СПОСОБ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В ОФИСНОМ ПОМЕЩЕНИИ

Алексеев В.В.[1], Клинков Д.А.[2], Яковлев А.В.[3]

Ключевые слова: *акустовибрационный канал, речевой сигнал, утечка информации, программно-аппаратный комплекс, речеподобная реверберационная помеха, генератор шума, коэффициент словесной разборчивости, уровень защищенности помещения, программное обеспечение.*

Аннотация

Цель работы: разработка способа обеспечения информационной безопасности офисного помещения от утечки информации по акустовибрационному каналу, основанного на применении речеподобной помехи, а также установление соответствия процедуры применения способа существующей нормативной правовой базе.

Методы: информационно-правовой анализ, спектральный и системный анализ, теория моделирования и подобия.

Результаты: обоснована эффективность применения речеподобной помехи при защите офисного помещения от утечки информации по акустовибрационному каналу; разработан способ защиты офисного помещения от утечки информации по акустовибрационному каналу; в систематизированном виде представлены его достоинства по сравнению с аналогичными средствами защиты информации; представлен вариант программно-аппаратного комплекса для его реализации; описано разработанное программное обеспечение, необходимое для генерации речеподобной реверберационной помехи и организации режима прерывания при отсутствии источника речевого сигнала; проведен вычислительный эксперимент по сравнительной оценке эффективности использования помех специального типа для защиты информации в офисном помещении; исследованы правовые вопросы обеспечения информационной безопасности и установлено соответствие процедуры применения способа положениям существующих нормативных правовых актов, относящихся к области технической защиты информации.

DOI: 10.21681/1994-1404-2023-2-44-53

Введение

В век информатизации существует, к сожалению, устойчивый спрос на информацию, добытую несанкционированным путем. Это является большой проблемой для организаций, осуществляющих обмен информацией в помещениях офисного типа. Следовательно, защита информации от злоумышленников является одной из актуальных задач научных исследований в области *информационной безопасности* [10].

Свойства информации в результате речевого взаимодействия людей, а именно: возможность идентификации личности, своевременность получения сведений и уровень конфиденциальности делают такую информацию более ценной, что и вызывает повышенный интерес у злоумышленников. Поэтому одна из важнейших задач в области информационной безопасности — защита конфиденциальной речевой информации от ее утечки по техническим каналам.

Анализ литературы в данной предметной области [1, 3, 5, 7, 10, 11, 16, 17] показал, что в настоящее время выделяют следующие технические каналы утечки речевой информации в помещениях: прямой акустический (воздушный), акустовибрационный (вибрационный), акустоэлектромагнитный (параметрический), акустоэлектрический, акустооптический (лазерный).

Основой для построения систем защиты информации от утечки по техническим каналам является национальный стандарт[4] Российской Федерации по защите информации.

[4] ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, 2009.

[1] ***Алексеев Владимир Витальевич****, доктор технических наук, профессор, член-корреспондент РАЕН, почетный радист РФ, заведующий кафедрой информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: vvalex1961@mail.ru

[2] ***Клинков Дмитрий Александрович,*** *оператор научной роты Межвидового центра подготовки и боевого применения войск радиоэлектронной борьбы, г. Тамбов, Российская Федерация.*

E-mail: dmitkast1996@mail.ru

[3] ***Яковлев Алексей Вячеславович,*** *кандидат технических наук, доцент, доцент кафедры информационных систем и защиты информации Тамбовского государственного технического университета, г. Тамбов, Российская Федерация.*

