ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 ISSN 1995-5499
DOI: https://doi.org/10.17308/sait.2020.2/2915
Поступила в редакцию 29.04.2020
Подписана в печать 15.06.2020

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ИДЕНТИФИКАЦИИ УГРОЗ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВОЗНИКАЮЩИХ ЗА СЧЕТ НИЗКОЧАСТОТНЫХ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

© 2020 Д. А. Короченцев✉ , Л. В. Черкесова

Донской государственный технический университет
пл. Гагарина, 1, 344000 Ростов-на-Дону, Российская Федерация

Аннотация. В статье рассмотрены физические основы формирования технического канала утечки информации, возникающего за счет низкочастотных акустоэлектрических преобразований. Приведена, с представлением в виде имитационной модели, используемая в настоящее время при проведении специальных исследований методика инструментально-расчетного контроля защищенности речевой информации в рассматриваемом канале утечки информации. На основе разработанной имитационной модели, используя паттерн проектирования MVP, разработано программное средство. Представлены основные классы программного средства, реализующего модель. Продемонстрирован функционал разработанного программного средства и даны рекомендации по возможному применению разработанного программного средства идентификации угроз нарушения информационной безопасности, возникающих за счёт низкочастотных акустоэлектрических преобразований.

Ключевые слова: объект информатизации, акустоэлектрические каналы утечки информации, защита информации, угроза информационной безопасности, имитационная модель, информационная безопасность.

ВВЕДЕНИЕ

В настоящее время техническая защита информации приобретает все большее значение. Это обусловлено, прежде всего, активным развитием методов и средств добывания информации, позволяющих несанкционированно получать все больший объём информации на безопасном расстоянии, оснащением служебных и жилых помещений, а в последнее время автомобилей и других транспортных средств, разнообразной электро- и радиоэлектронной аппаратурой, являющейся источником случайных опасных сигналов.

Построение эффективной системы защиты информации возможно лишь при условии полного и всестороннего обследования объекта информатизации (ОИ) на наличие возможных технических каналов утечки информации (ТКУИ) [4, 8, 12].

Практически на любом ОИ находятся те или иные технические средства (ТС), относящиеся к вспомогательным техническим средствам и системам (ВТСС): телефоны, датчики пожарной и охранной сигнализации, системы диспетчерской (громкоговорящей) связи, оргтехника, системы связи и т. д. [1, 5, 6, 17–19]. Эти ТС в нормальном режиме работы могут образовывать технические каналы утечки информации.

✉ Короченцев Денис Александрович
e-mail: center-bit@yandex.ru

Достаточно хорошо известны способы несанкционированного получения защищаемой информации за счёт подключения технических средств разведки (ТСР) к функциональным линиям указанных ВТСС. В качестве ТСР, например, могут выступать малошумящие усилители низкой частоты с высоким коэффициентом усиления и специальными наборами элементов подключения [5, 11, 13, 14, 16, 17]. Подобные каналы утечки создаются за счёт явления акустоэлектрических преобразований (АЭП) в элементах технических средств.

Проявление АЭП рассматриваемых ТКУИ в большинстве случаев не связано с качеством исполнения того или иного ТС, а является сопутствующим его деятельности.

В общем случае, канал утечки информации, образованный за счёт АЭП, можно разделить на низкочастотный (НЧ) и высокочастотный (ВЧ) каналы утечки информации [1, 5, 14].

Целью исследований является разработка, в виде имитационной модели, программного средства идентификации угроз нарушения информационной безопасности, возникающих за счет низкочастотных акустоэлектрических преобразований.

МАТЕРИАЛЫ И МЕТОДЫ

Для идентификации технических каналов утечки информации, образованных за счёт НЧ акустоэлектрических преобразований, на объекте информатизации проводятся специальные исследования, позволяющие оценить значения величины отношения «информативный сигнал/шум» Δ_i и словесной разборчивости речи W на выходных контактах ТС. Специальные исследования проводятся в соответствии с методикой инструментально–расчётного контроля защищенности речевой информации в канале НЧ АЭП (далее — Методика) [1, 14].

Методика предназначена для оценки защищенности акустической речевой информации от утечки, возникающей в результате низкочастотных акустоэлектрических преобразований, когда информативные сигналы, содержащие акустическую речевую информацию, могут быть зарегистрированы в виде электрических сигналов в линиях связи технических средств, в шине заземления, в проводах сети электропитания, а также при воздействии на ТС звуковых колебаний, возникающих при произношении или воспроизведении речи.

