A. S. Porkhun, A. V. Dushkin, R. V. Meshcheryakov, Yu. V. Savchenko, V. A. Shcherbakov, Software and hardware complex for investigation of technical channels of information leakage based on high-frequency irradiation method, *Comp. nanotechnol.*, 2022, Volume 9, Issue 4, 55–62

https://www.mathnet.ru/eng/cn396

2.3.6 *МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

INFORMATION SECURITY

DOI: 10.33693/2313-223X-2022-9-4-55-62

УДК 004.9

Программно-аппаратный комплекс для исследования технических каналов утечки информации на основе метода высокочастотного облучения

А.С. Порхун[1, a] ©, А.В. Душкин[1, 2, b] ©, Р.В. Мещеряков[3, c] ©, Ю.В. Савченко[4, b] ©, В.А. Щербаков[1, d] ©

[1] **Национальный исследовательский университет «Московский институт электронной техники», г. Москва, г. Зеленоград, Российская Федерация**

[2] **МИРЭА – Российский технологический университет, г. Москва, Российская Федерация**

[3] **Институт проблем управления имени В.А. Трапезникова Российской академии наук, г. Москва, Российская Федерация**

[4] **Институт микроприборов и систем управления имени Л.Н. Преснухина Национального исследовательского университета «Московский институт электронной техники», г. Москва, г. Зеленоград, Российская Федерация**

[a] **E-mail: tolik.porkhun@mail.ru**

[b] **E-mail: a_dushkin@mail.ru**

[c] **E-mail: meshcheryakov.roman@gmail.com**

[d] **E-mail: svasvarog@yandex.ru**

Аннотация. Вариант создания канала утечки информации с использованием высокочастотного облучения (например, вспомогательных технических средств или полуактивных закладочных устройств, установленных в помещении) относится к числу активных способов получения акустической речевой информации. В данной работе приводится обоснование требований к техническим характеристикам и схеме построения устройства обнаружения сигналов высокочастотного облучения. Оно служит для разработки программно-аппаратного комплекса для исследования технических каналов утечки информации, использующих в своей основе метод высокочастотного облучения. Конечной целью является создание макета средства обнаружения и подавления приемных устройств аппаратуры высокочастотного облучения на базе программно-определяемых устройств. В работе описывается подход к созданию аппаратной и программной частей комплекса, приводятся результаты исследований по обнаружению сигналов в широком частотном диапазоне.

Ключевые слова: акустическая речевая информация, акустическая речевая разведка, выделенное помещение, высокочастотное облучение, объект защиты, программно-аппаратный комплекс, сигнал

ССЫЛКА НА СТАТЬЮ: Порхун А.С., Душкин А.В., Мещеряков Р.В., Савченко Ю.В., Щербаков В.А. Программно-аппаратный комплекс для исследования технических каналов утечки информации на основе метода высокочастотного облучения // Computational Nanotechnology. 2022. Т. 9. № 4. С. 55–62. DOI: 10.33693/2313-223X-2022-9-4-55-62

DOI: 10.33693/2313-223X-2022-9-4-55-62

Software and Hardware Complex for Investigation of Technical Channels of Information Leakage Based on High-frequency Irradiation Method

A.S. Porkhun[1, a] ©, A.V. Dushkin[1, 2, b] ©, R.V. Meshcheryakov[3, c] ©, Yu.V. Savchenko[4, b] ©, V.A. Shcherbakov[1, d] ©

[1] National Research University of Electronic Technology, Moscow, Zelenograd, Russian Federation

[2] MIREA – Russian Technological University, Moscow, Russian Federation

[3] Institute of Control Problems named after V.A. Trapeznikov RAS, Moscow, Russian Federation

[4] Institute of Microdevices and Control Systems named after L.N. Presnukhina of the National Research University of Electronic Technology, Moscow, Zelenograd, Russian Federation

[a] E-mail: tolik.porkhun@mail.ru

[b] E-mail: a_dushkin@mail.ru

[c] E-mail: meshcheryakov.roman@gmail.com

[d] E-mail: svasvarog@yandex.ru

Abstract. The option of creating an information leakage channel using high-frequency radiation (for example, auxiliary technical means or semi-active stowage devices installed indoors) is one of the active methods for obtaining acoustic speech information. This paper provides a rationale for the requirements for technical characteristics and the scheme for constructing a device for detecting high-frequency radiation signals. It serves to develop a software and hardware complex for the study of technical channels of information leakage, based on the method of high-frequency irradiation. The ultimate goal is to create a prototype of a means for detecting and suppressing receiving devices of high-frequency irradiation equipment based on software-defined devices. The paper describes an approach to the creation of the hardware and software parts of the complex, presents the results of studies on the detection of signals in a wide frequency range.