E-mail: yava73@bk.ru

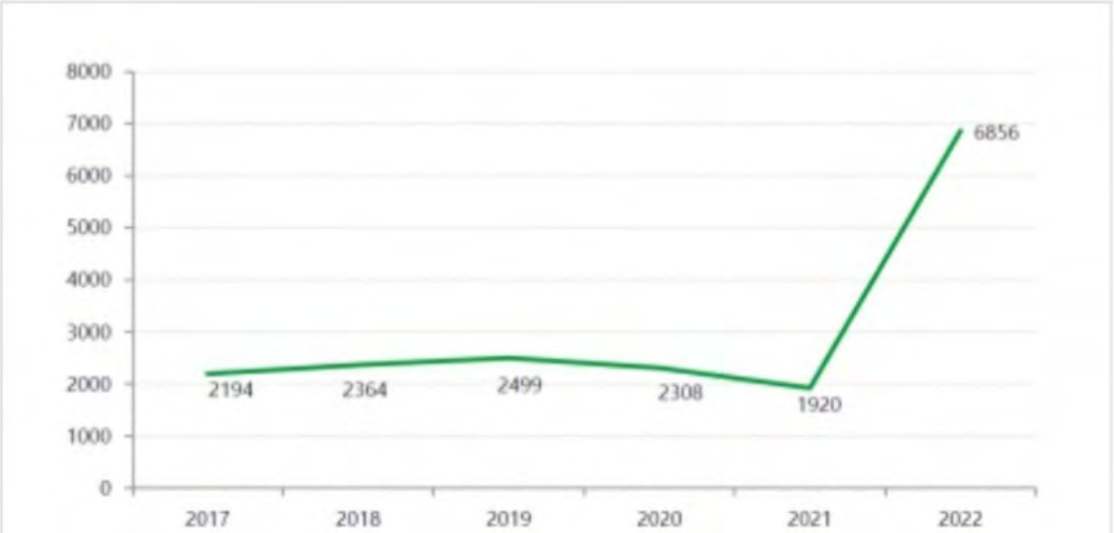


Рис. 1. Количество утечек данных

Динамика утечки речевой информации

Согласно исследованиям экспертно-аналитического центра компании *InfoWatch*[5], была выявлена мировая тенденция увеличения количества утечек по техническим каналам речевой информации за последние 5 лет (*рис. 1*).

Число утечек речевой информации выросло почти в два раза в мире и в полтора раза — в России (по сравнению с 1 полугодием 2021 г.)[6]. Кроме того:

- во всем мире в первой половине года «утекли» около 3 *млрд* записей персональных данных и платежной информации;
- более 30% информации, представленной на теневых форумах, украдено из компаний США, 13% — из российских компаний;
- количество скомпрометированных записей в России за первое полугодие 2022 г. превысило население страны — более 187 *млн* записей;
- доля утечек, вызванных умышленными нарушениями, превысила 96%;
- более 80% утечек информации спровоцированы хакерскими атаками;
- зафиксирован существенный рост утечек информации категории «коммерческая тайна» — ее доля превысила 13%;
- резко выросла доля утечек в промышленности и в торговле.

По итогам первой половины 2022 г. экспертно-аналитическим центром компании *InfoWatch* зарегистрирована 2 101 утечка информации ограниченного доступа в мире, что почти в два раза (на 93,2%) больше, чем за аналогичный период предыдущего года (*рис. 2*). Количество утечек в России за первое полугодие 2022 г. составило 305 (на 45,9% больше по сравнению с I полугодием 2021 г.).

Нормативные правовые требования в области защиты информации

В процессе исследования уточнены цели правовых, организационных и технических мер в области защиты информации:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;
- соблюдение конфиденциальности информации, имеющей ограничение доступа;
- реализация права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления *требований* к защите информации, а также *ответственности* за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации. К *правовой* защите информации относится защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль над их исполнением[7]. В этой связи исследованы *требования* основных нор-

[5] Компания *InfoWatch* — ведущий российский разработчик решений для обеспечения информационной безопасности организаций.

[6] Отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года // Infowatch. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения: 21.02.2023); Актуальные киберугрозы: итоги 2022 года // Positive technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022 (дата обращения: 21.02.2023); Потери от утечек данных // Tadviser. URL: https://www.tadviser.ru/index.php (дата обращения: 21.02.2023).

[7] ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения, 2008.