Сущность рассматриваемой Методики [2, 3, 5, 7, 16] заключается в том, что ТС подвергается акустическому воздействию тональным сигналом на среднегеометрической частоте октавы F_i, где i — номер октавы. На выходных контактах ТС измеряется уровень сигнала и шума $U_{сш i}$.

Одновременно измеряется звуковое давление тонального сигнала в месте расположения ТС L_i. Затем источник акустического сигнала выключается и измеряется уровень шума $U_{ш i}$.

По результатам обработки результатов измерений выполняется оценка отношения «сигнал/шум» в i-й октаве Δ_i на выходе вспомогательного технического средства и/или системы, и сравнение с нормативным значением $\Delta_н$.

При выполнении неравенства

$$\Delta_i \le \Delta_н \qquad (1)$$

считается, что проверяемое ВТСС не подвержено явлению низкочастотных акустоэлектрических преобразований. В противном случае производится расчёт значения словесной разборчивости речи W_c. Рассчитанное значение W_c сравнивается с нормированным значением $W_н$ [5, 16].

При выполнении неравенства

$$W_c \le W_н \qquad (2)$$

устанавливается, что проверяемое ВТСС не подвержено НЧ АЭП.

В противном случае необходимо провести оценку возможностей перехвата речевой информации из защищаемого помещения по каналу низкочастотного акустоэлектрического преобразования, для чего необходимо определить коэффициент затухания $K_{л,i}$ опасных сигналов исследуемой линии на среднегеометрических частотах октавных полос [16]. С учётом $K_{л,i}$ исследуемой линии на средне-

геометрических частотах октавных полос рассчитывается отношение «сигнал/шум» на границе контролируемой зоны (КЗ) в *i*-й октаве Δ_i^*.

При выполнении неравенства

$$\Delta_i^* \le \Delta_н \qquad (3)$$

считается, что проверяемое ВТСС подвержено НЧ АЭП, однако характеристики исследуемой линии не позволяют случайному опасному сигналу выйти за границы КЗ. Если неравенство (3) не выполняется, то производится расчёт значения словесной разборчивости речи W_c^*, которое в дальнейшем сравнивается с нормированным значением.

При выполнении неравенства

$$W_c^* \le W_н \qquad (4)$$

устанавливается, что проверяемое ВТСС считается защищённым от утечки информации за счёт явления низкочастотных акустоэлектрических преобразований, в противном случае принимается решение о необходимости использования активных или пассивных методов защиты информации.

Концептуально рассматриваемую Методику можно представить в виде имитационной модели, графически изображенной на рис. 1.

Для определения подверженности вспомогательных технических средств и систем явлению низкочастотных акустоэлектрических преобразований собирают специальный измерительный стенд, общая структура описана в [2, 3, 5, 7, 16].

После сборки измерительного стенда, генератор низкой частоты настраивают на среднегеометрическую частоту 1-й октавы и измеряют уровни звукового давления L_1 и электрического сигнала и шума $U_{\tilde{n}ш1}$ на выходных контактах ТС на частоте 1-й октавы.