Key words: acoustic speech information, acoustic speech intelligence, allocated premises, high-frequency irradiation, object of protection, software and hardware complex, signal

FOR CITATION: Porkhun A.S., Dushkin A.V., Meshcheryakov R.V., Savchenko Yu.V., Shcherbakov V.A. Software and Hardware Complex for Investigation of Technical Channels of Information Leakage Based on High-frequency Irradiation Method. *Computational Nanotechnology*. 2022. Vol. 9. No. 4. Pp. 55–62. (In Rus.) DOI: 10.33693/2313-223X-2022-9-4-55-62

ВВЕДЕНИЕ

Комплекс мероприятий по обеспечению безопасности акустической речевой информации (АРИ) является одной из основных составляющих в ряде мероприятий по технической защите информации выделенных помещений (ВП). Выделенные помещения, как правило, оборудуются в органах системы государственного аппарата управления, на объектах военно-промышленного комплекса, в зданиях и сооружениях научно-исследовательских комплексов и т.д. Нормативно-методической базой, которой необходимо руководствоваться при решении задач обеспечения защиты ВП, являются нормативно-методические документы (НМД) регулятора в области информационной безопасности – Федеральной службы по техническому и экспортному контролю (ФСТЭК России); Федеральной службы безопасности России (ФСБ России) в вопросах, касающихся шифров и криптографии, и иные ведомственные НМД, которые разрабатываются на их основе.

В реальности очень часто, в нарушение инструкций, обсуждение вопросов конфиденциального характера выносится за пределы контролируемой зоны вне выделенных помещений. Сотрудники организаций в оперативном порядке обсуждают между собой рабочие вопросы, касающиеся информации ограниченного доступа. Причем, обычно разговоры такого рода, как правило, происходят в комнатах, офисах и помещениях, которые не оборудованы средствами защиты; на площадках без ограждающих конструкций и т.д. Учитывая данный факт, злоумышленники (конкуренты, иностранные агенты и т.д.) с большой долей вероятности могут получать информацию из данных помещений, используя различные методы съема информации [1–7], в том числе и метод высокочастотного облучения (ВЧО). Существующие средства защиты АРИ основываются на экранировании (в ущерб стоимости), акустическом зашумлении выделенного помещения (в ущерб эргономике), пространственному электромагнитному зашумлению (в ущерб электромагнитной совместимости (ЭМС)).

На данный момент одним из самых эффективных способов защиты АРИ от ее перехвата методом высокочастотного облучения является экранирование помещений. Однако данный способ довольно дорогостоящий. Поэтому разработка методов и средств защиты речевой информации от ее перехвата методом высокочастотного облучения является актуальной научной задачей. На рынке присутствует множество специализированных организаций, составляющих друг другу конкуренцию и выполняющих разработку, производство и реализацию технических средств защиты информации, дающих возможность инженерам качественно и эффективно решать вопросы защиты акустической информации от акустической речевой разведки (АРР). При этом совершенствование данных средств производится по следующим основным показателям: функциональные возможности, степень воздействия на персонал ВП (объекты защиты) и стоимость.

Цель статьи – с учетом проведенного анализа научной литературы по теме исследования необходимо обобщить, систематизировать и сформировать требования к средству обнаружения сигналов высокочастотного облучения (ВЧО) на базе SDR (software definition radio) технологии, привести обоснование схемы построения данного средства, дать описание экспериментальной установки и интерпретацию результатов исследований.

