

РАЗРАБОТКА ПРОГРАММНО- АППАРАТНОГО КОМПЛЕКСА ОЦЕНКИ И АНАЛИЗА АКУСТИЧЕСКОГО КАНАЛА УТЕЧКИ ИНФОРМАЦИИ

Защита выделенного или защищаемого помещения должна состоять из комплекса организационных, технических и иных мер предотвращающих несанкционированное получения или воздействия злоумышленником на защищаемую информацию. Оценка эффективности защищенности помещений по акустическому и виброакустическому каналам утечки информации определяется методическими документами ФСТЭК России. В статье рассматривается оценка утечки информации по акустическому каналу, приведены проблемы современных технических средств анализа исследуемого ТКUI. Для этого разработан программно-аппаратный продукт, позволяющий проводить оценку показателей акустической защищенности ограждающих конструкций помещения и выводить результаты в виде отчета.

Ключевые слова: информационная безопасность, утечка речевой информации, акустический канал, анализ звукоизоляционных свойств, ограждающие конструкции, оценка, защита информации, программно-технические каналы утечки информации.

Shpak V.A., Mikhailova U.V., Barankova I.I.

DEVELOPMENT OF SOFTWARE AND HARDWARE COMPLEX FOR EVALUATION AND ANALYSIS OF ACOUSTIC CHANNEL OF INFORMATION LOSS

Protection of dedicated or protected premises should consist of a set of organizational, technical and other measures that prevent unauthorized receipt or impact by an attacker on protected information. Evaluation of the effectiveness of the security of premises by acoustic and vibroacoustic channels of information leakage is determined by the methodological documents of the FSTEC of Russia. The article discusses the assessment of information leakage through the acoustic channel, presents the problems of modern technical means for analyzing

the studied channel of information loss. For this, a software and hardware product has been developed that allows evaluating the acoustic protection indicators of building envelopes and displaying the results in the form of a report.

Keywords: information security, speech information leakage, acoustic channel, analysis of sound insulation properties, enclosing structures, assessment, information protection, software and hardware channels of information leakage.

Защита акустической (речевой) информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта или учреждения. Для перехвата речевой информации предполагаемый «противник» может использовать каналы непреднамеренного прослушивания речи (без использования технических средств), а также широкий арсенал портативных средств акустической речевой разведки, позволяющих перехватывать речевую информацию по прямому акустическому, виброакустическому, электроакустическому и оптико-электронному (акустооптическому) каналам [1].

Выделенными (защищаемыми) помещениями называют помещения (служебные кабинеты, конференц-залы и т.п.), специально предназначенные для проведения различных кон-

фиденциальных мероприятий (совещаний, обсуждений, переговоров и т.п.). защите подлежит как само помещение, так и технические средства, расположенные в этом помещении, а именно основные технические средства и системы (ОТСС) и вспомогательные технические средства и системы (ВТСС). Кроме того, предусматриваются меры защиты от различных технических средств разведки, которые могут быть использованы злоумышленником для несанкционированного получения или воздействия на защищаемую информацию [2].

Совокупность объекта разведки, технического средства разведки, с помощью которого добывается информация, и физической среды, в которой распространяется информационный сигнал, называется техническим каналом утечки информации (рис. 1) [3].

На данный момент существует и исполь-



Рис. 1. Общая схема технического канала утечки информации

зуется множество готовых средств оценки и анализа вибро- и акустического канала утечки информации, таких семейств как «Спрут», «Шепот», «Аврора» и проч. Такие средства обеспечивают полную достоверность измерений и расчетов согласно существующему сборнику нормативно-методических документов ФСТЭК России, однако их преследует ряд недостатков. К таким недостаткам относятся сложность при разворачивании средства в рабочее состояние из-за проводного подключения компонентов комплекса и отсутствие функции автоматического формирования отчета акустической защищенности защищаемых помещений.