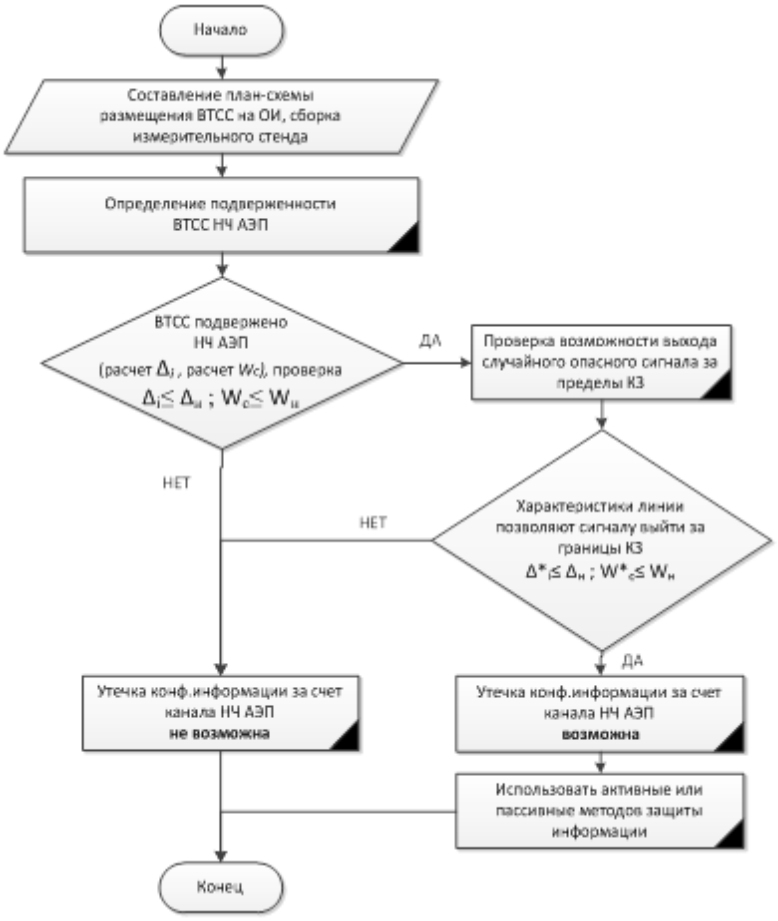

Рис. 1. Имитационная модель определения ТКУИ за счёт НЧ АЭП
[Fig. 1. Simulation model for determining technical channels of information leakage due to low-frequency acoustoelectric transformations]

Далее, генератор низкой частоты выключается, и измеряется уровень электрического шума на выходных контактах ТС $U_{ш1}$ в полосе пропускания фильтра анализатора (за уровень шумов принимается минимальное значение $U_{ш}$, зафиксированное в течение 30 с непрерывного измерения). Для среднегеометрических частот 2–5 октав измерения проводятся аналогично. В том случае, если применяются средства пассивной или активной защиты, то измерения проводятся аналогично, с той разницей, что дополнительно измеряется уровень шумов с отключенным средством защиты.

При невыполнении неравенства (3) и необходимости определения $K_{л,i}$, собирают схему, рассмотренную в [16, 17], и в точке отключения ВТСС на i-й частоте в исследуемую линию подают сигнал от генератора сигналов и измеряют пробником напряжение этого сигнала в двух точках: вблизи подачи сигнала в линию в точке Т1($U_{1,i}$) и на границе КЗ в точке Т2($U_{2,i}$). Результаты измерений фиксируются в протоколе специальных исследований.

Специальные исследования на подверженность явлению низкочастотных акусто-электрических преобразований проводятся для всех возможных режимов работы ВТСС и для всех возможных вариантов подключения технического средства разведки к ВТСС. Порядок обработки результатов измерений и расчета $\Delta_i(\Delta_i^*), W_c(W_c^*)$ приведен в [2, 3, 5, 16].

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Имитационная модель идентификации угроз нарушения информационной безопасности, возникающих за счет НЧ АЭП, реализована посредством программного средства, компоненты которого разрабатывались на языке C#, с использованием платформы .NET Framework 2.0 – 4.5.2. в среде разработки Unity3D 2018.4 и JetBrains Rider.

В качестве паттерна проектирования рассматриваемого программного средства использовался паттерн «Модель–Вид–Представитель» (Model–View–Presenter (MVP)) [9, 10, 20].

Основными классами программного средства, реализующими используемый паттерн проектирования «Модель–Вид–Представитель», являются следующие:

• **Task** — класс задачи, содержащий в себе интерфейс условия ITaskCompleteChecker и возвращающий в систему состояние условия (выполнен / не выполнен). На основе этого класса строится система этапов, которая проверяет выполнение всех задач, принадлежащих данному этапу (например, условия вида «установка генератора низкой частоты», «расстояние между экранированной акустической колонкой и ВТСС», «расстояние между вспомогательным техническим средством и/или системой и анализатором спектра» и др.);

• **IDataProvider** — интерфейс, определяющий тип данных, необходимых классу, который запрашивается (например: класс *CalculationTableLabLFAT* — это таблица в протоколе с результатами специальных исследований, а *CalculationTableLabLFATProvider* — класс, реализующий интерфейс *IDataProvider* с параметром *CalculationTableLabLFAT* и предоставляющий рассматриваемую таблицу протокола специальных исследований);

• **TestBenchForLFAT** — класс, который реализует логику работы измерительного стенда. Этот класс проверяет условия сборки измерительного стенда и моделирует значения параметров используемых технических средств в соответствии в выбранным вариантом (например: уровень звукового давления акустического сигнала на среднегеометрической частоты 1-й октавы; уровень электрического сигнала и шума на выходных контактах ВТТС на частоте 1-й октавы и т. д.);

• **TableView** — класс, реализующий обработку результатов измерений. Рассматриваемый класс принимает модель данных, в соответствии с которой строит отображение. Модель данных не только содержит в себе информацию о том, какую структуру имеют данные, но и какие логические связи есть с другими моделями данных, а также как они рассчитываются.