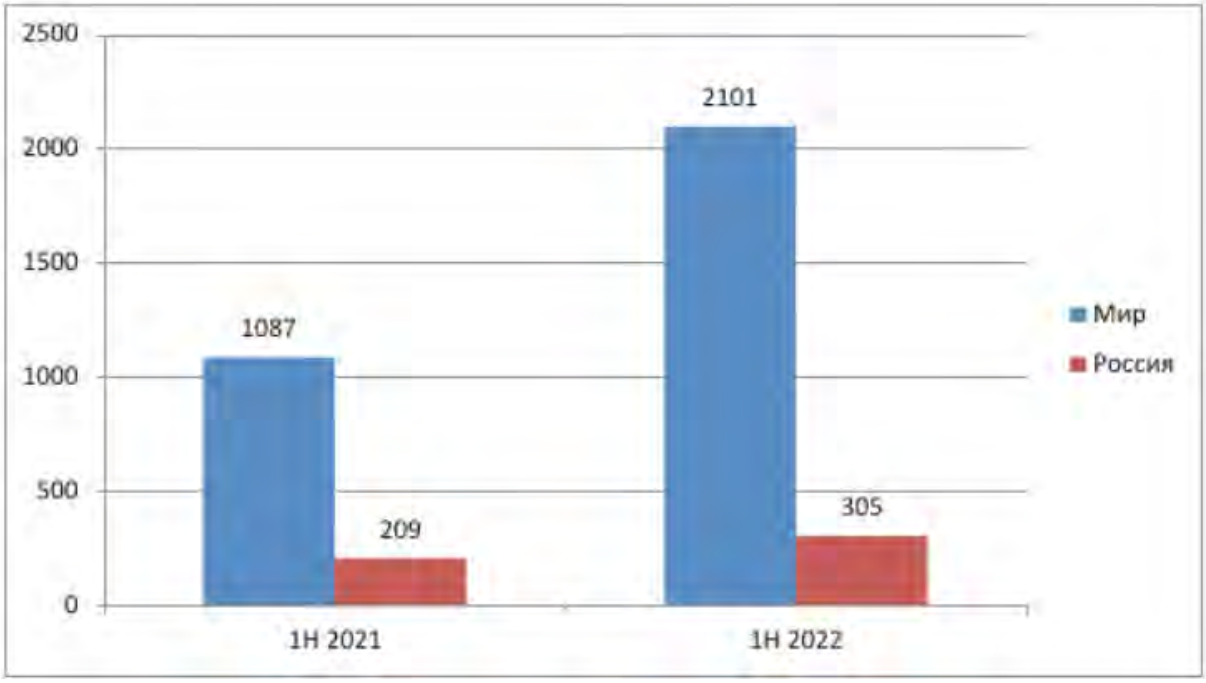


Рис. 2. Число утечек данных в мире и России в первых полугодиях 2021 и 2022 гг.

мативных правовых актов, относящихся к технической защите информации, включая:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне».

Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»;

Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне».

Положения данных нормативных правовых актов применяются при организации защиты информации от утечки по акустовибрационному каналу в помещениях офисного типа.

Как известно, акустовибрационный канал утечки информации характерен для двух видов акустической разведки: речевой и сигнальной. Основным *недостатком* технических средств защиты информации по акустовибрационному каналу является то, что при их создании требования нормативных документов по обеспечению комфортного ведения переговоров играют второстепенную роль [2]. Проведенные исследования показали, что применение речеподобной помехи в сочетании с «Акустоматом»[8] позволяет обеспечить эти требования [15].

В связи с этим противодействие нарушению *конфиденциальности* информации по акустовибрационному каналу в помещениях офисного типа приобретает особое значение в условиях всё возрастающей актуальности противодействия техническим средствам разведки. При этом решение задачи разработки *способа*, обеспечивающего *гарантированную* [8] защиту речевой информации в офисном помещении, предопределяет совершенствование существующих и разработку новых математических моделей и алгоритмов, формирующих и передающих помеховый сигнал.

Проблема защиты речевой информации

Акустовибрационный канал включает следующие компоненты: источник сигнала, среда распространения, агент, принимающий данные. Его особенностью является то, что для получения конфиденциальной информации нет необходимости проникновения в помещение. Устройство нелегального съема акустовибрационной информации может быть установлено вне охраняемого помещения, что порождает трудность его нахождения и сравнительную легкость монтажа.

[8] «Акустомат» — программный модуль генератора реверберационной помехи, предназначенный для прерывания ее генерации при отсутствии речевого сигнала субъектов переговоров в офисном помещении.

Принцип работы канала основан на способности звуковой волны вызывать механические колебания в препятствиях, через которые она проходит при распространении. Эти колебания при помощи соответствующего оборудования и программного обеспечения преобразуются в связный текст. При исследовании проведен анализ основных конструкций, пропускающих речевую информацию: несущие стены и перегородки, перекрытия, оконные рамы, коробы дверных проемов, стекла, трубы тепло- и водоснабжения, каналы вентиляции [13].

Устройства съема речевой информации — стетоскопы (диагностические приборы) и контактные микрофоны, способные преобразовывать получаемую в виде механических колебаний информацию в акустический сигнал. Преобразование происходит в два этапа: сначала данные переводятся в формат электромагнитных колебаний, затем в акустическую информацию. Такое преобразование не всегда дает возможность воспроизвести разборчивую речь, но часть сведений можно получить путем программного восстановления смысла по контексту.

Устройство съема речевой информации может быть установлено на перегородку со стороны соседнего офиса или на трубы системы отопления и водоснабжения. Поиск затрудняется из-за невозможности свободно проводить обследования помещений, принадлежащих другим собственникам. Сложность поиска, непредсказуемость места установки повышают вероятность пропуска устройства съема информации. Проще, дешевле и оперативнее применять средства защиты информации с *речеподобной помехой*.

Противодействовать утечке информации по акустовибрационному каналу при ведении переговоров в офисном помещении целесообразно активными методами, в том числе используя естественные помехи.