АНАЛИЗ РАБОТЫ СРЕДСТВ ПЕРЕХВАТА АКУСТИЧЕСКОЙ РЕЧЕВОЙ ИНФОРМАЦИИ МЕТОДОМ ВЫСОКОЧАСТОТНОГО ОБЛУЧЕНИЯ

Анализ работы средств перехвата акустической речевой информации методом высокочастотного облучения показал, что этот способ имеет следующие особенности:

- пассивное (полуактивное) закладное устройство, передатчик и приемник должны работать на одинаковых частотах в определенном диапазоне;
- передатчик излучает мощный СВЧ узкополосный сигнал;
- небольшая дальность активации закладного устройства (по сравнению с излучаемой мощностью);
- в системе для приема и передачи сигнала необходимо использовать направленные антенны с узкой диаграммой направленности;
- в закладных устройствах, как правило, используется как аналоговая (AM, FM), так и цифровая модуляция (PPM);
- уровень переизлученного сигнала достаточно слабый;
- закладное устройство имеет достаточно низкое потребление энергии, в результате чего может находится в активном состоянии долгое время (месяцы, годы);
- небольшая полоса пропускания приемника;
- уровень мощности облучающего сигнала может влиять на здоровье людей, находящихся в зоне облучения.

Эти особенности необходимо учитывать при обосновании требований к средствам обнаружения сигналов и средствам подавления приемных устройств аппаратуры высокочастотного облучения.

ОБОСНОВАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ОБНАРУЖЕНИЯ СИГНАЛОВ ВЫСОКОЧАСТОТНОГО ОБЛУЧЕНИЯ

Для обоснования требований к средствам обнаружения сигналов высокочастотного облучения воспользуемся итогами анализа из предыдущего раздела, приведем конкретные примеры и систематизируем эти данные.

Учитывая технические характеристики систем акустической разведки на основе метода ВЧО, приведенные в [8–14], можно заметить, что минимальная

частота работы систем акустической разведки на основе ВЧО – 140 МГц, а максимальная – 4 ГГц. Таким образом, с учетом вышеприведенных данных, средство обнаружения сигналов ВЧО может работать в диапазоне частот 140–4000 МГц. Анализ показывает, что минимальная мощность, которая требуется для нормальной работы систем акустической разведки, использующих ВЧО, – 10 мВт, при этом максимальное расстояние до закладки – до 10 м, а максимальная мощность передатчика может быть до 10 кВт. С учетом этого, требования к устройству обнаружения сигналов ВЧО могут быть следующими. Минимальная мощность определяется дальностью активации закладки и должна быть не менее 10 мВт. Так как требования санитарных норм и действующих ограничений на территории Российской Федерации к выходной мощности передатчика отсутствует, то она может быть не ограничена.

Требования к антенне закладного устройства: рабочий диапазон частот должен совпадать с требованиями к рабочему диапазону устройства или быть не хуже. Антенна должна быть всенаправленная, поскольку направление облучения неизвестно. По максимальной входной мощности ограничений нет, выходное сопротивление 50 Ом. Требований к полосе пропускания, полосе обзора и разрешению по частоте устройства обнаружения сигналов ВЧО не предъявляется, поскольку будут использоваться цифровые методы обработки сигналов. Требования к входному тракту устройства обнаружения: входное сопротивление 50 Ом, разъем должен быть совместим с разъемом антенны.

Система должна работать на основе технологии Software definition radio (SDR), то есть должна быть возможность программирования устройства, не вызывающая затруднений. При этом должен использоваться популярный язык программирования, например, C#. Для устройства должно быть руководство по программированию (Programming guide) или аналог. Устройство должно подключаться к средству вычислительной техники (или автоматизированной системе) при помощи широко распространенного интерфейса, например, USB или Ethernet. Общие требования к устройству: должно быть носимым, портативным; пригодным для работы в офисных условиях; масса не больше 5 кг; питание от сети, аккумулятора или средства вычислительной техники.

АНАЛИЗ ВОЗМОЖНЫХ СХЕМ ПОСТРОЕНИЯ

Некоторые из вариантов построения системы по технологии SDR описаны в [15; 16]. Суть Software definition radio заключается в том, что характеристики радиомодуля можно менять программным способом [17]. Например, в нашем случае целесообразно изменение рабочей частоты и вида модуляции. Это становится возможным за счет применения цифровых программируемых устройств на основе программируемых логических интегральных схем (ПЛИС), кристальных систем с возможностями программирования (SoC) микропроцессоров широкого применения (GPP) и цифровых сигнальных процессоров (ЦСП). В «идеальном» приемо-передатчике SDR аналого-цифровой преобразователь (АЦП) принимает аналоговый сигнал с антенны и преобразует его в цифровой вид. Далее, за счет цифровой обработки сигнала на выход устройства поступают преобразованные программным способом в удобный для человека вид данные. Особенностью данного варианта является ограничение диапазона частот, определяемое частотой дискретизации АЦП. Теорема Котельникова гласит, что она должна быть больше, чем удвоенная частота принимаемого сигнала.