При запуске программного средства появляется пользовательский интерфейс, который состоит из четырёх основных компонентов: панель «Меню» (1), панель устройств (2), рабочая область (3), список задач (4) (см. рис. 2).

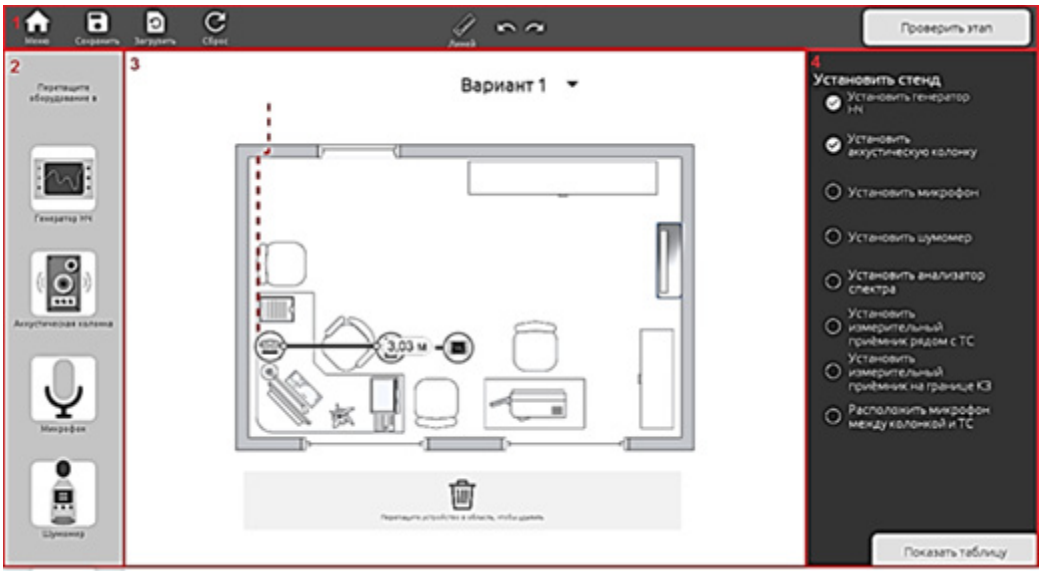

Рис. 2. Пользовательский интерфейс программного средства
[Fig. 2. User interface of the software tool]

Панель «Меню» содержит в себе основные элементы управления. Среди них находится кнопка возврата в описательную часть имитационной модели (кнопка «Меню»), кнопка сброса хода этапа специальных исследований ОИ, кнопка вызова инструмента «Линейка» и кнопка проверки правильности выполнения этапов специальных исследований ОИ в соответствии с Методикой. Кнопка линейки является переключателем.

Сам инструмент «линейка» работает только в пределах рабочей области и позволяет измерять расстояние между двумя точками (например, между ВТСС и экранированной акустической колонкой (см. рис. 2)). Кнопка выполнения этапа является контекстной, и в зависимости от состояния либо выполняет проверку этапа специальных исследований объекта информатизации, либо вызывает таблицу из протокола.

Панель инструментов содержит в себе необходимое контрольно-измерительное оборудование (КИО), используемое при проведении специальных исследований ОИ, и представляет собой пиктограмму и подпись с названием.

Рабочая область содержит в себе план-схему объекта информатизации, область для удаления КИО и меню выбора вариантов, в виде выпадающего списка, (в качестве вариантов используются различные ОТСС, часто размещаемые на объекте ОИ, например, на рис. 2 представлен вариант 1, ВТСС — телефонный аппарат). При смене варианта происходит сброс всего проделанного процесса. Рабочая область, в пределах которой производится сборка измерительного стенда, представляет собой объект информатизации со схематично изображенными ограждающими конструкциями, техническими средствами, предметами интерьера, мебелью. В нижней части рабочей области имеется область для удаления, при перетягивании в которую контрольно-измерительное оборудование удаляется из рабочей области и появляются на панели устройств.