Естественные помехи, связанные с работой систем жилищно-коммунального хозяйства, снижают уровень разборчивости сигнала, но к ним необходимо добавить помехи, имеющие техническое происхождение. Для решения задачи защиты информации в офисном помещении разработан *способ генерации* в среде распространения сильного помехового сигнала, который невозможно доступными злоумышленнику техническими средствами отфильтровать от информационного сигнала. Для зашумления акустовибрационного канала утечки используют генераторы белого шума, связанные с излучателями, устанавливаемые на стенах, стеклах, трубах отопления и др. Комбинированное средство — система акустовибрационной защиты — может применяться для защиты от утечек по акустическому и акустовибрационному каналу помещений, в которых обрабатываются данные, содержащие служебную, государственную и др. тайну [9, 12]. Система формирует широкополосные акустические и вибрационные маскирующие шумовые помехи в воздушной среде, элементах ограждающих конструкций и в инженерно-технических коммуникациях защищаемых помещений. Система управляется при помощи дистанционного пульта.

Генерация шума имеет следующие особенности:

- вместе с белым шумом создается речеподобный шум, что улучшает маскирующие характеристики, отделение помехи от речевого сигнала становится маловероятным;
- мощность шума автоматически повышается при усилении речи, что улучшает степень защиты;
- маскирующие шумы не мешают рабочему процессу.

В этой связи было проведено исследование основных видов помех.

Помехи, формируемые из скрываемого сигнала, бывают двух типов [4]: речеподобная реверберационная и речеподобная инверсионная.

Речеподобная реверберационная помеха формируется из фрагментов скрываемого речевого сигнала путем многократного их наложения с различными уровнями.

Комбинированные помехи формируются путем смешения различного вида помех, например, помех типа «речевой хор» и «белый шум», речеподобных реверберационной и инверсионной помех.

Как показали результаты экспериментов, помеха типа «белый шум» по сравнению с помехами типа «розовый шум» и шумовая речеподобная обладает худшими маскирующими свойствами, проигрывая по энергетике 0,8—1,2 дБ [16].

Значительно более низкими маскирующими свойствами обладает «коричневый шум» — шумовая помеха со спадом спектральной плотности 6 дБ на октаву в сторону высоких частот. По сравнению с помехами типа «розовый шум» и шумовая речеподобная она проигрывает по энергетике 4,1—4,2 дБ, а при равной мощности приводит к повышению разборчивости более чем в полтора раза (*табл.*1).

Следовательно, для обеспечения защиты информации в офисном помещении целесообразно использование речеподобной реверберационной помехи.

Способ защиты речевой информации от утечки по акустовибрационному каналу

Защита речевой информации от утечки по акустовибрационному каналу в офисном помещении строится по *принципу*: уменьшение отношения q_i *сигнал/помеха* в зоне приема сигнала злоумышленником.

Разработан способ (по аналогии с [6]) реализации модели формирования речеподобной реверберационной помехи, формируемой из случайной смеси звуков русской речи, который можно реализовать на ПЭВМ. Суть предлагаемого способа формирования помехи заключается в следующем:

- на микрофон подаются речевые сигналы субъектов переговоров;
- речеподобная помеха формируется путем многократного наложения фрагментов скрываемого речевого сигнала с различными амплитудами, поступающими с шести однотипных каналов (оп-

Таблица 1

Значения отношения сигнал/шум, при которых обеспечивается требуемая эффективность защиты акустической (речевой) информации

Вид помехи	Словесная разборчивость W, %	Отношение q_i сигнал/шум в октавных полосах					Отношение с/ш в полосе частот 180—5600 Гц
		250	500	1000	2000	4000	
«Белый шум»	20	+ 0,8	- 2,2	- 10,7	- 18,2	- 24,7	- 10,0
	30	+ 3,1	+ 0,1	- 8,4	- 15,9	- 22,4	- 7,7
	40	+ 5,1	+ 2,1	- 6,4	- 13,9	- 20,4	- 5,7
«Розовый шум» (шум со спадом спектральной плотности 3 дБ на октаву)	20	- 5,9	- 5,9	- 11,4	- 15,9	- 19,4	- 8,8
	30	- 3,7	- 3,7	- 9,2	- 13,7	- 17,2	- 6,7
	40	- 1,9	- 1,9	- 7,4	- 11,9	- 15,4	- 4,9
«Коричневый шум» (шум со спадом спектральной плотности 6 дБ на октаву)	20	- 14,1	- 11,1	- 3,6	- 15,1	- 15,6	- 13,0
	30	- 12,0	- 9,0	- 11,5	- 13,0	- 13,5	- 10,8
	40	- 10,0	- 7,2	- 9,7	- 11,2	- 11,7	- 9,0
Шумовая речеподобная помеха	20	- 3,9	- 7,9	- 12,9	- 15,9	- 16,9	- 9,0
	30	- 1,7	- 5,7	- 10,7	- 13,7	- 14,7	- 6,8
	40	+ 0,1	- 3,9	- 8,9	- 11,9	- 12,9	- 5,0

тимальное количество каналов определено экспериментально);
- в каждом канале помеховый сигнал представляет собой звуки русской речи, которые поступают на микрофон;
- помеховый сигнал подается на звуковую карту компьютера, с линейного выхода которой он может быть подан на звуковую колонку или на внешний вход генератора шума системы акустовибрационной защиты.