Для преодоления этого противоречия можно дополнительно ввести между антенной и АЦП высокочастотный линейный тракт, обладающий дополнительным усилением и избирательными свойствами за счет смещения спектра принимаемого сигнала в более низкочастотную область.

Устройства, использующие технологию SDR, как правило, содержат аппаратную и программную части. Аппаратная состоит из физических устройств: антенн (широкополосных), радиочастотных конвертеров, ЦАП/АЦП. Программная часть служит для преобразования сигналов промежуточной частоты, их демодуляции с помощью программируемых микропроцессоров [18]. Универсальность SDR заключается в возможности ее перепрограммирования устройства. Причем, это является многократной функцией. Соответственно, возможно изменение и других характеристик – вида модуляции, стандарта отправляемых данных и т.д. Эта особенность SDR позволяет формировать цифровой сигнал с необходимыми характеристиками, и далее, преобразовывать его в аналоговый при помощи ЦАП [18; 19].

В отличие от аналогового приемного устройства, в котором велико влияние температурного режима на разброс параметров принимаемого и преобразуемого сигнала, имеются нелинейные искажения в широком диапазоне частот, технология SDR позволяет производить конвертацию сигнала напрямую из тракта промежуточной частоты. Схема SDR обладает следующими достоинствами:

1) температурный режим аппаратной части практически не влияет на характеристики обрабатываемых сигналов;
2) конфигурирование настроек отсутствует;
3) достаточно легкое исполнение переменных фильтров с затуханием более 80 дБ;
4) характеристики фазы и частоты внутреннего гетеродина могут меняться в широком диапазоне.

В схеме SDR присутствуют радиочастотный модуль (RF Section), состоящий из аналоговых компонентов, а также модуль промежуточной частоты (IF Section) и модуль обработки базовой полосы (Baseland Section), выполненные на цифровой компонентной базе.

ОБОСНОВАНИЕ СТРУКТУРНОЙ СХЕМЫ УСТРОЙСТВА

При проектировании системы защиты АРИ от утечки за счет ВЧО на основе SDR целесообразно использовать приемо-передатчик HackRF One.

Отметим преимущества SDR HackRF One, которые играют важную роль в устройстве обнаружения сигналов высокочастотного облучения.

1. Антенны являются распространенным источником слабых сигналов. Потери в линии «антенна – Analog Frontend» – снижают отношение принимаемого сигнала к шуму. Этих потерь в линии передачи можно избежать, разместив LNA (low noise amplifier) после антенны. Он обеспечивает достаточное усиление, чтобы компенсировать потери.
2. В радиочастотном тракте осуществляется перенос радиосигнала в область более низких частот. Встроенный генератор, сигнал которого подается на смеситель, управляется программным способом и точность установки частоты намного лучше, чем в аналоговых радиосистемах.
3. В радиочастотном тракте для подавления помеховых сигналов присутствуют так называемые фильтры «основной полосы» с частотой среза 1,75–28 МГц, которые также управляются программный способом. Параметры данных фильтров намного точнее определяются, чем у аналоговых фильтров.
4. Микроконтроллер и ПЛИС позволяют подключать SDR HackRF One к автоматизированной системе (АС) или средству вычислительной техники (СВТ) через USB интерфейс и управлять рабочими параметрами устройства программным способом, а также принимать и передавать данные между АС (или СВТ) и SDR HackRF One. Поэтому возможна непосредственная цифровая обработка сигналов (ЦОС) на АС или СВТ, что значительно облегчает процесс обнаружения сигналов ВЧО.
5. Стоимость SDR HackRF One, без дополнительных комплектующих, составляет до десяти тысяч рублей, что сравнительно с контрольно-измерительным оборудованием и средствами защиты акустической информации от утечки за счет ВЧО, и является недорогим решением.

Именно эти преимущества послужили причиной выбора SDR технологии для использования при разработке устройства обнаружения сигналов ВЧО.