Список задач содержит в себе этапы Методики, разбитые на подзадачи, которые необходимо выполнить для завершения этапа. Каждая подзадача имеет соответствующий маркер, который отображает её состояние ((выполнено или не выполнено), см. рис. 2).

Первым этапом Методики является сборка специального измерительного стенда, для этого необходимо выбрать КИО на панели устройств и перетащить его в рабочую область. После нажатия на кнопку проверки выполнения этапа, программа произведёт проверку условий и отметит те, которые были успешно выполнены.

После того, как специальный измерительный стенд был собран в соответствии с правилами проведения инструментального кон-

троля, необходимо произвести измерения и получить исходные данные для расчета $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$.

Для этого необходимо нажать по пиктограмме соответствующего КИО (например, анализатору спектра или шумомеру) в рабочей зоне, вызвав тем самым диалоговое окно, в котором будут отображаться результаты измерений. В диалоговых окнах некоторого КИО есть элементы управления (например, в диалоговом окне акустической колонки есть переключатель её состояния (вкл./выкл.), а в окне генератора НЧ можно перестраивать среднегеометрическую частоту генерируемого сигнала с 1-й по 5-ю октавы). На рис. 3 графически изображено проведение измерений уровней звукового давления L_1 и электрического сигнала и шума $U_{сш1}$ на выходных контактах ТС на частоте 1-й октавы (275 Гц).

После того, как проведены измерения значений уровней звукового давления L_i, электрического сигнала и шума $U_{сшi}$ на выходных контактах ТС, электрического шума на выходных контактах ТС $U_{шi}$, а в случае невыпол-

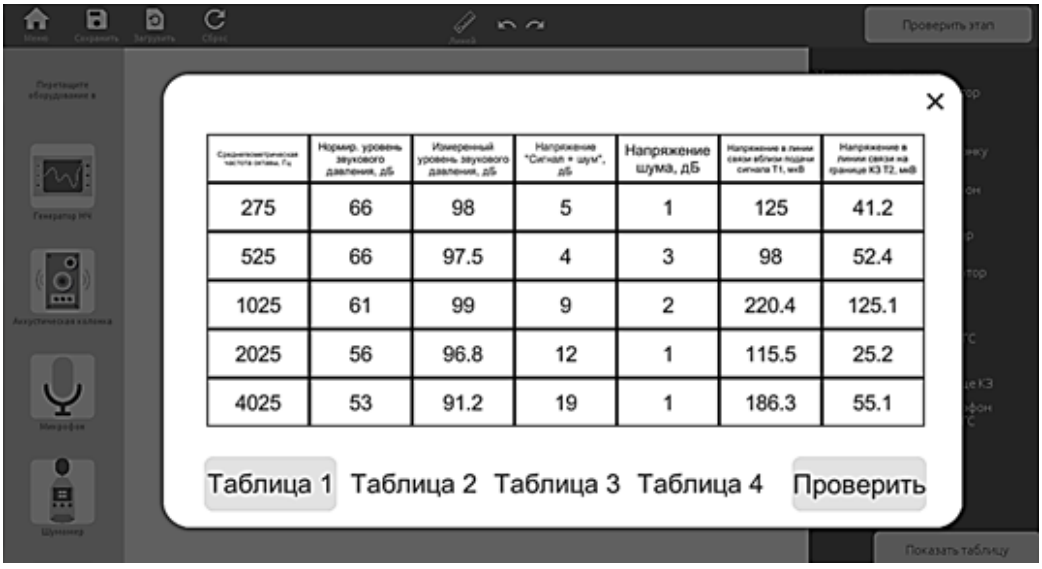

Рис. 3. Проведение измерений уровней звукового давления и электрического сигнала и шума на выходных контактах ВТТС на частоте 275 Гц

[Fig. 3. Measurement of sound pressure levels and electrical signal and noise at the output contacts of auxiliary equipment and systems at a frequency of 275 Hz]