Программно-аппаратный комплекс защиты речевой информации

Для реализации данного способа защиты речевой информации в офисном помещении разработан программно-аппаратный комплекс (ПАК) «Система активной акустической и вибрационной защиты речевой информации» с учетом требований национальных и межгосударственных стандартов[9].

Основными *задачами* ПАК являются: генерация речеподобной помехи для обеспечения защиты информации по акустовибрационному каналу утечки информации, вычисление коэффициента *W* словесной разборчивости для оценки уровня *защищенности* помещения, непрерывный анализ звуков в помещении, построение спектра сигнала (*рис. 3*).

Кроме того, ПАК позволяет:
- обучить методам активной защиты информации от утечки по акустическому и акустовибрационному каналу с наглядной демонстрацией;
- оценить эффективность защиты акустической информации и настройки с помощью разработанного программного обеспечения уровня акустического шума и интенсивности вибродатчиков;
- исследовать звукоизолирующие свойства материалов ограждающих конструкций и коммунальных систем;
- тестировать новые виды помех для защиты информации от утечки по акустическому и акустовибрационному каналу.

Состав ПАК (*рис. 4*):
1. Генератор акустического шума «Соната СА-65М»: полоса воспроизводимых частот 175—7500 *Гц* (5 октав), ток потребляемый 45 *мА*, максимальное число индивидуальных адресов 255. Продолжительность непрерывной работы не ограничена.
2. Генератор акустовибрационного шума «Соната СП-45М»: полоса воспроизводимых частот 175—7500 *Гц* (5 октав), ток потребляемый 20 *мА*, максимальное число индивидуальных адресов 255. Продолжительность непрерывной работы не ограничена.
3. Универсальный блок питания системы акустовибрационной защиты информации «Соната ИП-3»: система команд управления технических средств защиты информации, подключенными к выходу элек-

[9] ГОСТ Р 50840-95. Государственный стандарт Российской Федерации. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости. М. : Госстандарт России, 1997. 230 с.; ГОСТ 16600-72. Межгосударственный стандарт. Передача речи по трактам радиотелефонной связи. Требования к разборчивости речи и методы артикуляционных измерений. М. : СтандартИнформ, 2007. 74 с.; ГОСТ Р ИСО/МЭК15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель, 2012; СП 51.13330.2011. Защита от шума. Актуализированная редакция СНиП. М. : Минрегион России, 2011. 46 с.

