Для цитирования: *Д.А. Короченцев, Л.В. Черкесова, К.А. Намавир. Имитационная модель идентификации угроз нарушения информационной безопасности, возникающих за счет низкочастотных акустоэлектрических преобразований Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47(2): 65-74. DOI:10.21822/2073-6185-2020-47-2-65-74*
For citation: *D. A. Korochentsev, L. V. Cherkesova, K. A. Namavir. A simulation model for identifying information security threats from low-frequency acoustoelectric transformations. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47 (2): 65-74. (In Russ.) DOI:10.21822/2073-6185-2020-47-2-65-74*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 004.056/ББК 32.81
DOI: 10.21822/2073-6185-2020-47-2-65-74

ИМИТАЦИОННАЯ МОДЕЛЬ ИДЕНТИФИКАЦИИ УГРОЗ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ВОЗНИКАЮЩИХ ЗА СЧЕТ НИЗКОЧАСТОТНЫХ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Д.А. Короченцев, Л.В. Черкесова, К.А. Намавир
Донской государственный технический университет,
344000, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. *В статье рассмотрены физические основы формирования технического канала утечки информации, возникающего за счет низкочастотных акустоэлектрических преобразований.* ***Метод.*** *Исследование основано на методах имитационного моделирования. Применена методика инструментально-расчетного контроля защищенности речевой информации в рассматриваемом канале утечки информации.* ***Результат.*** *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 имитационной модели идентификации угроз нарушения информационной безопасности, возникающих за счёт низкочастотных акустоэлектрических преобразований.* ***Вывод.*** *Разработанная имитационная модель может использоваться специалистами по безопасности, как крупных, так и малых предприятий, реализующих мероприятия по защите информации. 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*

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

A SIMULATION MODEL FOR IDENTIFYING INFORMATION SECURITY THREATS FROM LOW-FREQUENCY ACOUSTOELECTRIC TRANSFORMATIONS

D.A. Korochentsev, L.V. Cherkesova, K.A. Namavir
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344000, Russia

Abstract. Aim. *The article considers the physical basis for the formation of a technical channel of information leakage due to low-frequency acoustoelectric transformations.* ***Methods.*** *The research was based on simulation modelling methods. The method of instrumental and computational control of the security of speech information in the considered channel of information leakage was applied.* ***Results.*** *Based on the developed simulation model, using the Model-View-Presenter design pattern, a software tool was*

developed. The main software classes implementing this model are presented. The functionality of the developed software tool is demonstrated and recommendations are given on the possible application of the developed simulation model for identifying threats to information security due to low-frequency acoustoelectric transformations. ***Conclusion.*** *The developed simulation model can be used by security specialists at both large and small enterprises, which implement measures for ensuring information protection. The model creates conditions for its active implementation in the educational process of training specialists in the field of information security, using both traditional (contact work) and distance learning formats.*

Keywords: *computerization object, acoustoelectric channels of information leakage, information protection, threat to information security, simulation model, information security*

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.

Постановка задачи. 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.

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].

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].

Методы исследования. Методика инструментально–расчётного контроля защищенности речевой информации в канале НЧ АЭП 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

$$\Delta_i \leq \Delta_{\text{н}} \qquad (1)$$

считается, что проверяемое ВТСС не подвержено явлению низкочастотных акустоэлектрических преобразований.

В противном случае, производится расчёт значения словесной разборчивости речи $W_{\text{с}}$. Рассчитанное значение $W_{\text{с}}$ сравнивается с нормированным значением $W_{\text{н}}$ [16, 5].

При выполнении неравенства

$$W_{\text{с}} \leq W_{\text{н}} \qquad (2)$$

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 $К_{л,i}$ опасных сигналов исследуемой линии на среднегеометрических частотах октавных полос [16].

С учётом $К_{л,i}$ исследуемой линии на среднегеометрических частотах октавных полос рассчитывается отношение «сигнал/шум» на границе контролируемой зоны (КЗ) в ***i***-й октаве Δ_i^*.

При выполнении неравенства

$$\Delta_i^* \leq \Delta_{\text{н}} \qquad (3)$$

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

$$W_c^* \leq W_{\text{н}} \qquad (4)$$

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 которого представлена на рис.2.

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 $U_{сш1}$ на выходных контактах ТС на частоте 1–й октавы.

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).