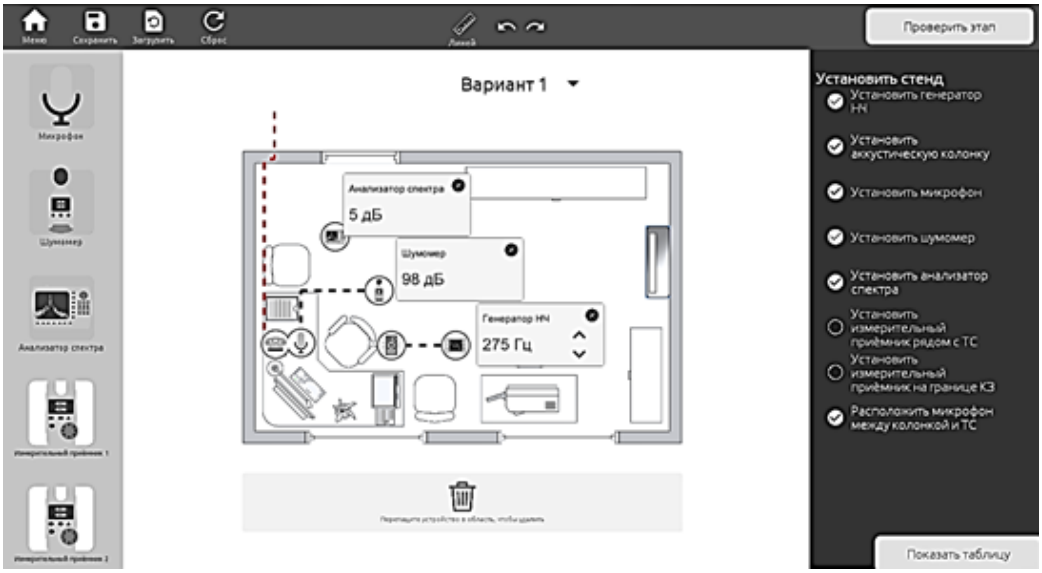

Рис. 4. Таблица значений, измеренных с помощью КИО

[Fig. 4. Table of values measured using control and measuring equipment]

нения неравенств 1 и 2, напряжения сигнала в точках Т1($U_{1,i}$) и Т2($U_{2,i}$), на среднегеометрических частотах всех октав, они заносятся в протокол специальных исследований ОИ (табл. 1, появляющаяся после нажатия контекстной кнопки в панели «Список задач», см. рис. 4).

Далее, производится обработка результатов измерений и расчет $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$ [2, 3, 5, 16]. Результаты расчетов вручную заносятся в таблицу протокола специальных исследований, которая визуально разделена на табл. 1–4.

Дополнительным функционалом табл. 2–4 является проверка результатов расчёта, полученных в соответствии с порядком обработки результатов измерений. Если в ячейку таблицы было внесено правильное значение, после нажатия кнопки «Проверить», цвет заливки ячейки измениться на зеленый, в противном случае ячейка окрасится красным.

ЗАКЛЮЧЕНИЕ

Выполненная в виде программного средства имитационная модель идентификации угроз нарушения информационной безопасности, возникающих за счёт явления низкочастотных акустоэлектрических преобразований, позволяет, варьируя набором исходных данных (выбор вариантов используемых вспомогательных технических средств и / или систем), моделировать ситуации, при которых рассматриваемый технический канал утечки информации может быть актуальным (расчёт $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$) и проверка выполнения неравенств 1–4).

Такая имитационная модель может использоваться специалистами по безопасности как крупных, так и малых предприятий, реализующих мероприятия по защите информации. Помимо этого, указанная модель создает условия для её активного внедрения в образовательный процесс подготовки специалистов в области информационной безопасности, с применением как традиционных (в виде контактной работы), так и дистанционных форм обучения.

Разработанная имитационная модель может использоваться при изучении таких дисциплин как: «Техническая защита информации», «Технические средства защиты информации», «Аттестация объектов информатизации» и др.

КОНФЛИКТ ИНТЕРЕСОВ

Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Бузов, Г. А.* Защита от утечки информации по техническим каналам: Учебное пособие / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев. – М. : Горячая линия - Телеком, 2005. 416 с.

2. *Волков, Д. С.* Методика оценки защищенности систем передачи данных от утечки речевой конфиденциальной информации по каналам электроакустических преобразований / Д. С. Волков, А. О. Козлов // Научный поиск. – 2014. – № 2.5. – С. 4–6.

3. Временная методика оценки защищенности основных технических средств и систем...: Нормативно-методический документ // Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. – М. : Гостехкомиссия России, 2002.