Рис. 3. Схема основных процессов программы

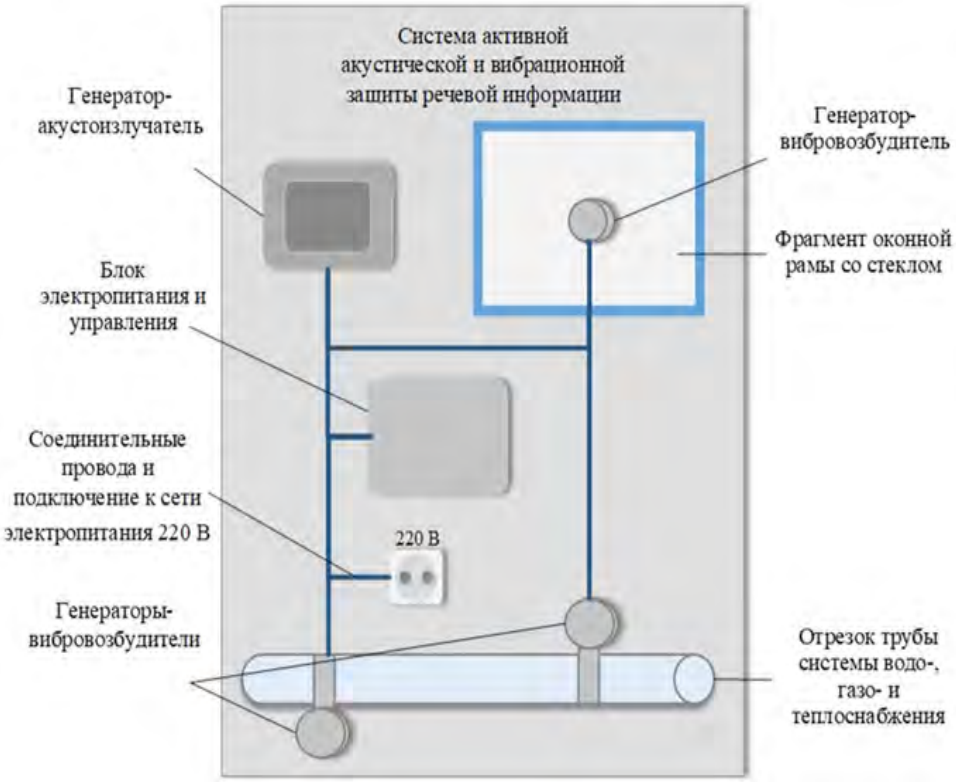


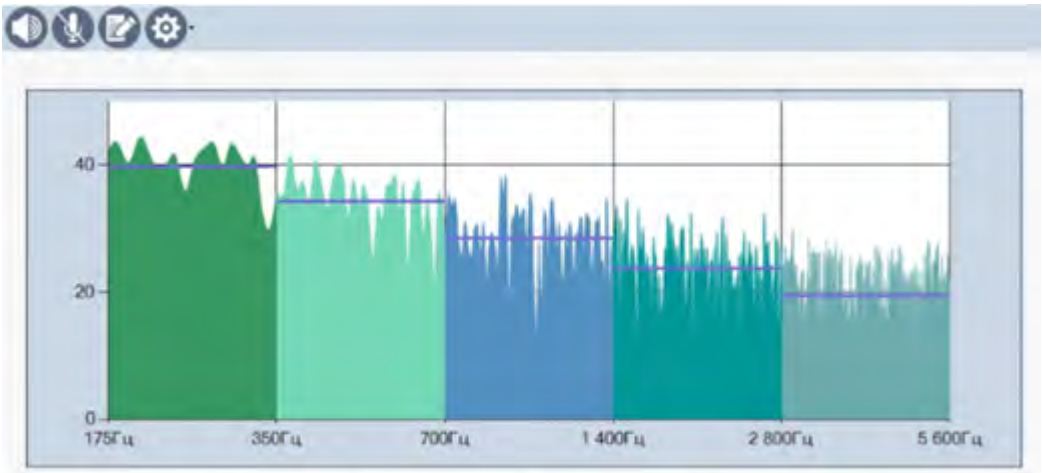
Рис. 4. Функциональная схема ПАК «Система активной акустической и вибрационной защиты речевой информации»

тропитания: *ReBus*3, интерфейс для подключения к ПЭВМ: *USB* 2.0, продолжительность непрерывной работы не более 8 *час*, количество логически адресуемых устройств 255.

4. Генератор акустовибрационного шума «Соната СВ-45М»: полоса воспроизводимых частот 175—7500 *Гц* (5 октав), ток потребляемый 20 *мА*, максимальное число индивидуальных адресов 255. Продолжительность непрерывной работы не ограничена.
5. Программное обеспечение «ИСИДОРА» («Измерительная система дополненной реальности — Акустика»), разработанное с помощью языка программирования C# [14].
6. Микрофон.
7. Динамики.

Разработанное для настройки средств защиты информации (СЗИ) программное обеспечение «ИСИДОРА» позволяет регулировать уровень создаваемой акустической помехи для соответствия требованиям защищенности помещения и одновременно комфортного ведения разговора в данном помещении (*рис. 5*).

Анализ звука выполняется путем использования подключенного микрофона. После включения функции устройство начинает записывать звук. По истечении определенного времени в память записываются данные об изменениях звука за этот временной отрезок.



№ октавы	Диапазон частот	Средняя частота	Уровень сигнала, дБ	Уровень шума, дБ	W
1	175-350	250	72,0203210441...	42,998011294931	0,99622359111...
2	350-700	500	83,2573470191...	41,1686627267...	0,99622359111...
3	700-1400	1000	92,7085700058...	28,4820979658...	0,99622359111...
4	1400-2800	2000	84,2516611439...	26,9002811186...	0,99622359111...
5	2800-5600	4000	83,8139085167...	22,762621022739	0,99622359111...

Рис. 5. Скриншот работы программного обеспечения «ИСИДОРА»

Рис. 6. Преимущества программно-аппаратного комплекса

Над массивом данных выполняется быстрое преобразование Фурье, основанное на разложении исходной непрерывной функции от времени на совокупность базисных гармонических функций различной частоты, амплитуды и фазы. Вычисление значений амплитуды позволяют построить *спектр* сигнала. Массив данных очищается, освобождая место для следующей порции данных. Процесс цикличен, условием работы является включенная функция записи.

По сравнению с аналогичными средствами защиты информации разработанный программно-аппаратный комплекс обладает преимуществами, приведёнными на рис. 6.

Уникальность программно-аппаратного комплекса состоит в следующем:

– широкий спектр представленных средств активной защиты информации;
– относительно невысокая стоимость;
– простота освоения работы с комплексом;
– имеется специальное программное обеспечение с целью настройки уровней маскирующих сигналов.

Кроме того, разработанный ПАК обеспечивает совместную работу с ПЭВМ, микрофонами, источниками звука; настройку уровней маскирующих сигналов, обеспечивающих допустимый уровень словесной разборчивости на границе контролируемой зоны, что является дополнительным преимуществом его перед аналогами.