Для решения первого недостатка существующих средств оценки и анализа акустического канала утечки информации была разработана схема шумомера (рис. 2). Данная схема построена на основе операционного усилителя LM386 и отличается наличием фильтров низких и верхних частот, позволяющих проводить проверку как на пяти октавах, так и на семи. Коэффициент усиления микросхемы LM386 можно регулировать подстроечным резистором RP2. Собранная схема подключается к микроконтроллеру Arduino Nano. Беспроводная связь с устройством управления комплексом обеспечивается за счет Wi-Fi модуля ESP 12e. Собранный шумо-

мер энергетически автономен благодаря Li-ion аккумулятору.

В качестве генератора шума в разрабатываемом комплексе временно используется портативная беспроводная акустическая колонка JBL Flip 5. К ее преимуществам относятся компактность, автономность, наличие уда-

ропрочного корпуса, однако использование генератора шума, не предназначенного для проверки защищаемых помещений, требует дополнительной настройки в эквалайзере из-за неровной амплитудно-частотной характеристики тестового сигнала [4].

Очень важно правильно интерпретиро-

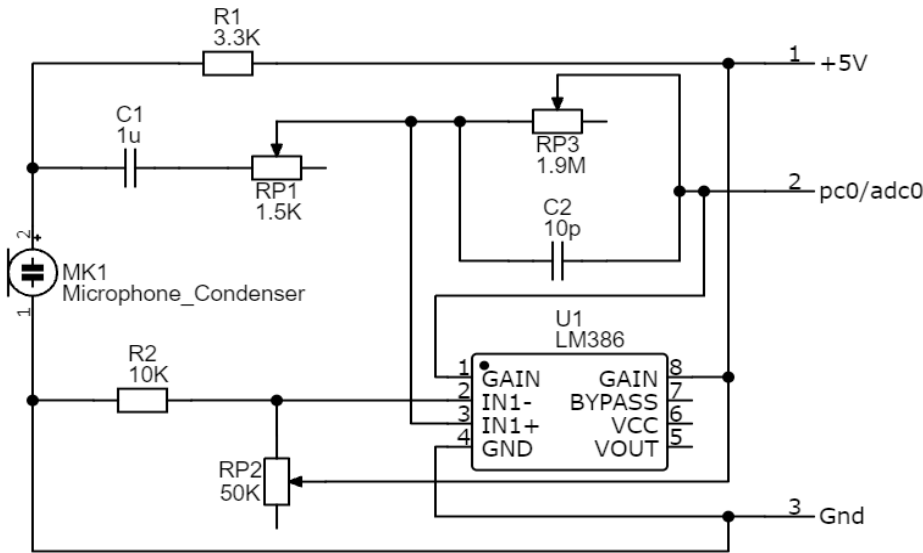


Рис. 2. Схема шумомера

вать данные полученные с АЦП, поскольку значения уровня звукового давления имеют нелинейную зависимость от имеющихся значений АЦП с выхода аналогового контакта Arduino. Для этого нужно откалибровать шумомер по эталонному измерителю шума CEM DT-8851. Для наиболее точной калибровки нужно произвести несколько измерений на каждой октаве для обоих шумомеров. На основе полученных данных можно провести корреляцию между значениями методом линейной регрессии.

Управление шумомером и его режимами работы осуществляется посредством разработанного программного продукта для оценки изоляционных свойств ограждающих конструкций. Данное ПО было разработано в программной среде C#. Для работы приложения в качестве полноценного комплекса необходимо и достаточно использовать ноутбук с ОС Windows 7 и .NET Framework 5.0. В программе реализована форма для указания основных сведений об исследуемом объекте (рис. 3).

Название исследуемого объекта:	Объект 1
Адрес исследуемого объекта:	г. Магнитогорск ул. Ленина 38 ауд. 2122
Назначение исследуемого объекта:	лаборатория ТЗИ
План-схема исследуемого объекта:	...
Звукоусиление:	не установлено
Далее	

Рис. 3. Стартовая форма ПО

Одно из преимуществ разрабатываемого ПО, по сравнению с существующими аналогами — наличие графического редактора (рис. 4) для расстановки контрольных точек (КТ) на техническом плане исследуемого помещения. КТ поделены на типы ограждающих кон-

струкций (окна, стены и т.д.), каждый из которых поделен на различные виды типовых конструкций. Типовые виды ограждающих конструкций взяты из методики ФСТЭК России. В окне расстановки КТ каждый тип ограждающих конструкций обозначен своим

цветом: стены и сплошные перегородки кирпичного цвета, двери — коричневые, перекрытия — серые, а окна — голубые. Помимо вида и типа для каждой КТ можно настраивать толщину и прочие особенности конструкций, характерные для того или иного типа ограждающей конструкции.