4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Введ. 01.02.2008 – М. : Стандартинформ, 2006. — 12 с.

5. *Дураковский, А. П.* Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: Учебное пособие / А. П. Дураковский, И. В. Куницын, Ю. Н. Лаврухин – М. : НИЯУ МИФИ, 2015. – 152 с.

6. *Емельянов, С. Л.* Техническая разведка и технические каналы утечки информации /

С. Л. Емельянов // Системы обработки информации. – 2010. – Вып. 3. – С. 20–23.

7. *Железняк, В. К.* Некоторые методические подходы к оценке эффективности защиты речевой информации / В. К. Железняк, Ю. К. Макаров, А. А. Хорев // Специальная техника. – М. : 2000. – № 4. – С. 39–45.

8. *Зайцев, А. П.* Технические средства и методы защиты информации / А. П. Зайцев, А. А. Шелупанов. – М. : Машиностроение, 2009. – 507 с.

9. *Павловский, Ю. Н.* Имитационные модели и системы / Ю. Н. Павловский. – М. : Фазис: ВЦ РАН, 2000. С. 134.

10. Паттерны разработки: MVC vs MVP vs MVVM vs MVI // URL: https://habr.com/ru/post/ 344184/

11. *Скрипник, Д. А.* Общие вопросы технической защиты информации. / Д.А. Скрипник. Режим доступа: http:// www. intuit. ru / goods_store/ebooks/8563

12. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К), Гостекомиссия России. – М. : 2001 г.

13. *Титов, А. А.* Инженерно-техническая защита информации: Учебное пособие для студентов специальностей «Организация и технология защиты информации», «Комплексная защита объектов информатизации» и «Информационная безопасность телекоммуникационных систем» / А. А. Титов. – Томск : Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 197 с.

14. *Торокин, А. А.* Инженерно–техническая защита информации / А. А. Торокин. – М. : Гелиос АРВ, 2005

15. *Халяпин, Д. Б.* Акустоэлектрические, акустопреобразовательные каналы утечки информации и возможные способы их подавления / Д. Б. Халяпин. – М. : «Мир безопасности», № 5. – С. 47–53.

16. *Хорев, А. А.* Контроль эффективности защиты вспомогательных технических средств / А. А. Хорев // Защита информации. Инсайд. – СПб. : Издательский дом «Афина», 2009. – № 1. – С. 42–52.

17. *Хорев, А. А.* Технические каналы утечки акустической (речевой) информации / А. А. Хорев // Специальная техника. – М. : 2009. – № 5. – С. 12–26.

18. *Хорев, А. А.* Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев. – М. : Гостехкомиссия РФ, 1998. – 320 с.

19. *Хорев, А. А.* Способы и средства защиты информации. Учебное пособие. / А. А. Хорев. – М. : МО РФ, 2000. – 316 с.

20. Mallawaarachchi Vijini. 10 Common Software Architectural Patterns in a nutshell / Mallawaarachchi Vijini // Towards Data Science. Режим доступа: https://towardsdatascience.com/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013

Короченцев Денис Александрович – канд. техн. наук, исполняющий обязанности заведующего кафедрой «Кибербезопасность информационных систем», Донской государственный технический университет.
E-mail:center-bit@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4491-3376

Черкесова Лариса Владимировна – д-р техн. наук, профессор кафедры «Кибербезопасность информационных систем», Донской государственный технический университет.
E-mail: chia2002@inbox.ru
ORCID iD: https://orcid.org/0000–0002–9392–3140

DOI: https://doi.org/10.17308/sait.2020.2/2915 ISSN 1995-5499
Received 29.04.2020
Accepted 15.06.2020

DEVELOPMENT OF A SOFTWARE TOOL FOR THE IDENTIFICATION OF THREATS TO INFORMATION SECURITY CAUSED BY LOW-FREQUENCY ACOUSTOELECTRIC TRANSFORMATIONS

© 2020 D. A. Korochentsev✉, L. V. Cherkesova

Don State Technical University
1, Gagarin square, 344000 Rostov-on-don, Russian Federation

Annotation. The article considers the physical basis for the formation of a technical channel of information leakage that occurs due to low-frequency acoustoelectric transformations. The method of instrumental and computational control of the security of speech information in the considered channel of information leakage, which is currently used in special research, is presented in the form of a simulation model. Using the developed simulation model and the MVP design pattern, we developed a software tool. The article presents the main classes of the software model. It demonstrates the functionality of the software tool, and provides recommendations for the possible use of the simulation model for identifying threats to information security that occur due to low-frequency acoustoelectric transformations.
Keywords: informatisation object, acoustoelectric channels of information leakage, information protection, information security threat, simulation model, information security.