Заключение

Своевременное обеспечение защиты речевой информации в офисном помещении позволяет своевременно реагировать на возникающие угрозы, исключить возможность срывов выполнения задач. Разработанный способ защиты речевой информации позволяет изучать процесс утечки информации по техническим

каналам и методы ее защиты, а также применять разнообразные модули и дополнительное программное обеспечение для оценки эффективности применения различных способов защиты информации, что наглядно демонстрирует возможности различных методов обеспечения информационной безопасности.

Таким образом, по результатам исследований разработан программно-аппаратный комплекс, включающий минимальный набор устройств, обеспечивающих безопасность конфиденциальной речевой информации в помещении офисного типа, а также разработано программное обеспечение, позволяющее регулировать уровень создаваемой реверберационной речеподобной помехи для соответствия требованиям защищенности помещения и одновременно комфортного разговора в данном помещении.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, старший научный сотрудник, президент НПО «Эшелон», профессор кафедры информационной безопасности МГТУ им. Э. Н. Баумана, г. Москва, Российская Федерация.*
E-mail: a.markov@bmstu.ru

Литература

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. М. : Горячая линия-Телеком, 2005. 415 с.
2. Волчихина М.В. Метод адаптации параметров средств защиты информации на основе дискретного изменения амплитуды и тембра субъектов переговоров // Вестник ТГТУ. 2022. Т. 28. № 2. С. 226—234.
3. Ворона В.А., Костенко В.О. Способы и средства защиты информации от утечки по техническим каналам // Computational nanotechnology. 2016. № 3. С. 208—223.
4. Дворянкин С.В., Макаров Ю.К., Хорев А.А. Обоснование критериев эффективности защиты речевой информации от утечки по техническим каналам // Защита информации. Инсайд. 2007. № 2 (14). С. 18—25.
5. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. 2000. № 4. С. 39—45.
6. Зайцев А.П., Шелупанов А.А. Технические средства и методы защиты информации. М. : Машиностроение, 2009. 507 с.
7. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2021. 276 с. ISBN 978-5-93916-896-0.
8. Ловцов Д.А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74 .
9. Ловцов Д.А. Концептуально-логическое моделирование юридического понятия «тайна» // Информационное право. 2009. № 2. С. 12—14.
10. Ловцов Д.А., Верхоглядов А.А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. 2008. № 8. С. 55—64.
11. Ловцов Д.А., Ермаков И.В. Защита информации от доступа по нетрадиционным информационным каналам // НТИ. Сер. 2. Информ. процессы и системы. 2006. № 9. С. 1—9.
12. Ловцов Д.А., Федичев А.В. Архитектура национального классификатора правовых режимов информации ограниченного доступа // Правовая информатика. 2017. № 2. С. 35—54. DOI: 10.21681/1994-1404-2017-2-35-54 .
13. Макаров Ю.К., Хорев А.А. Методы защиты речевой информации и оценки их эффективности // Защита информации. Конфидент. 2001. № 4. С. 22—33.
14. Свидетельство № 2019667587 RU. Измерительная система дополненной реальности — Акустика («ИСИДОРА»): Программа для ЭВМ / Машкова О.С., Савилова У.А., Шибков Д.А., Яковлев А.В., Яковлева Д.А. (RU). № 2019666736; заявл. 17.12.19; зарегистр. 25.12.19 // Бюл. 2019. № 6.
15. Торокин А.А. Инженерно-техническая защита информации. М. : Гелиос АРВ, 2005. 958 с. ISBN 5-85438-140-0.
16. Хорев А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: системы виброакустической защиты // Специальная техника. 2013. № 4. С. 31—63.
17. Хорев А.А. Техническая защита информации. М. : НПЦ «Аналитика», 2008. 436 с.

A METHOD FOR PROTECTING SPEECH INFORMATION IN OFFICE PREMISES

Vladimir Alekseev, *Dr.Sc. (Technology), Professor, corresponding member of the Russian Academy of Natural Sciences, Honoured Radio Operator of the Russian Federation, Head of the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: vvalex1961@yandex.ru

Dmitrii Klinkov, *operator of the research unit of the Interbranch Centre for Training and Combat Use of Electronic Warfare Troops of the Russian Federation, Tambov, Russian Federation.*
E-mail: dmitkast1996@mail.ru

Aleksei Iakovlev, *Ph.D. (Technology), Associate Professor at the Department of Information Systems and Information Protection of the Tambov State Technical University, Tambov, Russian Federation.*
E-mail: yava73@bk.ru

Keywords: *acoustic vibration channel, speech signal, information leakage, software and hardware system, speech-like reverberation interference, noise generator, speech intelligibility coefficient, premises' protection level, software.*

Abstract

Purpose of the work: developing a method for ensuring information security of office premises against information leakage via acoustic vibration channels which is based on using speech-like interference as well as finding whether the procedure for using this method of protection complies with current legal regulations.