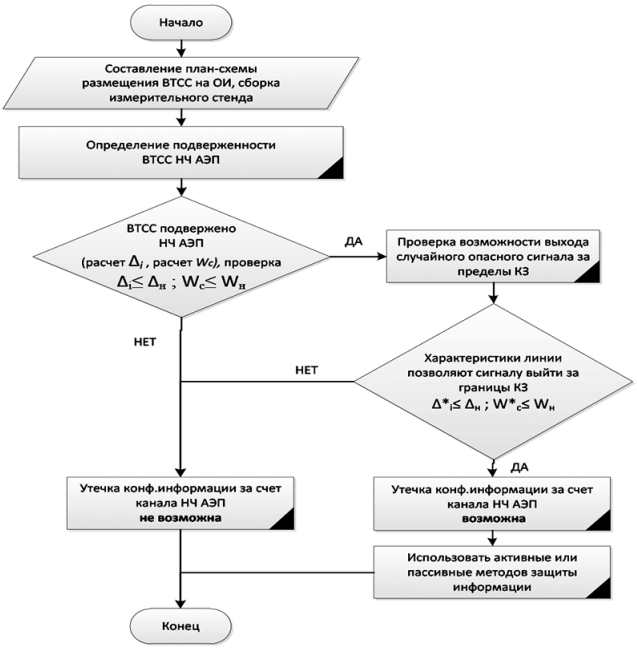

Рис. 1. Имитационная модель определения технических каналов утечки информации за счёт низкочастотных акустоэлектрических преобразований
Fig. 1. Simulation model for determining technical channels of information leakage due to low-frequency acoustoelectric transformations

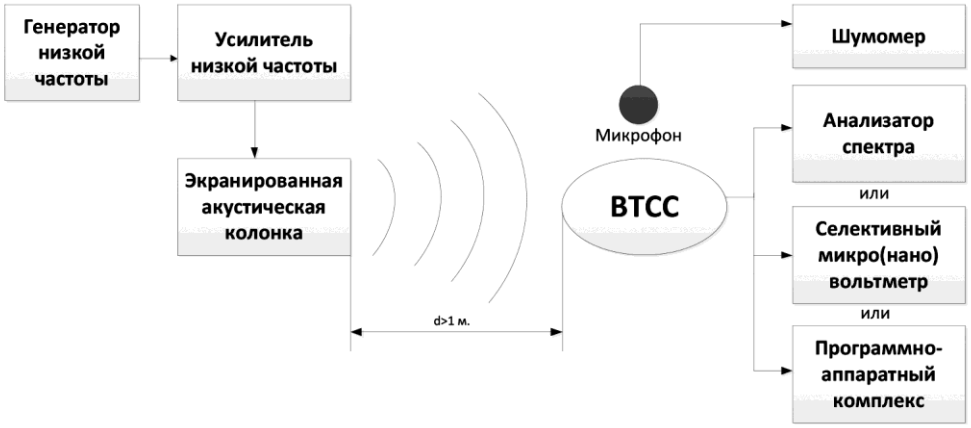

Рис. 2. Специальный измерительный стенд, используемый для определения канала низкочастотных акустоэлектрических преобразований
Fig. 2. A special measuring stand used to determine the channel of low-frequency acoustoelectric conversions

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 $К_{л,i}$, собирают схему, представленную на рис. 3, 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.

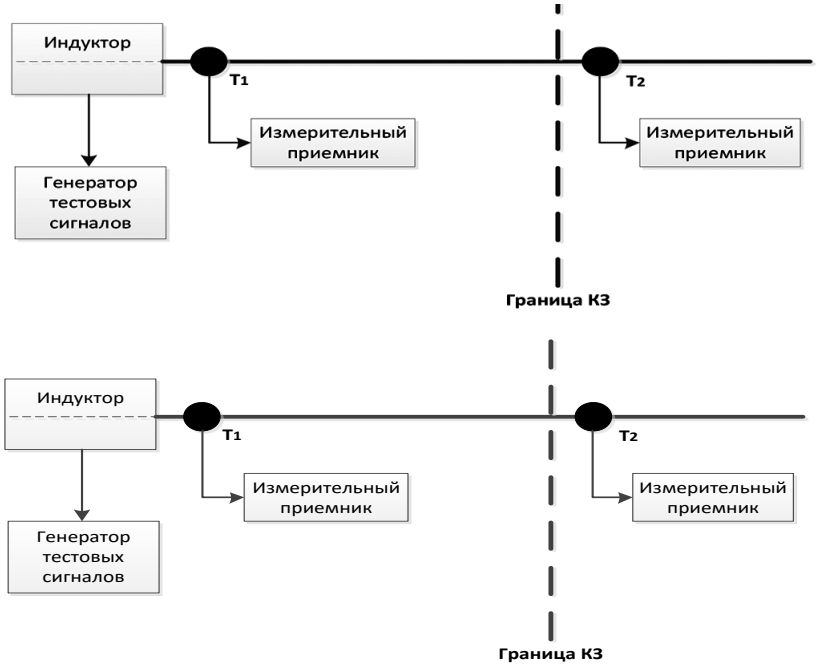

Рис. 3. Схема измерения коэффициента затухания исследуемой линии ВТСС
Fig. 3. Circuit for measuring the attenuation coefficient of the investigated VTSS line