CONFLICT OF INTEREST

The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.

REFERENCES

1. *Buzov G. A. , Kalinin S. V. , Kondratyev A. V.* Protection against information leakage through technical channels: the manual. Moscow : Hotline-Telecom, 2005. 416 p.

2. *Volkov D. S., KozlovA. O.* Method of assessing the security of data transmission systems from leakage of speech confidential information through channels of electroacoustic transformations // Scientific search. 2014. No. 2.5. P. 4–6.

3. A temporary method for assessing the security of basic hardware and systems...: Normative and methodological document // Collection of temporary methods for assessing the security of confidential information from leakage through technical channels. Moscow : State Technical Commission Of Russia, 2002.

4. GOST R 51275-2006. Information protection. Object of Informatization. Factors that affect information. Generalities. Yes. 01.02.2008. Moscow: STANDARTINFORM, 2006. 12 p.

5. *Durakovsky A. P., KunitsynI. V., Lavrukhin Yu. N.* Control of speech information security in premises. Certification tests of auxiliary technical means and systems for information security requirements: Tutorial. Moscow : National Research Nuclear University MEPhI, 2015. 152 p.

6. *Emelyanov S. L.* Technical intelligence and technical channels of information leakage // Information processing Systems. 2010. V. 3. P. 20–23.

7. *Zheleznyak V. K., MakarovYu. K., Horev A. A.* Some methodological approaches to evaluating the effectiveness of speech information protection. Special technique. Moscow : 2000. No. 4. P. 39–45.

8. Zaitsev A. P., Shelupanov A. A. Technical means and methods of information protection. Moscow : Mashinostroenie, 2009. 507 p.

9. Pavlovsky Yu. N. Simulation models and systems. M. : fazis: VC RAS, 2000. P. 134.

✉ Korochentsev Denis A.
e-mail: center-bit@yandex.ru

10. Development patterns: MVC vs MVP vs MVVM vs MVI. Available at: https://habr.com/ru/post/344184/

11. *Skripnik D. A.* General issues of technical protection of information. Available at: http:// www. intuit. ru /goods_store/ebooks/8563

12. Special requirements and recommendations for the protection of confidential information, the state Commission of Russia. Moscow: 2001.

13. *Titov A. A.* Engineering and technical protection of information: A textbook for students of the specialties "Organization and technology of information protection", "Complex protection of information objects" and "information security of telecommunication systems". Tomsk : Tomsk state University of control systems and Radioelectronics, 2010. 197 p.

14. *Torokin A. A.* Engineering and technical protection of information. Moscow : Helios ARV, 2005.

15. *Chaliapin D. B.* Acoustoelectric, custom-searchengine channels of information leakage and possible ways of their suppression. Moscow : "The world of security". No. 5. P. 47–53.

16. *Horev A. A.* Control of the effectiveness of protection of auxiliary technical means // Information Protection. Insider trading. St. Petersburg : Publishing house "Athena", 2009. No 1, P. 42–52.

17. *Horev A. A.* Technical channels for leakage of acoustic (speech) information // Special technique. Moscow : 2009. No. 5. P. 12–26.

18. *Horev A. A.* Protection of information from leakage through technical channels. Part 1. Technical channels for information leakage. Moscow : State technical Commission of the Russian Federation, 1998. 320 p.

19. *Horev A. A.* Methods and means of information protection. Textbook. Moscow : MO RF, 2000. 316 p.

20. *Mallawaarachchi Vijini.* 10 Common Software Architectural Patterns in a nutshell // Towards Data Science. Available at: https://towardsdatascience.com/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013

Korochentsev Denis A. – PhD in Technical Sciences, Acting Head of the Department of Cyber Security of Information Systems, Don State Technical University.
E-mail:center-bit@yandex.ru
ORCID iD: https://orcid.org/0000-0002-4491-3376

Cherkesova Larisa V. – DSc in Technical Sciences, Professor, Department of Cyber Security of Information Systems, Don State Technical University.
E-mail: chia2002@inbox.ru
ORCID iD: https://orcid.org/0000–0002–9392–3140