ЭКСПЕРИМЕНТАЛЬНЫЙ ЛАБОРАТОРНЫЙ СТЕНД

Собран экспериментальный лабораторный стенд, который отображен на рис. 1. В его состав входят: лабораторный ноутбук с развернутым на нем специальным разработанным лично программным обеспечением, SDR HackRF One, высокочастотный генератор SMB 100A, направленная антенна, закрытая в радиопрозрачном материале.

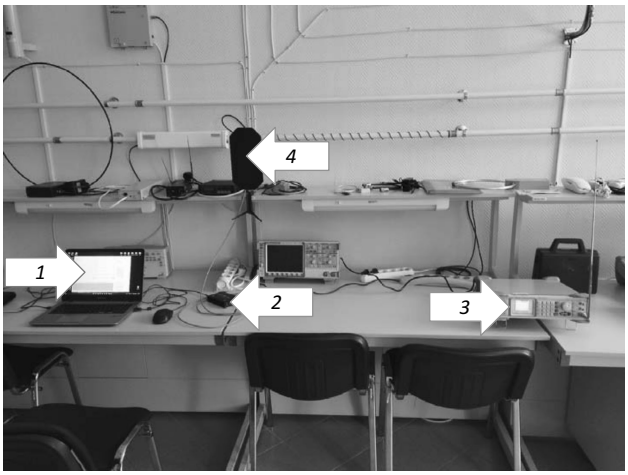

Рис. 1. Экспериментальный стенд для поиска сигналов ВЧО при помощи SDR HackRF One:

1 – ноутбук со специальным программным обеспечением; *2* – SDR HackRF One; *3* – ВЧ-генератор SMB 100A; *4* – направленная антенна

Fig. 1. Experimental stand for searching for HFI signals using SDR HackRF One:

1 – laptop with special software; *2* – SDR HackRF One; *3* – RF generator SMB 100A; *4* – directional antenna

Проведены экспериментальные исследования по обнаружению гармонических сигналов различной частоты (0,35, 0,5, 1, 3,2 ГГц) и мощностью +20 дБм (100 мВт). Виды экрана настройки высокочастотного генератора SMB 100A, а также результатов обработки и отображения принятого сигнала при помощи разработанного программного обеспечения, развернутого на ноутбуке, для HackRF One на частоте 1 ГГц отображены на рис. 2 и 3 соответственно.

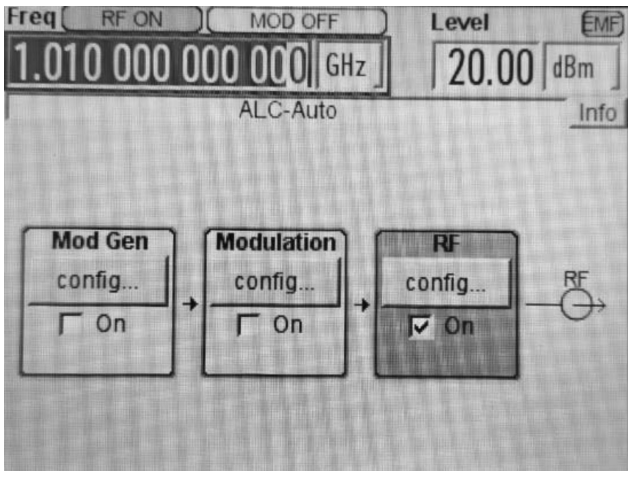

Рис. 2. Вид экрана настройки высокочастотного генератора SMB 100A

Fig. 2. Screen view of setting the high-frequency generator SMB 100A

Рис. 3. Вид экрана – результаты обработки и отображения принятого сигнала при помощи разработанного ПО для HackRF One на частоте 1 ГГц

Fig. 3. Screen view – the results of processing and displaying the received signal using developed software for HackRF One at 1 GHz

Таким образом, созданный экспериментальный лабораторный стенд показал свою работоспособность и готов к проведению исследований методов и способов обнаружения каналов утечки за счет ВЧО.

Дальнейшим этапом является разработка макета программно-аппаратного средства и соответствующего программного обеспечения для подавления приемных устройств аппаратуры высокочастотного облучения на базе SDR-приемо-передатчика.