После задания КТ в графическом редакторе и расстановки измерительного оборудования у КТ №1 в положение согласно мето-

дике ФСТЭК России, проводится автоматическое сканирование ограждающей конструкции. После окончания комплекса измерений в одной КТ приложение предложит оператору устройства управления комплексом переставить измерительное оборудование в другую КТ. Измерения должны проводиться при минимально возможных уровнях акустических и вибрационных шумов.

На основе выполненных измерений про-

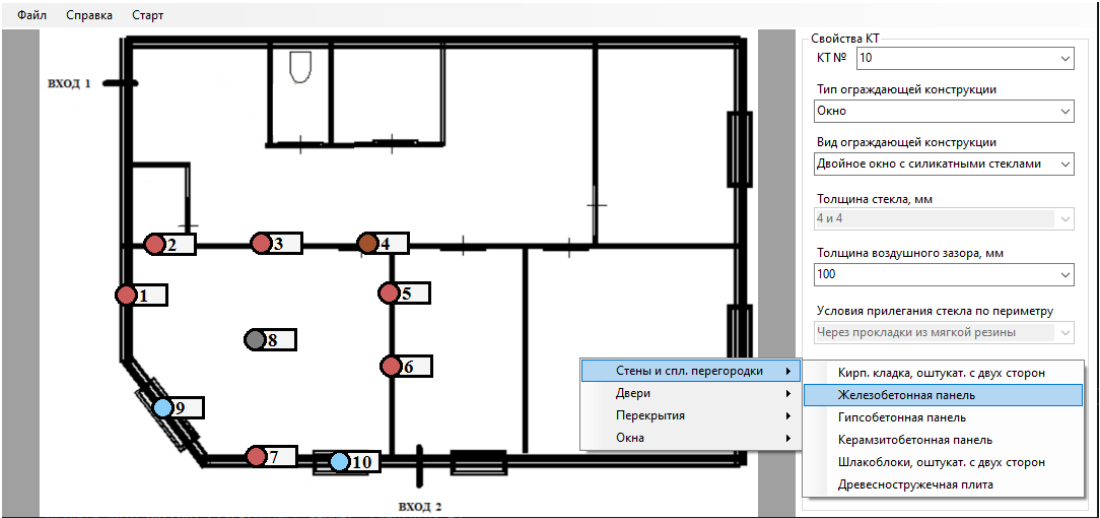


Рис. 4. Окно расстановки КТ

Результат сканирования						
Файл Справка						
КТ	Среднегеометрическая частота, Гц	Измеренный уровень акуст. шума в КТ, Дб	Уровень измеренного суммарного сигнала, Дб	Расчетный уровень акустического сигнала в КТ, Дб	Измеренный уровень акустического сигнала в помещении	Октавные уровни звукоизоляции в контрольной точке, Дб
1	250	36	39,1	3,1	70	66,9
(Железобетонная панель 100 мм.)	500	36	37,5	1,5	70	68,5
	1000	36	37,5	1,5	70	68,5
	2000	36	38,3	2,3	70	67,7
	4000	36	40,5	4,5	70	65,5
	8000	36	37,7	1,7	70	70,3
2	250	38	37,8	1,8	72	70,2
(Железобетонная панель 100 мм.)	500	38	38,2	2,2	72	69,8
	1000	38	37,8	1,8	72	70,2
	2000	38	38	2	72	70
	4000	38	53,4	15,4	72	54,6
	8000	38	46,8	8,8	72	61,2
3	250	36	60	22	70	48
(Железобетонная панель 100 мм.)	500	36	53	15	70	55

Рис. 5. Окно результатов сканирования

водятся расчеты звукоизоляции ограждающих конструкций на исследуемом объекте согласно методике ФСТЭК России. Результат расчетов выводится в таблицу на пользовательскую форму (рис. 5).