Порядок обработки результатов измерений и расчета $\Delta_i(\Delta_i^*)$, $W_c(W_c^*)$ приведен в [2, 3, 5, 16].

Обсуждение результатов. 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) (рис.4).

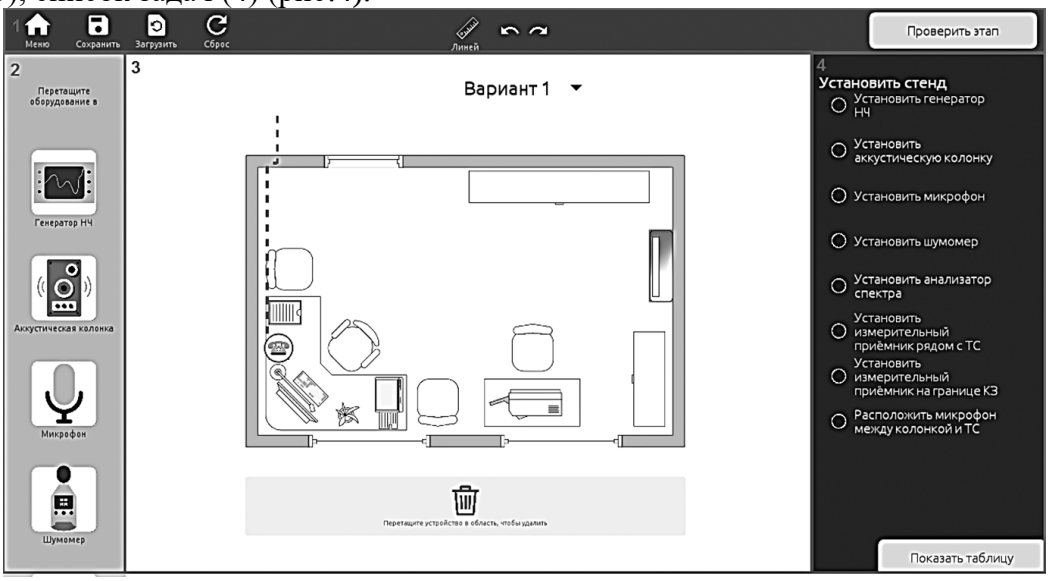

Рис. 4. Пользовательский интерфейс программного средства
Fig. 4. User interface of the software

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) (рис.5).

Кнопка выполнения этапа является контекстной, и в зависимости от состояния либо выполняет проверку этапа специальных исследований объекта информатизации, либо вызывает таблицу из протокола.

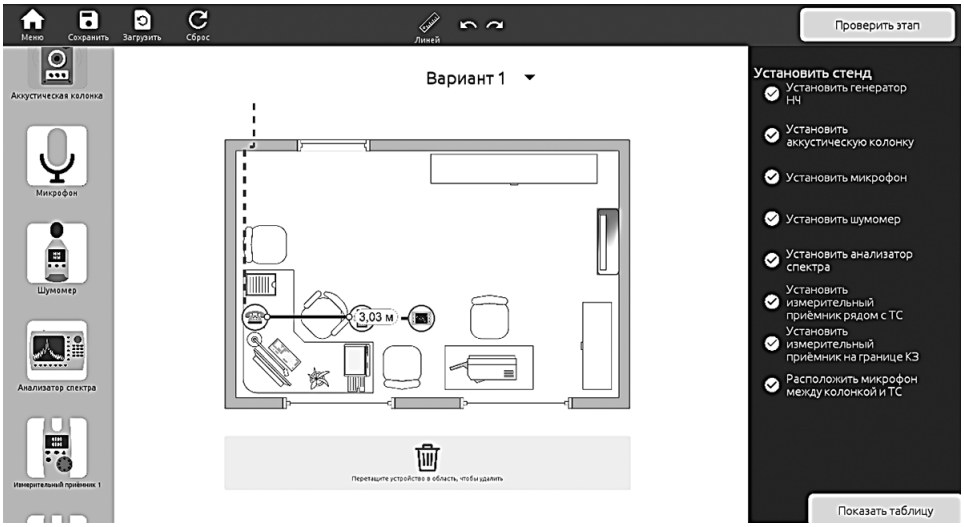

Рис. 5. Измерение расстояния между ВТСС и экранированной акустической колонкой
Fig. 5. Measurement of the distance between the VTSS and the shielded speaker

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 рисунке 4 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), рис. 5).