ВЫВОДЫ

На основе системного анализа по теме исследования обоснованы требования к средству обнаружения сигналов высокочастотного облучения. Рассмотрение различных вариантов построения устройств данного типа показали, что именно SDR-технология лучше всего подходит для разработки данного средства. Разработанное программное обеспечение к SDR HackRF One, собранный экспериментальный лабораторный стенд и проведенные экспериментальные исследования показали перспективность и возможность использования SDR-технологии для разработки методов и средств защиты АРИ от утечки за счет ВЧО на основе программно-аппаратного средства и соответствующего программного обеспечения для подавления приемных устройств аппаратуры высокочастотного облучения на базе SDR-приемо-передатчика.

Литература

1. *Magomedov Sh.G.* Assessment of the degree of influence of related factors on information security indicators // Russian Technological Journal. 2017. No. 5 (2). Pp. 47–56. URL: https://doi.org/10.32362/2500-316X-2017-5-2-47-56
2. *Porsev I.S., Melshiyan M.A., Dushkin A.V.* Analysis and control of the effectiveness of information protection against leakage through technical channels based on probabilistic assessment // Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). 2022. Pp. 398–401. DOI: 10.1109/ElConRus54750.2022.9755623.

References

1. *Magomedov Sh.G.* Assessment of the degree of influence of related factors on information security indicators. *Russian Technological Journal*. 2017. No. 5 (2). Pp. 47–56. URL: https://doi.org/10.32362/2500-316X-2017-5-2-47-56
2. *Porsev I.S., Melshiyan M.A., Dushkin A.V.* Analysis and control of the effectiveness of information protection against leakage through technical channels based on probabilistic assessment. *Conference of Russian Young Researchers in Electrical and Electronic Engineering* (*ElConRus*). 2022. Pp. 398–401. DOI: 10.1109/ElConRus54750.2022.9755623.

3. *Goncharov N., Dushkin A., Goncharov I.* Mathematical modeling of the security management process of an information system in conditions of unauthorized external influences // 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA), 20–22.11.2019. Lipetsk, Russia. IEEE. 2020. Pp. 77–82. DOI: 10.1109/SUMMA48161.2019.8947513.
4. *Noev A., Dushkin A., Sumin V.* Mathematical model for managing the dynamics of the development of information conflict in information systems // 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA), 20–22.11.2019. Lipetsk, Russia. IEEE. 2020. Pp. 88–93. DOI: 10.1109/SUMMA48161.2019.8947546.
5. *Исаев О.В., Гречушкина А.Ю., Душкин А.В., Зольников В.К.* и др. Анализ устойчивости функционирования информационной структуры интегрированной системы безопасности в условиях негативных воздействий // Промышленные АСУ и контроллеры. 2017. № 10. С. 52–60.
6. *Касаткина Т.И., Россихина Л.В., Душкин А.В.* и др. Применение технологии нейронных сетей в подсистеме безопасности информационных систем // Приборы и системы. Управление, контроль, диагностика. 2019. № 6. С. 31–38.
7. *Лысов А.В.* Электромагнитное зондирование акустически возбужденных объектов (радиолокационные системы акустической разведки). СПб.: Медиа-папир, 2020. 678 с.
8. The Thing. The Great Seal Bug // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/thing/index.htm (data of accesses: 21.10.2022).
9. SRT-56 // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/ec/srt56/index.htm (data of accesses: 21.10.2022).
10. EASYCHAIR // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/ec/ (data of accesses: 21.10.2022).
11. LOUDAUTO // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/nsaant/loudauto/index.htm (data of accesses: 21.10.2022).
12. SATYR // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/satyr/index.htm (data of accesses: 21.10.2022).
13. SRT-52 // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/ec/srt52/index.htm (data of accesses: 21.10.2022).
14. Pulsed Cavity. Resonant cavity microphone // Crypto Museum. URL: https://www.cryptomuseum.com/covert/bugs/ec/cavity/index.htm (data of accesses: 21.10.2022).
15. *Громов Ю.Ю., Шатских В.В., Провоторов А.А.* и др. Программа для радиомониторинга и идентификации радиосигналов «SDRPRO». Свидетельство о регистрации программы для ЭВМ № 2022612861, 01.03.2022. Заявка № 2022611806 от 10.02.2022.
16. *Семенюк А.В., Сычев И.В., Алферов Ю.В.* и др. Обеспечение информационной безопасности через анализ радиоэлектронной обстановки беспилотного летательного аппарата с помощью программного обеспечения SDR-приемника: тр. междунар. симпозиума «Надежность и качество». 2020. Т. 1. С. 104–108.
17. *Ефремова А.Е., Паращинец А.В., Мелихов С.В.* Программно-определяемая радиосистема (Software-defined radio, SDR). Принцип разработки высокочастотного линейного тракта // Апробация. 2019. № 12 (39). С. 27–30.
18. *Рябов И.В., Толмачев С.В., Лебедева А.А.* Принципы программно-определяемых радиосистем и их применение в рамках задачи исследования метеорной радиосвязи //