Methods used: information technology law analysis, spectral and system analysis, theory of similarity and modelling.

Study findings: a justification is given for the efficiency of using speech-like interference for protecting office premises against information leakage via acoustic vibration channels. A method for protecting office premises against information leakage via acoustic vibration channels is developed, and a systematic overview of its advantages compared with similar information protection means is given. A soft- and hardware system implementing the method is presented, and a description is given for the developed software needed for generating speech-like reverberation interference and ensuring an interrupt mode when the speech signal source is absent. A computational experiment for comparative assessment of the efficiency of using special types of interferences for protecting office premises information. Legal questions of ensuring information security are studied, and it is found that the procedure for using the method complies with the provisions of current legal regulations on technical means of information protection.

References

1. Buzov G.A., Kalinin S.V., Kondrat'ev A.V. Zashchita ot utechki informatsii po tekhnicheskim kanalam. M. : Goriachaia liniia-Telekom, 2005. 415 pp.
2. Volchikhina M.V. Metod adaptatsii parametrov sredstv zashchity informatsii na osnove diskretnogo izmeneniia amplitudy i tembra sub"ektov peregovorov. Vestnik TGTU, 2022, t. 28, No. 2, pp. 226–234.
3. Vorona V.A., Kostenko V.O. Sposoby i sredstva zashchity informatsii ot utechki po tekhnicheskim kanalam. Computational nanotechnology, 2016, No. 3, pp. 208–223.
4. Dvoriankin S.V., Makarov Iu.K., Khorev A.A. Obosnovanie kriteriev effektivnosti zashchity rechevoi informatsii ot utechki po tekhnicheskim kanalam. Zashchita informatsii. Insaid, 2007, No. 2 (14), pp. 18–25.
5. Zhelezniak V.K., Makarov Iu.K., Khorev A.A. Nekotorye metodicheskie podkhody k otsenke effektivnosti zashchity rechevoi informatsii. Spetsial'naia tekhnika, 2000, No. 4, pp. 39–45.
6. Zaitsev A.P., Shelupanov A.A. Tekhnicheskie sredstva i metody zashchity informatsii. M. : Mashinostroenie, 2009. 507 pp.
7. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2021. 276 pp. ISBN 978-5-93916-896-0.
8. Lovtsov D.A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66–74. DOI: 10.21681/1994-1404-2017-3-66-74 .
9. Lovtsov D.A. Kontseptual'no-logicheskoe modelirovanie iuridicheskogo poniatiia "taina". Informatsionnoe pravo, 2009, No. 2, pp. 12–14.

10. Lovtsov D.A., Verkhogliadov A.A. Informatsionnaia bezopasnost' sudebnykh avtomatizirovannykh informatsionnykh sistem: pravovoe regulirovanie i iurisdiktsiia. Rossiiskoe pravosudie, 2008, No. 8, pp. 55–64.
11. Lovtsov D.A., Ermakov I.V. Zashchita informatsii ot dostupa po netraditsionnym informatsionnym kanalam. NTI. Ser. 2. Inform. protsessy i sistemy, 2006, No. 9, pp. 1–9.
12. Lovtsov D.A., Fedichev A.V. Arkhitektura natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Pravovaia informatika, 2017, No. 2, pp. 35–54. DOI: 10.21681/1994-1404-2017-2-35-54 .
13. Makarov Iu.K., Khorev A.A. Metody zashchity rechevoi informatsii i otsenki ikh effektivnosti. Zashchita informatsii. Konfident, 2001, No. 4, pp. 22–33.
14. Svidetel'stvo No. 2019667587 RU. Izmeritel'naia sistema dopolnennoi real'nosti – Akustika ("ISIDORA"): Programma dlia EVM / Mashkova O.S., Savilova U.A., Shibkov D.A., Iakovlev A.V., Iakovleva D.A. (RU). No. 2019666736; zaiavl. 17.12.19; zaregistr. 25.12.19. Biul. 2019, No. 6.
15. Torokin A.A. Inzhenerno-tekhnicheskaia zashchita informatsii. M. : Gelios ARV, 2005. 958 pp. ISBN 5-85438-140-0.
16. Khorev A.A. Sposoby zashchity vydelennykh pomeshchenii ot utechki rechevoi (akusticheskoi) informatsii po tekhnicheskim kanalam: sistemy vibroakusticheskoi zashchity. Spetsial'naia tekhnika, 2013, No. 4, pp. 31–63.
17. Khorev A.A. Tekhnicheskaia zashchita informatsii. M. : NPTs "Analitika", 2008. 436 pp.