютера к другому осуществля-лась в соответствии с протоколом UDP (User Datagram Protocol), правильный выбор которого для трансляции аудосигналов в режиме реального времени был подтвержден результатами проведенного исследования. Отметим, что для работы с UDP протоколом в Java используются два класса: класс DatagramPacket, обеспечивающий задание значений IP-адреса и номера пор-та компьютера, на который будет передан аудиосигнал, и класс DatagramSocket, обеспечивающий задание значений длину буфера в байтах; адрес, на который будет отправлена датаграмма; номер порта, который уда-ленный компьютер использует для получения датаграммы, а также размеще-ния в предаваемых пакета собственно аудиоинформации. Оказалось, что по-теря пакетов во время трансляции аудиоинформации между компьютерами и, как следствие, потеря небольшого количества данных не приводили к зна-чительным, с точки зрения эксперта, искажениям воспроизводимого звуково-го сигнала. После поступления данных в выбранный порт, они записывались в поток SourceDataLine в выбранном формате, далее полученный аудиосиг-нал проходил программную процедуру усиления с помощью элемента управления MASTER_GAIN, преобразовывался в аналоговый сигнал, кото-рый передавался на динамики ПЭВМ.

**Анализ результатов исследования**

Рассмотрим результаты использования разработанного программного обеспечения. Интерфейс программы, запущенной на принимающем аудио-информацию компьютере представлена на рисунке 2

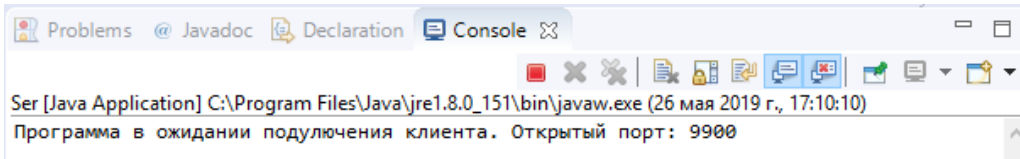


Рис. 2. Интерфейс программы, запущенной на принимающем компьютере, в режиме ожидания (ОС Windows 10)

Из рисунка 2 видно, что программа находится в режиме готовности приема аудиоинформации, передаваемой по локальной сети через порт 9900. После запуска на передающем компьютере соответствующего про-

граммного кода, у которого, по понятным причинам, интерфейс пользователя не предусмотрен, начинается передача звуковых сигналов, регистрируемых микро-фоном данного компьютера (рисунок 3).

Далее полученная аудиоинформация по мере ее поступления декоди-ровалась, преобразовывалась в аналоговый сигнал и передавалась на звуко-вые динамики для ее прослушивания. Технические характеристики ПЭВМ (ОС

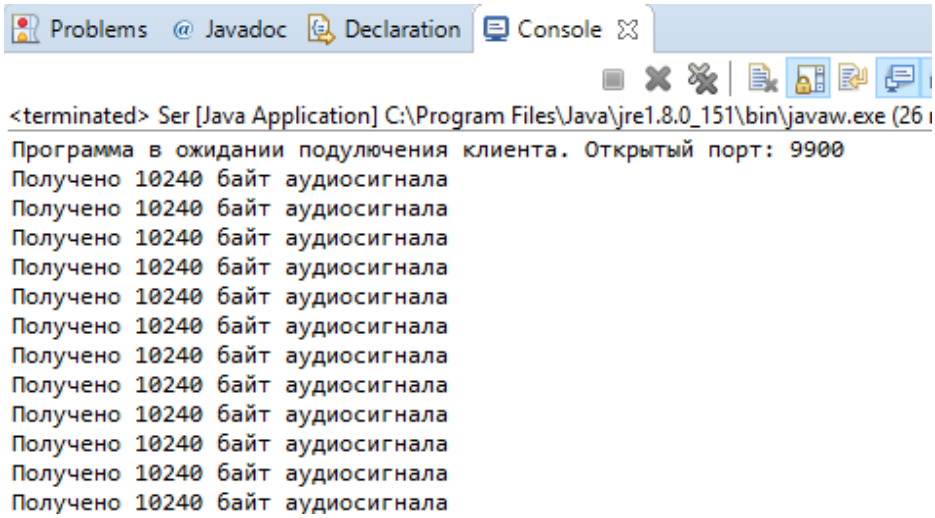


Рис. 3. Интерфейс программы, запущенной на принимающем компьютере, в режиме получения аудиоинформации (ОС Windows 10)

Из рисунка 3 видно, что факт приема каждой дейтаграммы сопровожда-ется выводом сообщения о получении 10240 байт.

Соответствующий интерфейс программы, работающий под управлением ОС Ubuntu 16.04, представлен на рисунке 4.

на ПЭВМ инсталлировались в зависимости от очередности исследова-тельских задач) и звуковых карт, использовавшихся в проведенных экспери-ментах, представлены в таблице 2.