3. *Goncharov N., Dushkin A., Goncharov I.* Mathematical modeling of the security management process of an information system in conditions of unauthorized external influences. *1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency* (*SUMMA*), *20–22.11.2019. Lipetsk, Russia. IEEE*. 2020. Pp. 77–82. DOI: 10.1109/SUMMA48161.2019.8947513.
4. *Noev A., Dushkin A., Sumin V.* Mathematical model for managing the dynamics of the development of information conflict in information systems. *1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency* (*SUMMA*), *20–22.11.2019. Lipetsk, Russia. IEEE*. 2020. Pp. 88–93. DOI: 10.1109/SUMMA48161.2019.8947546.
5. *Isaev O.V., Grechushkina A.Yu., Dushkin A.V., Zolnikov V.K.* et al. Analysis of the sustainability of the functioning of the information structure of the integrated security system under negative impacts. *Industrial ACS and Controllers*. 2017. No. 10. Pp. 52–60. (In Rus.)
6. *Kasatkina T.I., Rossikhina L.V., Dushkin A.V.* et al. Application of neural networks technology in the security subsystem of information systems. *Devices and Systems. Management, Control, Diagnostics*. 2019. No. 6. Pp. 31–38. (In Rus.)
7. *Lysov A.V.* Electromagnetic sounding of acoustically excited objects (radar systems of acoustic reconnaissance). St. Petersburg: Media Paper, 2020. 678 p.
8. The Thing. The Great Seal Bug. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/thing/index.htm (data of accesses: 21.10.2022).
9. SRT-56. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/ec/srt56/index.htm (data of accesses: 21.10.2022).
10. EASYCHAIR. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/ec/ (data of accesses: 21.10.2022).
11. LOUDAUTO. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/nsaant/loudauto/index.htm (data of accesses: 21.10.2022).
12. SATYR. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/satyr/index.htm (data of accesses: 21.10.2022).
13. SRT-52. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/ec/srt52/index.htm (data of accesses: 21.10.2022).
14. Pulsed Cavity. Resonant cavity microphone. *Crypto Museum*. URL: https://www.cryptomuseum.com/covert/bugs/ec/cavity/index.htm (data of accesses: 21.10.2022).
15. *Gromov Yu.Yu., Shatskikh V.V., Provotorov A.A.* et al. Program for radio monitoring and identification of radio signals "SDRPRO". Certificate of registration of the computer program No. 2022612861, 03.01.2022. Application No. 2022611806 10.02.2022.
16. *Semenyuk A.V., Sychev I.V., Alferov Yu.V.* et al. Ensuring information security through the analysis of the electronic environment of an unmanned aerial vehicle using the software of the SDR receiver. *Proceedings of the International Symposium "Reliability and Quality"*. 2020. Vol. 1. Pp. 104–108.
17. *Efremova A.E., Parashchinets A.V., Melikhov S.V.* Software-defined radio (Software-defined radio, SDR). The principle of developing a high-frequency linear path. *Approbation*. 2019. No. 12 (39). Pp. 27–30. (In Rus.)
18. *Ryabov I.V., Tolmachev S.V., Lebedeva A.A.* Principles of software-defined radio systems and their application in the framework of the problem of studying meteor radio

Современные наукоемкие технологии. 2019. № 7-1. С. 59–66.

19. *Руднев А.Н.* Повышение помехоустойчивости системы с прямым расширением спектра с модифицированной ФМ-4 со сдвигом // Промышленные АСУ и контроллеры. 2022. № 1. С. 8–11.
20. *Kulikov G.V.*, *Do Ch.*, *Samokhina E.V.* Optimal nonlinear filtering of M-PM signals against the background of harmonic interference with a random initial phase // Russian Technological Journal. 2021. No. 9 (6). Pp. 46–56. URL: https://doi.org/10.32362/2500-316X-2021-9-6-46-56.

communications. *Modern Science-intensive Technologies*. 2019. No. 7-1. Pp. 59–66. (In Rus.)