Первым этапом Методики является сборка специального измерительного стенда, в соответствии схемой, представленной на рис. 2. 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. Помимо этого, для проверки правильности расположения КИО относительно друг друга и ВТСС, можно воспользоваться линейкой (рис.5).

После того, как специальный измерительный стенд был собран в соответствии с правилами проведения инструментального контроля, 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. 6 графически изображено проведение измерений уровней звукового давления L_1 и электрического сигнала и шума $U_{ш1}$ на выходных контактах ТС на частоте 1–й октавы (275 Гц).

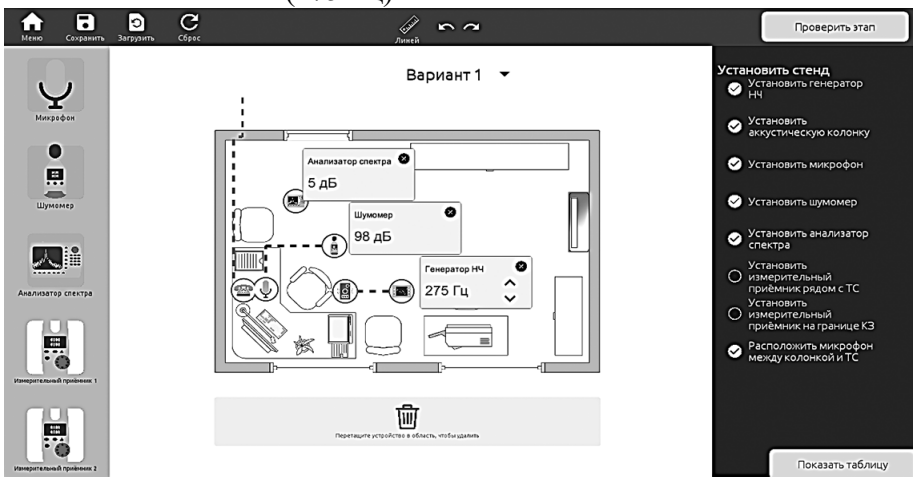

Рис. 6. Проведение измерений уровней звукового давления и электрического сигнала и шума на выходных контактах ВТТС на частоте 275 Гц
Fig. 6. Carrying out measurements of the levels of sound pressure and electrical signal and noise at the output contacts of VTTS at a frequency of 275 Hz

После того, как проведены измерения значений уровней звукового давления L_i, электрического сигнала и шума U_{cui} на выходных контактах ТС, электрического шума на выходных контактах ТС U_{ui}, а в случае невыполнения 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 (таблица 1, появляющаяся после нажатия контекстной кнопки в панели «Список задач», рис. 7).

Рис. 7. Таблица значений, измеренных с помощью КИО
Fig. 7. Table of values measured with KIO

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 таблицы 1-4 (рис. 8).

Рис. 8. Результат проверки расчетов по измеренным значениям
Fig. 8. Result of verification of calculations based on measured values

Дополнительным функционалом таблиц 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 изменится на зеленый, в противном случае ячейка окрасится красным.

Вывод. 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.

Библиографический список:

1. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия - Телеком, 2005. 416 с.
2. Волков Д.С., Козлов А.О. Методика оценки защищенности систем передачи данных от утечки речевой конфиденциальной информации по каналам электроакустических преобразований // 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., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации: Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.
6. Емельянов С.Л. Техническая разведка и технические каналы утечки информации // Системы обработки информации. – 2010. – Вып. 3. – С. 20–23.
7. Железняк В. К., Макаров Ю. К., Хорев А. А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – М.: 2000. № 4, с. 39–45.
8. Зайцев А.П., Шелупанов А.А., Технические средства и методы защиты информации. 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. URL 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». – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 197 с.
14. Торокин А.А. Инженерно–техническая защита информации. - М.: Гелиос АРВ, 2005
15. Халяпин Д.Б. Акустоэлектрические, акустопреобразовательные каналы утечки информации и возможные способы их подавления. М.: «Мир безопасности», № 5, с. 47-53
16. Хорев А.А. Контроль эффективности защиты вспомогательных технических средств // Защита информации. Инсайд. – Издательский дом «Афина», СПб.: 2009. - № 1, с. 42-52
17. Хорев А.А. Технические каналы утечки акустической (речевой) информации // 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. – М.: Гостехкомиссия РФ, 1998. – 320 с.
19. Хорев А.А. Способы и средства защиты информации. Учебное пособие. – М.: МО РФ, 2000. – 316 с.
20. Common Software Architectural Patterns in a nutshell / Vijini Mallawaarachchi // Towards Data Science [Электронный ресурс] URL: https://towardsdatascience.com/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013