Оказалось, что задержка между произнесенным и переданным звуко-выми сигналами

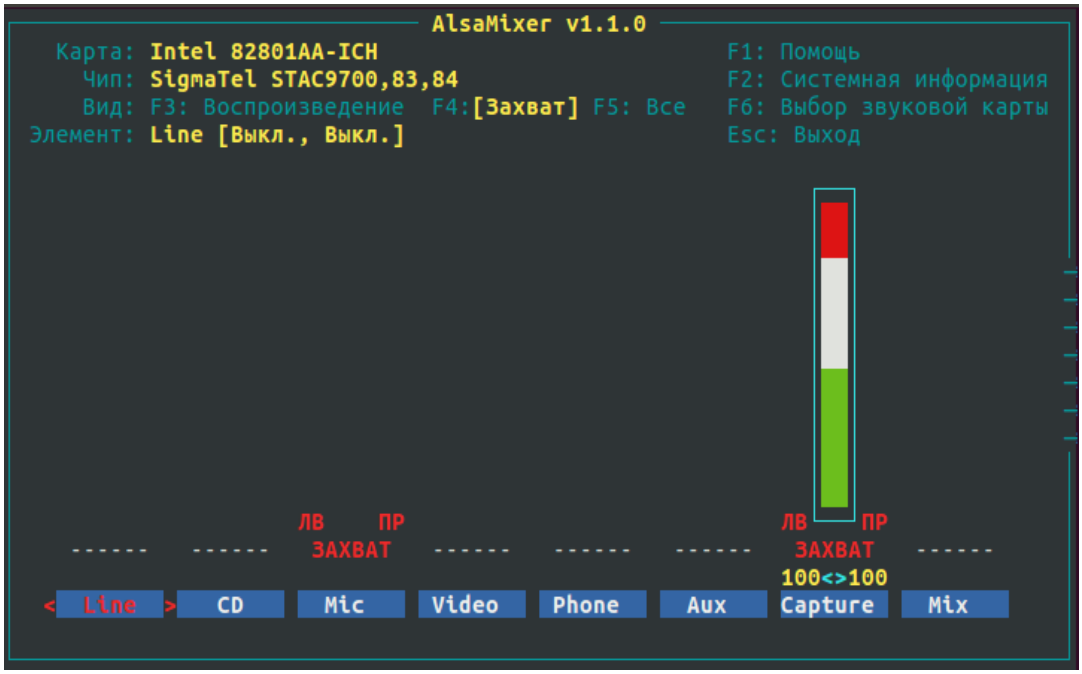


Рис. 4. Интерфейс программы, запущенной на принимающем компьютере, в режиме получения аудиоинформации (ОС Ubuntu 16.04)

*Таблица 2*

**Наименование и характеристики ПЭВМ и звуковых карт, использовавшихся при проведении экспериментов**

| ПЭВМ передающей стороны | | | |
|---|---|---|---|
| Наименование ПЭВМ | Технические характеристики ПЭВМ | Наименование звуковой карты | Технические характеристики звуковой карты |
| Ноутбук Acer Extensa EX2520-51D5 | Процессор: Intel Core i5-6200U Тактовая частота процессора: 2300 МГц Объем оперативной памяти: 6 Гб Тип памяти: DDR3-1600 Видеокарта: NVID-IA GeForce 940M Объем жесткого диска: 1000 Гб Тип жесткого диска: HDD Интерфейс жесткого диска: Serial ATA Макс. скорость адаптера LAN: 1000 Мбит/с Емкость аккумуля-тора: 2520 мА·ч Wi-Fi: 802.11 a/b/g/n/ac | Intel High-Definition Audio Realtek ALC255 | 20-разрядный ЦАП; частоты дискретизации 32кГц/44,1кГц/48кГц /96кГц; программный выбор напряжения питания микрофона 3,3 В и 5 В; программный выбор усиления +6/12/20/30 дБ для аналогового микрофонного входа |
| ПЭВМ приемной стороны | | | |
| Наименование ПЭВМ | Технические характеристики ПЭВМ | Наименование звуковой карты | Технические характеристики звуковой карты |
| Ноутбук Asus K50IN | Процессор: Intel Pentium Dual-Core T4300 Тактовая частота процессора: 2100 МГц Объем оперативной памяти: 4 Гб Тип памяти: DDR2 Видеокарта: NVID-IA GeForce G 102M Объем жесткого диска: 250 Гб Тип жесткого диска: HDD Интерфейс жесткого диска: Serial ATA Макс. скорость адаптера LAN: 1000 Мбит/с Емкость аккумуля-тора: 2520 мА·ч Wi-Fi: 802.11 a/b/g/n/ac | Intel High-Definition Audio Realtek ALC662 | Шестиканальный ЦАП с поддержкой 16/20/24-разрядных форматов PCM; частоты дискретизации 44,1кГц/48кГц /96кГц; программный выбор напряжения питания микрофона 2,5 В и 3,2 В; программный выбор усиления +10/20/30 дБ для аналогового микрофонного входа |

при использовании ОС WIINDOWS 7, 10 составила порядка 2 с, при использовании ОС Ubuntu 16.04 – задержка между сигналами экс-пертом не обнаруживалась. При этом качество воспроизводимого звукового сигнала при нахождении источника звукового сигнала на удалении 3 м от микрофона оказалось таковым, что экспертом было распознано 100% кон-тента речевой информации.