19. *Rudnev A.N.* Improving the noise immunity of a direct spread spectrum system with a modified FM-4 with a shift. *Industrial ACS and Controllers*. 2022. No. 1. Pp. 8–11. (In Rus.) DOI: 10.25791/asu.1.2022.1337.
20. *Kulikov G.V.*, *Do Ch.*, *Samokhina E.V.* Optimal nonlinear filtering of M-PM signals against the background of harmonic interference with a random initial phase. *Russian Technological Journal*. 2021. No. 9 (6). Pp. 46–56. URL: https://doi.org/10.32362/2500-316X-2021-9-6-46-56.

Статья проверена программой Антиплагиат. Оригинальность – 92,76%

Р е ц е н з е н т: *Хорев А.А.*, доктор технических наук, профессор; заведующий кафедрой «Информационная безопасность» Национального исследовательского университета «Московский институт электронной техники»

Статья поступила в редакцию 30.10.2022, принята к публикации 09.12.2022
The article was received on 30.10.2022, accepted for publication 09.12.2022

СВЕДЕНИЯ ОБ АВТОРАХ

Порхун Анатолий Сергеевич, аспирант; инженер по защите информации кафедры «Информационная безопасность» Национального исследовательского университета «Московский институт электронной техники». Москва, Зеленоград, Российская Федерация. E-mail: tolik.porkhun@mail.ru

Душкин Александр Викторович, доктор технических наук, доцент; профессор кафедры «Информационная безопасность» Национального исследовательского университета «Московский институт электронной техники». Москва, Зеленоград, Российская Федерация; профессор кафедры КБ-3 «Безопасность программных решений», МИРЭА – Российский технологический университет. Москва, Российская Федерация. SPIN: 9285-2678; ORCID: 0000-0002-8078-8971; E-mail: a_dushkin@mail.ru

Мещеряков Роман Валерьевич, доктор технических наук, профессор; заведующий лабораторией Института проблем управления им. В.А. Трапезникова Российской академии наук. Москва, Российская Федерация. SPIN: 7783-0247; E-mail: meshcheryakov.roman@gmail.com

Савченко Юрий Васильевич, доктор технических наук, профессор; профессор Института микроприборов и систем управления им. Л.Н. Преснухина Национального исследовательского университета «Московский институт электронной техники». Москва, Зеленоград, Российская Федерация. Author ID: 524376; E-mail: a_dushkin@mail.ru

Щербаков Виталий Алексеевич, доктор технических наук, доцент; профессор кафедры «Информационная безопасность» Национального исследовательского университета «Московский институт электронной техники». Москва, Зеленоград, Российская Федерация. E-mail: svasvarog@yandex.ru

ABOUT THE AUTHORS

Anatoly S. Porkhun, postgraduate student; engineer of information security at the Department of Information Security of the National Research University of Electronic Technology. Moscow, Zelenograd, Russian Federation. E-mail: tolik.porkhun@mail.ru

Alexander V. Dushkin, Dr. Sci. (Eng.), Associate Professor; Professor at the Department of Information Security of the National Research University of Electronic Technology. Moscow, Zelenograd, Russian Federation; Professor at the Department KB-3 «Security of Software Solutions», MIREA – Russian Technological University. Moscow, Russian Federation. SPIN: 9285-2678; ORCID: 0000-0002-8078-8971; E-mail: a_dushkin@mail.ru

Roman V. Meshcheryakov, Dr. Sci. (Eng.), Professor; Head of the Laboratory of the Institute of Control Problems named after V.A. Trapeznikov RAS. Moscow, Russian Federation. SPIN: 7783-0247; E-mail: meshcheryakov.roman@gmail.com

Yury V. Savchenko, Dr. Sci. (Eng.), Professor; Professor at the Institute of Microdevices and Control Systems named after L.N. Presnukhina of the National Research University of Electronic Technology. Moscow, Zelenograd, Russian Federation. Author ID: 524376; E-mail: a_dushkin@mail.ru

Vitaly A. Shcherbakov, Dr. Sci. (Eng.), Associate Professor; Professor at the Department of Information Security of the National Research University of Electronic Technology. Moscow, Zelenograd, Russian Federation. E-mail: svasvarog@yandex.ru