References:

1. Buzov G.A., Kalinin S.V., Kondrat'yev A.V. Zashchita ot utechki informatsii po tekhnicheskim kanalam: Uchebnoye posobiye. - M.: Goryachaya liniya - Telekom, 2005. 416 s. [Buzov G. A., Kalinin S. V., Kondratyev A.V. Protection against information leakage through technical channels: the manual. - Moscow: Hotline-Telecom, 2005. 416 p. (In Russ)]
2. Volkov D.S., Kozlov A.O. Metodika otsenki zashchishchennosti sistem peredachi dannykh ot utechki rechevoy konfidentsial'noy informatsii po kanalam elektroakusticheskikh preobrazovaniy // Nauchnyy poisk. 2014. № 2.5, s. 4-6. [Volkov D. S., Kozlov A. 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, pp. 4-6. (In Russ)]
3. Vremennaya metodika otsenki zashchishchennosti osnovnykh tekhnicheskikh sredstv i sistem...: Normativno–metodicheskiy dokument // Sbornik vremennykh metodik otsenki zashchishchennosti konfidentsial'noy informatsii ot utechki po tekhnicheskim kanalam. – M.: Gostekhkomissiya Rossii, 2002. [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. (In Russ)]
4. GOST R 51275-2006. Zashchita informatsii. Ob"yekt informatizatsii. Faktory, vozdeystvuyushchiye na informatsiyu. Obshchiye polozheniya. – Vved. 01.02.2008 – M.: Standartinform, 2006. — 12 s [GOST R 51275-2006. Information protection. Object of Informatization. Factors that affect information. Generalities. - Yes. 01.02.2008-Moscow: STANDARTINFORM, 2006. 12 p. (In Russ)]
5. Durakovskiy A.P., Kunitsyn I.V., Lavrukhin YU.N. Kontrol' zashchishchennosti rechevoy informatsii v pomeshcheniyakh. Attestatsionnyye ispytaniya vspomogatel'nykh tekhnicheskikh sredstv i sistem po trebovaniyam bezopasnosti informatsii: Uchebnoye posobiye. – M.: NIYAU MIFI, 2015. − 152 s. [Durakovsky A. P., Kunitsyn I. 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: niyau MEPhI, 2015. 152 p. (In Russ)]

6. Yemel'yanov S.L. Tekhnicheskaya razvedka i tekhnicheskiye kanaly utechki informatsii // Sistemy obrabot-ki informatsii. – 2010. – Vyp. 3. – S. 20–23. [Emelyanov S. L. Technical intelligence and technical channels of information leakage / / information processing Systems. 2010. Vol. 3. pp. 20-23. (In Russ)]

7. Zheleznyak V. K., Makarov YU. K., Khorev A. A. Nekotoryye metodicheskiye podkhody k otsenke effektivnosti zashchity rechevoy informatsii // Spetsial'naya tekhnika. – M.: 2000. № 4, s. 39–45. [Zheleznyak V. K., Makarov Yu. K., Horev A. A. Some methodological approaches to evaluating the effectiveness of speech information protection / / Special technique. Moscow: 2000. No. 4, pp. 39-45. (In Russ)]

8. Zaytsev A.P., Shelupanov A.A., Tekhnicheskiye sredstva i metody zashchity informatsii. M.: Mashino-stroyeniye, 2009. – 507 s. [Zaitsev A. P., Shelupanov A. A., Technical means and methods of information protection. Moscow: Mashinostroenie, 2009. 507 p. (In Russ)]

9. Pavlovskiy YU.N. Imitatsionnyye modeli i sistemy / YU.N. Pavlovskiy. — M.: Fazis: VTS RAN, 2000. S. 134. [Pavlovsky Yu. N. Simulation models and systems / Yu. Pawlowski. - M.: fazis: VC RAS, 2000. P. 134. (In Russ)]

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

11. Skripnik D.A. Obshchiye voprosy tekhnicheskoy zashchity informatsii. URL http:// www. intuit. ru /goods_store/ebooks/8563 [Skripnik D. A. General issues of technical protection of information. URL http: / / www. intuit. ru /goods_store/ebooks/8563(In Russ)]

12. Special requirements and recommendations for the protection of confidential information (PAGE-K), the state Commission of Russia. - Moscow: 2001.