Итоговая схема работы комплекса указа-

на на рис. 6. Устройство управления комплексом по Bluetooth передает на генератор шума тест-сигнал. Генератор шума излучает полученный акустический сигнал через ограждающую конструкцию в месте установки КТ. Шум, прошедший ограждающую конструк-



Рис. 6. Общий принцип работы комплекса

цию улавливается шумомером, обрабатывается АЦП и по сети Wi-Fi передается на устройство управления комплексом. Последний этап — устройство управления комплексом по полученному уровню звукового давления рассчитывает звукопоглощающие свойства исследуемой ограждающей конструкции согласно нормативно-методическому документу по противодействию акустической речевой разведке.

По полученным результатам составляется отчет в PDF формате. В отчет входят: информация об исполнителе проверки помещения, адресе и функциональном назначении помещения, план помещения с расставленными на нем КТ, таблица с проведенными измерениями и расчетами для каждой КТ, а также заключение о соответствии помещения требованиям безопасности.

Выполнив оценку работы разрабатываемого средства оценки и анализа акустического канала утечки информации можно составить заключение о том, что данный программно-аппаратный продукт, выполняя измерения, получает достоверные данные, а также упрощает процедуру анализа полученных данных. Комплекс легко разворачивать в рабочее состояние благодаря полностью беспроводному подключению компонентов. Положительными отличительными особенностями программной части комплекса являются наличие функций графического редактора расстановки КТ и создания автоматического развернутого отчета акустической защищенности защищаемых помещений, оформленного согласно требованиям ФСТЭК России, в PDF формате.

Литература

1. Оценка эффективности защиты акустической (речевой) информации. – «электрон. текст. дан.». – Москва: [б.и.], 20.08.2016. – Режим доступа: <https://itsec2012.ru/ocenka-effektivnosti-zashchity-akusticheskoy-rechevoy-informacii>.
2. Акустическая защита выделенного (защищаемого) помещения. – Электрон. журн. – Москва: DELPHI PLUS - ежедневные новости IT-технологий, 2017. – режим доступа к журн.: <https://www.delphiplus.org/>.
3. Хорев, А. А. Технические каналы утечки информации, обрабатываемой техническими средствами. / Хорев, А. А. // – Электрон. журн. – Москва: Бюро научно-технической информации, 2006. – режим доступа к журн.: <http://www.bnti.ru/>.
4. JBL flip5 ACH / JBL flip5 frequency response / EQ // – Электрон. журн. – Новосибирск: Webstudius Новосибирск, 2021. – режим доступа: <https://webstudius.com/jbl-flip5-achh-jbl-flip5-frequency-response>.
5. Михайлова, У. В. Эффективность применения СЗИ от утечки по акустическим каналам / У. В. Михайлова, Г. И. Лукьянов // Вестник УрФО. Безопасность в информационной сфере. 2014. № 4 (14). С. 14–18.
6. Михайлова, У. В. Защита информации в помещении от утечки по акустическому каналу /

У. В. Михайлова, Г. И. Лукьянов // Актуальные проблемы современной науки, техники и образования: тезисы докладов 76-й Междунар. науч.-техн. конф. 2018. С. 294.

7. Баранкова И. И. Компетентностно-ориентированный подход к формированию лабораторий учебно-тренировочных средств при подготовке специалистов в области информационной безопасности // Информационное противодействие угрозам терроризма. 2015. Т. 1. № 25. С. 46–50.

8. Лукьянов, Г. И. Защита информации по виброакустическим каналам с использованием СЗИ «СОНАТА» / Г. И. Лукьянов, У. В. Михайлова, И. И. Баранкова, М. В. Коновалов // Актуальные проблемы современной науки, техники и образования. 2015. Т. 2. № 1. С. 186–188.

9. Хорев, А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев // М: НПЦ «Аналитика», 2008. 436 с.

10. Григорьев И. А., Казановский А. И. / Методический подход к оценке эффективности защиты речевой информации // Вестник ВГТУ. 2010. №5. URL: <https://cyberleninka.ru/article/n/metodicheskiy-podhod-k-otsenke-effektivnosti-zaschity-rechevoy-informatsii>.