**Заключение**

Результаты экспериментов, проведенных в соответствие в разработан-ной методикой, подтверждают гипотезу о возможности использования пер-сонального компьютера, подключенного к локальной вычислительной сети, в качестве устройства несанкционированного получения акустической речевой информации, например, в случае запуска

злоумышленником соответствую-щей программы, ранее установленной на ПЭВМ, находящейся в помещении для проведения конфиденциальных мероприятий, перед проведением соот-ветствующего мероприятия.


**Литература**

1. Устройство звуковой карты – URL: http://refleader.ru/jgeujgotr.html – (дата обращения: 02.04.2019).

2. Мураховский В. Железо ПК. – URL: https://ru.scribd.com/doc/13164129/pc#15 – (дата обращения: 02.04.2019).

3. Формат записи. – URL: https://docs.oracle.com/javase/7/docs/api/javax/sound/sampled/AudioFormat.html – (дата обращения: 02.04.2019).

4. Доступ к микрофону. – URL: https://getadmx.com/?Category=Windows_10_2016&Policy=Microsoft.Policies.AppPrivacy::LetAppsAccessMicrophone&Language=ru-ru – (дата обращения: 02.04.2019).

5. Формат кодирования. – URL: https://docs.oracle.com/javase/7/docs/api/javax/sound/sampled/AudioFormat.Encoding.html – (дата обращения: 02.04.2019).

6. Термины – Glossary. – URL: https:// http://kanst.mediatory.ru/index.files/vegas7/v7rus/Glossary2.htm – (дата обращения: 02.04.2019).

7. Зайцев А.П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.

**References**

1. Ustrojstvo zvukovoj karty – URL: http://refleader.ru/jgeujgotr.html – (data obrashhenija: 02.04.2019).

2. Murahovskij V. Zhelezo PK. – URL: https://ru.scribd.com/doc/13164129/pc#15 – (data obrashhenija: 02.04.2019).

3. Format zapisi. – URL: https://docs.oracle.com/javase/7/docs/api/javax/sound/sampled/AudioFormat.html – (data obrashhenija: 02.04.2019).

4. Dostup k mikrofonu. – URL: https://getadmx.com/?Category=Windows_10_2016&Policy=Microsoft.Policies.AppPrivacy::LetAppsAccessMicrophone&Language=ru-ru – (data obrashhenija: 02.04.2019).

5. Format kodirovanija. – URL: https://docs.oracle.com/javase/7/docs/api/javax/sound/sampled/AudioFormat.Encoding.html – (data obrashhenija: 02.04.2019).

6. Terminy – Glossary. – URL: https:// http://kanst.mediatory.ru/index.files/vegas7/v7rus/Glossary2.htm – (data obrash-henija: 02.04.2019).

7. Zajcev A.P. Tehnicheskie sredstva i metody zashhity informacii: Uchebnik dlja vuzov / A.P. Zajcev, A.A. Shelupanov, R.V. Meshherjakov i dr.; pod red. A.P. Zajceva i A.A. Shelupanova. – M.: OOO «Izdatel'stvo Mashinostroenie», 2009. – 508 s.



**БЕЛЯЕВ Дмитрий Олегович,** старший преподаватель Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 19. E-mail: belyaev-urfu@yandex.ru

**ВОЛЧКОВ Дмитрий Николаевич,** бакалавр Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 19. E-mail: vlc_d.n.@mail.ru

**ПОРШНЕВ Сергей Владимирович,** доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», 620002, г. Екатеринбург, ул. Мира, 19; ведущий научный сотруд-

ник Федеральное государственное бюджетное учреждение науки «Институт математики и механики им. Н.Н. Красовского» Уральского отделения Российской академии наук, 620990, г. Екатеринбург, ул. Софьи Ковалевской, 16; E-mail: s.v.porshnev@urfu.ru

**BELYAEV Dmitry,** Senior Lecturer of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, B.N.Yeltsin Ural Federal University, Ekaterinburg, 620002, Mira street, 19. E-mail: belyaev-urfu@yandex.ru

**VOLCHKOV Dmitry,** Bachelor of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, B.N. Yeltsin Ural Federal University., Mira str., 19, Ekaterinburg, 620002, Russia. E-mail: vlc_d.n.@mail.ru

**PORSHNEV Sergey,** Dr.Sc., Professor, head of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, B.N.Yeltsin Ural Federal University, Ekaterinburg, 620002, Mira street, 19; Leading Researcher of The N.N. Krasovskii Institute of Mathematics and Mechanics of the Ural Branch of the Russian Academy of Sciences, S. Kovalevskaja str. 16, Yekaterinburg, 620990, Russia. E-mail: s.v.porshnev@urfu.ru