13. Titov A.A. Inzhenerno-tekhnicheskaya zashchita informatsii: Uchebnoye posobiye dlya studentov spetsial'nostey «Organizatsiya i tekhnologiya zashchity informatsii», «Kompleksnaya zashchita ob"yektov informatizatsii» i «Informatsionnaya bezopasnost' telekommunikatsionnykh sistem». – Tomsk: Tomsk. gos. un-t sistem upravleniya i radioelektroniki, 2010. – 197 s. [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. (In Russ)]

14. Torokin A.A. Inzhenerno–tekhnicheskaya zashchita informatsii. - M.: Gelios ARV, 2005 [Torokin A. A. Engineering and technical protection of information. - Moscow: Helios ARV, 2005(In Russ)]

15. Khalyapin D.B. Akustoelektricheskiye, akustopreobrazovatel'nyye kanaly utechki informatsii i voz-mozhnyye sposoby ikh podavleniya. M.: «Mir bezopasnosti», № 5, s. 47-53 [Chaliapin D. B. Acoustoelectric, customsearchengine channels of information leakage and possible ways of their suppression. Moscow: "The world of security", no. 5, pp. 47-53(In Russ)]

16. Khorev A.A. Kontrol' effektivnosti zashchity vspomogatel'nykh tekhnicheskikh sredstv // Zashchita in-formatsii. Insayd. – Izdatel'skiy dom «Afina», SPb.: 2009. - № 1, s. 42-52 [Horev A. A. Control of the effectiveness of protection of auxiliary technical means / / information Protection. Insider trading. - Publishing house "Athena", St. Petersburg.: 2009. No. 1, pp. 42-52(In Russ)]

17. Khorev A.A. Tekhnicheskiye kanaly utechki akusticheskoy (rechevoy) informatsii // Spetsial'naya tekhnika. - M.: 2009. - № 5, s. 12-26 [Horev A. A. Technical channels for leakage of acoustic (speech) information / / Special technique. - Moscow: 2009. No. 5, pp. 12-26 (In Russ)]

18. Khorev A.A., Zashchita informatsii ot utechki po tekhnicheskim kanalam. Chast' 1. Tekhnicheskiye kanaly utechki informatsii. – M.: Gostekhkomissiya RF, 1998. – 320 s. [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. (In Russ)]

19. Khorev A.A. Sposoby i sredstva zashchity informatsii. Uchebnoye posobiye. – M.: MO RF, 2000. – 316 s. [Horev A. A. Methods and means of information protection. Textbook. - Moscow: MO RF, 2000. 316 p. (In Russ)]

20. Common Software Architectural Patterns in a nutshell / Vijini Mallawaarachchi // Towards Data Science [Электронный ресурс] URL: https://towardsdatascience.com/10-common-software-architectural-patterns-in-a-nutshell-a0b47a1e9013

Сведения об авторах:

Кореченцев Денис Александрович, доктор технических наук, исполняющий обязанности заведующего кафедрой кибербезопасности информационных систем; ORCID 0000-0002-4491-3376; e-mail: center-bit@yandex.ru

Черкесова Лариса Владимировна, доктор технических наук, профессор, кафедра кибербезопасности информационных систем; e-mail: chia2002@inbox.ru

Намавир Константин Аркадьевич, студент, кафедра кибербезопасности информационных систем; e-mail: k.namavir@gmail.com

Information about the authors:

Denis A. Korechentsev, Dr. Sci.(Technical), Acting Head of the Department of Cybersecurity of Information Systems; ORCID 0000-0002-4491-3376; e-mail: center-bit@yandex.ru

Larisa V. Cherkesova, Dr. Sci.(Technical), Prof., Department of Cybersecurity of Information Systems; e-mail: chia2002@inbox.ru

Konstantin A.Namavir, Student, Department of Cybersecurity of Information Systems; e-mail: k.namavir@gmail.com

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 02.03.2020.
Принята в печать 18.04.2020.

Conflict of interest.
The authors declare no conflict of interest.
Received 02.03.2020.
Accepted for publication 18.04.2020.