References

1. Ocenka jeffektivnosti zashhity akusticheskoy (rechevoj) informa-cii. – «jelektron. tekst. dan.». – Moskva: [b.i.], 20.08.2016. – Rezhim dostupa: <https://itsec2012.ru/ocenka-effektivnosti-zashchity-akusticheskoy-rechevoy-informacii>.

2. Akusticheskaja zashhita vydelennogo (zashhishhaemogo) pomeshhenija. – Jelektron. zhurn. – Moskva: DELPHI PLUS - ezhednevnye novosti IT-tehnologij, 2017. – rezhim dostupa k zhurn.: <https://www.delphiplus.org/>.

3. Horev, A. A. Tehnicheskie kanaly utechki informacii, obrabaty-vaemoj tehničeskimi sredstvami. / Horev, A. A. // – Jelektron. zhurn. – Moskva: Bjuro nauchno-tehnicheskoy informacii, 2006. – rezhim dostupa k zhurn.: <http://www.bnti.ru/>.

4. JBL flip5 AChH / JBL flip5 frequency response / EQ // – Jelektron. zhurn. –Novosibirsk: Webstudius Novosibirsk, 2021. – rezhim dostupa: <https://webstudius.com/jbl-flip5-achh-jbl-flip5-frequency-response>.

5. Mihajlova, U. V. Jeffektivnost' primeneniya SZI ot utechki po akusticheskim kanalam / U. V. Mihajlova, G. I. Luk'janov // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2014. № 4 (14). P. 14–18.

6. Mihajlova, U. V. Zashhita informacii v pomeshhenii ot utechki po akusticheskomu kanalu / U. V. Mihajlova, G. I. Luk'janov // Aktual'nye pro-blemy sovremennoj nauki, tehniki i obrazovanija: tezisy dokladov 76-j Mezhdunar. nauch.-tehn. konf. 2018. P. 294.

7. Barankova I. I. Kompetentnostno-orientirovannyj podhod k formirovaniju laboratorij uchebno-trenirovochnyh sredstv pri podgotovke specialistov v oblasti informacionnoj bezopasnosti // Informacionnoe protivodejstvie ugrozam terrorizma. 2015. Т. 1. № 25. P. 46–50.

8. Luk'janov, G. I. Zashhita informacii po vibroakusticheskim kana-lam s ispol'zovaniem SZI «SONATA» / G. I. Luk'janov, U. V. Mihajlova, I. I. Barankova, M. V. Konovalov // Aktual'nye problemy sovremennoj nauki, tehniki i obrazovanija. 2015. Т. 2. № 1. P. 186–188.

9. Horev, A. A. Zashhita informacii ot utechki po tehničeskim kana-lam. Chast' 1. Tehnicheskie kanaly utechki informacii / A. A. Horev // М: NPC «Analitika», 2008. 436 p.

10. Grigor'ev I. A., Kazanovskij A. I. / Metodicheskij podhod k ocenke jeffektivnosti zashhity rechevoj informacii // Vestnik VGTU. 2010. №5. URL: <https://cyberleninka.ru/article/n/metodicheskiy-podhod-k-otsenke-effektivnosti-zaschity-rechevoy-informatsii>.

ШПАК Виталий Алексеевич, студент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: xxx-yyy-2014@inbox.ru

МИХАЙЛОВА Ульяна Владимировна, кандидат технических наук, доцент кафедры Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: ylianapost@gmail.com

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующая кафедрой Информатики и Информационной Безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, проспект Ленина, 38. E-mail: inna_barankova@mail.ru

SHPAK Vitaliy Alekseevich, student of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: xxx-yyy-2014@inbox.ru

MIKHAILOVA Uliana Vladimirovna, Candidate of Technical Sciences, Associate Professor of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: ylianapost@gmail.com

BARANKOVA Inna Ilyinichna, Doctor of Technical Sciences, Head of the Department of Informatics and Information Security of Nosov Magnitogorsk State Technical University (NMSTU). 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru