СКРЫТЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ: АНАЛИЗ ДЕЙСТВУЮЩЕЙ НОРМАТИВНО- МЕТОДИЧЕСКОЙ БАЗЫ, ТЕРМИНОЛОГИЯ

В статье проведен анализ результатов научных исследований скрытых технических каналов утечки информации (СТКУИ, здесь под СТКУИ авторы предложили понимать технические каналы утечки информации (ТКУИ), мер противодействия, которые не предусмотрены действующими нормативными документами в области ТЗИ). Например, ТКУИ, создаваемые линиями электропередач, в которых зависимость потребления электроэнергии от времени определяется нагрузкой центральных процессоров (CPU) средств вычислительной техники (СВТ), управляемых предустановленной специальной программой; акустический ультразвуковой ТКУИ, образованный пассивными колонками и наушниками без использования микрофона; низкочастотные магнитные колебания, возникающие при работе CPU СВТ; радиоизлучение, сопровождающее в процесс ввода информации на смартфоне, которое регистрируется и анализируется на смартфоне нарушителя с помощью FM-тюнера; вариаций теплового излучения корпуса СВТ; акустического излучения, генерируемого дисковыми накопителями в процессе записи и считывания информации; электромагнитного излучения, возникающего в процессе обращения к различным устройствам через порт USB; оптического излучения светодиодных индикаторов СВТ и т.д.

Результаты проведенного анализа свидетельствуют о наличии реальных угроз несанкционированного доступа к информации, обрабатываемой в СВТ, через СТКУИ, а также необходимости проведения целенаправленных исследований данных ТКУИ и дальнейшего совершенствования нормативно-методической базы в области ТЗИ.

В данной статье проведен анализ действующей российской и зарубежной нормативно-методической базы в области технической защиты информации (ТЗИ), науч-

ных публикаций в данной области и обосновано целесообразность дополнения традиционно используемых в области технической защиты информации понятий «технический канал утечки информации (ТКУИ)», «скрытый канал» утечки информации понятием «скрытый технический канал утечки информации (СТКУИ)». Дано определение понятия СТКУИ, а также предложены его структурная схема и классификация СТКУИ.

Ключевые слова: скрытый технический канал утечки информации, средство вычислительной техники, вредоносное программное обеспечение.

Porshnev S.V., Belyaev D.O.

HIDDEN TECHNICAL CHANNELS OF INFORMATION LEAKAGE DEVELOPED IN COMPUTER EQUIPMENT: ANALYSIS OF THE REGULATORY AND METHODOLOGICAL FRAMEWORK, TERMINOLOGY

In article, an analysis of the results of scientific research of hidden technical channels of information leakage is carried out (here, under the hidden technical channels of information leakage, the authors proposed to understand technical channels of information leakage, measures to counteract which are not provided for by current regulatory documents in the field of technical information protection). For example, technical channels of information leakage created by power lines, in which the dependence of electricity consumption on time is determined by the load of central processing units (CPUs) of computer equipment controlled by a pre-installed special program; acoustic ultrasonic technical channel of information leakage formed by passive speakers and headphones without the use of a microphone; low-frequency magnetic vibrations that occur during the operation of the cpu of the computer equipment; radio radiation that accompanies the process of entering information on a smartphone, which is recorded and analyzed on the intruder's smartphone using an fm tuner; variations in thermal radiation of the computer equipment body; acoustic radiation generated by disk drives in the process of recording and reading information; electromagnetic radiation that occurs during access to various devices via the USB port; optical radiation of LED indicators of computer equipment, etc.

The results of the analysis indicate the presence of real threats unauthorized access to information processed at the computer device, using a hidden technical channels of information leakage and the need for targeted research of the data leakage channels and further improvement of normative-methodical base in the field of technical protection of information.

This article analyzes the current Russian and foreign regulatory and methodological framework in the field of technical information protection, scientific publications in this field and justifies the expediency of supplementing the traditionally used in the field of technical information

protection concepts of “technical channel of information leakage”, “hidden channel” of information leakage with the concept of “hidden technical channel of information leakage”. The definition of the concept of a hidden technical channel of information leakage is given, as well as its structural scheme and classification of hidden technical channels of information leakage are proposed.

Keywords: *hidden technical channel of information leakage, computer hardware, malicious software.*

Введение

Техническим каналом утечки информации (ТКУИ) называется совокупность источников информации (передатчик – объект разведки), линия связи (протяженная физическая среда), по которой распространяется информационный сигнал (собственно, канал передачи), а также средство приёма (перехвата) информации [1, 2]. Понятие «ТКУИ» оказывается неразрывно связанным с понятием «фактор, воздействующий на информацию» – «явление, действие или процесс, результатом которых являются утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней» [3]. Печень объективных и субъективных факторов (внутренних и внешних), воздействующих на защищаемую информацию, обрабатываемую средствами вычислительной техники, которые непосредственно формируют ТКУИ выделен в [4].

Отметим, что в отечественной нормативно-методической базе обеспечения информационной безопасности (в части, защиты информации, обрабатываемой с использованием средств вычислительной техники, от утечки по техническим каналам) особое внимание уделено рассмотрению источников угроз безопасности информации и технических каналов утечки, формируемым ввиду наличия факторов таких факторов, как побочные электромагнитные излучения, наводки, наличие акустоэлектрических преобразователей в элементах технических средств [устройств] обработки и передачи информации, а также доступ к защищаемой информации с применением технических средств, съема информации, несанкционированный доступ к защищаемой информации (см., например, [5]).

Однако оказывается, что также существуют ТКУИ, наличие которых обусловлено факторами, не входящими в приведенный выше перечень (например, акустические эманации, возникающие при отображении визуаль-

ной информации на экране, параметры которых определяются законом формирования изображения [6] и др.), и которые для краткости будем называть далее «скрытыми техническими каналами утечки информации» (СТКУИ). (Обоснование определения данного термина будет дано ниже.)

Обзор современного состояния открытых зарубежных научных исследований СТКУИ, проведенный авторами данной статьи [7], позволил сделать обоснованный вывод о высокой активности зарубежных ученых в исследованиях СТКУИ, в которых для получения доступа к информации, обрабатываемой средствами вычислительной техники, используются физические поля различной природы, а также о необходимости разработки соответствующей нормативно-правовой и методической базы по противодействию данным СТКУИ, в которой должно быть определено понятие СТКУИ.

В статье дано обоснование определения понятия СТКУИ, предложены его структурная схема и классификация СТКУИ.

Обоснование определения понятия «скрытый технический канал утечки информации»

Впервые понятие «скрытый канал» (covert channels) было введено в научный оборот в 1973 г. Батлером Лэмпсоном [8], под которым автор предложил понимать канал связи (коммуникационный канал), изначально не предназначенный для передачи информации, нарушающий установленную политику безопасности информации.

В соответствие с [9] «скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности информации. В соответствие с ГОСТ Р 53113.1-2008 п. 6.1 угрозы безопасности, которые могут быть реализованы с помощью скрытых каналов, включают в себя:

- внедрение вредоносных программ и данных;
- подачу злоумышленником команд агенту для выполнения;
- утечку криптографических ключей или паролей;
- утечку отдельных информационных объектов.

Понятие «скрытый канал» также используется для систематизации угроз безопасности информации. Например, в банке данных угроз безопасности ФСТЭК России присутствуют следующие угрозы безопасности информации: «УБИ.111: Угроза передачи данных по скрытым каналам» [10], «УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации» [11], непосредственно связанные с рассматриваемым понятием.

Отметим, что в [12] указано, что «скрытые каналы используются для систематического взаимодействия вредоносных программ (компьютерных вирусов) с нарушителем безопасности при организации атаки на автоматизированные системы, которая не обнаруживается средствами контроля и защиты». Аналогичный алгоритм взаимодействия с потенциальным злоумышленником реализуется посредством разработки и использования вредоносного программного обеспечения формирования скрытого технического канала утечки информации [13]. Отметим, что с обсуждаемой технологией связано понятие «advanced persistent threat» (APT) – «развитая устойчивая угроза», для которой характерно установление и расширение перечня изделий и технологий злоумышленника внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений нарушения политики безопасности информационной системы. Однако этот сценарий извлечения интересующей злоумышленника информации является частным случаем СТКУИ.

К несомненным достоинствам стандартов [9, 12] следует отнести: введение в постановку задачи обеспечения безопасности информации понятия «скрытый канал»; классификацию и систематизацию скрытых каналов; введение требований анализа защищенности информации от утечки по данным каналам и выработки адекватных мер защиты. Также отметим, что в стандартах [9, 12] определена важная особенность скрытого канала, состоящая в невозможности его идентификации

применяемыми средствами контроля и средствами защиты информации, а также нейтрализации утечки и последствий этой утечки. В тоже время в них не дано определения термина «скрытый ТКUI». При этом, очевидно, что понятие «скрытый канал» можно использовать не только применительно к атакам, реализуемым путем несанкционированного доступа в информационную систему и использования вредоносного программного обеспечения для нарушения конфиденциальности, целостности и доступности информации, но и к явлениям, связанным с формированием технических каналов утечки информации, однако данный факт упущен разработчиками стандартов [9, 12].

Анализ зарубежной нормативно-методической базы позволяет сделать вывод о том, что в ней не дается определения понятия «скрытый ТКUI». В тоже время в некоторых зарубежных стандартах по информационной безопасности используется понятие «скрытый канал» (англ. «covert channel»), связанное с нарушениями принятой в организации политики безопасности режимов обработки, хранения и передачи информации с использованием систем информационных технологий и автоматизированных систем, то есть исключительно в задаче обеспечения программно-аппаратной защиты информации.

Например, в стандарте [14], разработанном Национальным центром компьютерной безопасности США в соответствии с директивой 52 51 1 и утвержденном в ноябре 1993 г., определяется понятие «скрытый канал» и описаны некоторые механизмы анализа скрытых каналов. В разделе 2.1 обсуждаемого стандарта приводится четыре определения термина «скрытый канал»:

1. Канал связи является скрытым, если он вообще не предназначен для передачи информации.

2. Канал связи является скрытым (напрямую, косвенным), если он основан на передаче переменных, описывающих ресурсные состояния».

3. Скрытые каналы «определены как такие каналы, которые существуют вследствие реализации политики распределения ресурсов и управления ресурсами.

4. Скрытые каналы – это те каналы, которые «используют объекты, обычно не рассматриваемые как объекты данных, для передачи информации от одного субъекта другому».

С точки зрения целей нашего исследования, наиболее близкими понятию «скрытый технический канал утечки информации» оказываются определения 1 и 4.

В стандарте [14] скрытые каналы классифицируются на:

1. Каналы хранения и синхронизации данных.

2. Зашумленные и незашумленные каналы (канал считается незашумленным, если символы, передаваемые отправителем, совпадают с символами, принимаемыми получателем с вероятностью, равной 1; каналы считаются зашумленными в случае, когда биты, передаваемые отправителем, не могут быть приняты правильно с вероятностью, равной 1, если не используются соответствующие коды исправления ошибок).

3. Агрегированные и неагрегированные каналы (несколько переменных данных, которые могут быть независимо друг от друга использованы для формирования скрытых каналов, могут быть использованы в качестве группы для амортизации затрат на синхронизацию (и, возможно, декодирование) информации. Таким образом, результирующие каналы агрегируются. Каналы могут агрегироваться последовательно, параллельно или в комбинациях последовательного и параллельного агрегирования для получения оптимальной (максимальной) полосы пропускания).

Методами идентификации скрытых каналов, согласно стандарту [14], являются:

1. Синтаксический анализ информационных потоков.

2. Добавление семантических компонентов к анализу информационных потоков.

3. Метод матрицы общих ресурсов (SRM).

4. Метод «невмешательства» (анализ информационных потоков производится с использованием модели информационной системы).

Таким образом, скрытые технические каналы утечки информации, возникающие в процессе функционирования средств вычислительной техники, не рассматриваются стандартом [14].

Среди зарубежных стандартов также отметим стандарт [15] и его обновленную версию [16], известные под аббревиатурами FIPS 140-2 и FIPS 140-3, при этом последний стандарт базируется на стандартах ISO/IEC 19790:2012 и ISO/IEC 24759:2017. Стандарты FIPS 140-2 и FIPS 140-3 относятся к стандартам

компьютерной безопасности правительства США, определяющим требования к криптографическим модулям.

Разделы 4.11 стандарта FIPS 140-2, 7.12 стандарта ISO/IEC 19790:2012 и 6.12 стандарта /IEC 24759:2017 (на последних двух стандартах базируется FIPS 140-3), посвящены смягчению последствий других атак на криптографические системы, среди которых выделены:

1. Атаки, основанные на анализе энергопотребления.

2. Атаки по времени (атака по сторонним каналам, в которой атакующий пытается скомпрометировать криптосистему с помощью анализа времени, затрачиваемого на исполнение криптографических алгоритмов).

3. Атаки, использующие ошибки вычислений.

4. Атаки, использующие побочные электромагнитные излучения.

В [17] в дополнение к указанным видам атак авторами предлагается атака с использованием скрытого акустического канала, наряду с побочным электромагнитным излучением сопровождающего функционирование аппаратных средств криптографического преобразования и атака с использованием скрытого канала в оптическом диапазоне электромагнитных волн. Таким образом, в зарубежной нормативно-методической базе и научно-исследовательских трудах встречается также термин, схожий с понятием «скрытый канал» – «side-channel attacks» (атаки по сторонним (или побочным) каналам), который может быть употреблен в контексте проблематики исследования скрытых технических каналов утечки информации.

Отметим, что термин «side-channel attacks» в [17] употребляется исключительно в контексте криптоанализа, исключающего математический анализ шифрующего алгоритма. В качестве примера можно привести идентифицированную уязвимость CVE-2013-4576 из базы данных общеизвестных уязвимостей информационной безопасности [18], обнаруженную в программном обеспечении для шифрования информации и создания электронных подписей GnuPG 1.x и позволяющую осуществить операцию акустического криптоанализа во время дешифрования.

Таким образом, в зарубежной, также как и в отечественной нормативно-правовой базах отсутствуют определения понятия «скрытый ТКУИ».

В этой связи дадим собственное определение понятия «скрытый ТКUI», принимая при этом во внимание выше изложенное: под скрытым техническим каналом утечки информации, обрабатываемой средствами вычислительной техники, следует понимать паразитный (побочный, вторичный) по отношению к основному (блокированному) техническому каналу утечки информации путь несанкционированного распространения информативного сигнала, представляющий собой совокупность управляемого или неуправляемого злоумышленником источника информации, формирующего информативный сигнал, физической среды распространения этого сигнала, по своей природе происхождения отличной от природы происхождения среды распространения сигнала основного канала утечки, и средства приёма (перехвата) сигнала, управляемого злоумышленником.

Структурная схема СТКУИ, соответствующая данному автором определению, приведена на рисунке 1.2.

Рис.1. Структурная схема скрытого технического канала утечки информации: 1 – источник информации; 2 – источник информативного сигнала; 2' – источник сигнала в источнике 2, формирующий паразитный (вторичный, побочный) информативный сигнал, не анализируемый в ходе общепринятой методологии защиты информации от утечки по техническим каналам при ее обработке с использованием СВТ; 3 – техническое средство защиты информации (пассивное, активное); 4 – среда распространения информативного сигнала от источника 2'; 5 – техническое средства приёма (перехвата) сигнала от источника 2'; 6 – несанкционированный получатель (злоумышленник); 7 – помехи (физическая природа помех совпадает с физической природой сигнала от источника 2')

Из рисунка 1 видно, что СТКУИ обеспечивает для потенциального злоумышленника возможность дистанционно управлять (в частности, программно) как источником сигнала 2' (в том числе и через среду распространения источника 2') с целью преднамеренного формирования сигнала и извлечения из его параметров информативной составляющей, так и средой распространения с целью воздействия на источник сигнала и

обрабатываемые им информационные ресурсы.

В качестве примера СТКУИ, реализованного по схеме, приведенной на рисунке 1, можно привести СТКУИ, описанный в [13]. Здесь специалистами центра кибербезопасности из Университета им. Бен-Гуриона в Негеве (г. Беэр-Шева, Израиль) были исследованы побочные акустические излучения, формируемые накопителями на жестких магнитных дисках (НЖМД) во время процессов поиска, чтения и записи информации и существующие параллельно с побочными электромагнитными излучениями НЖМД, измерение которых регламентируется действующей нормативно-правовой базой в области ТЗИ. Результаты проведенных исследований показали, что законы изменения параметров акустических сигналов определяются особенностями механизмов операций поиска, чтения и записи информации на НЖМД. Для управления акустическими сигналами, генерируемыми НЖМД, авторы разработали программное обеспечение «DiskFiltration», устанавливаемое на скомпрометированном средстве вычислительной техники, которое обеспечивало за счет программного управления движением рычага привода жесткого диска генерацию модулированного информационным сигналом акустического излучения на выбранных звуковых частотах. Генерируемое акустическое излучение перехватывается ближайшим приёмником (например, смартфоном, умными часами, ноутбуком и т. д.) с предустановленным программным обеспечением, позволяющим извлечь информативную составляющую из принятого сигнала. Также программа «DiskFiltration» обеспечивает изменения значения отношения «сигнал/шум» на стороне злоумышленника с помощью реализованного на передающей стороне алгоритма изменения параметров шумоподавления и увеличения интенсивности информативного акустического излучения с параметрами, не позволяющими идентифицировать нестандартное поведение НЖМД) с целью оптимального приёма и дальнейшего анализа.

Классификация СТКУИ

Основываясь на введенном определении понятия СТКУИ, а также обзоре результатов исследований скрытых технических каналов утечки информации, обрабатываемой средствами вычислительной техники [7] мы предлагаем следующую классификацию данных каналов, представленную на рисунке 2.

Рис. 2. Классификация скрытых технических каналов утечки информации

Из рисунка 2 видно, что многообразие скрытых ТКUI ввиду их неочевидности и потенциальной опасности ставит перед специалистами по обеспечению информационной безопасности нетривиальные задачи по выработке оптимальной методологии поиска СТКУИ, анализа защищенности информации от утечки по данным каналам и предложению оптимальных способов и средств защиты.

Заключение

На основе проведенного анализа определений понятия «скрытый канал» в отечественной и зарубежной нормативно-правовой базе обоснована необходимость определения понятия «скрытый технический канал утечки информации» и дано его определение, а также предложена соответствующая классификация СТКУИ.

Литература

1. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. – М.: Горячая линия-Телеком, 2015.
2. Зайцев, А. П. Технические средства и методы защиты информации. Учебник для вузов – 7-е изд., испр. / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая Линия–Телеком, 2018.
3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
4. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
5. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 30 августа 2002 г.
6. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: <https://ieeexplore.ieee.org/abstract/document/8835386> – (дата обращения: 15.10.2019).
7. Поршнев, С.В., Беляев, Д.О. Обзор результатов исследований скрытых технических каналов утечки информации, обрабатываемой средствами вычислительной техники. 2020, В: Вестник УрФО. Безопасность в информационной сфере.
8. Lampson, B. W.A Note on the Confinement Problem A Note on the Confinement Problem, Communications of the ACM, 16, 10 (Oct. 1973), pp 613-615.
9. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

10. Банк данных угроз безопасности информации. – URL: <https://bdu.fstec.ru/ubi/threat/view/id/526> – (дата обращения: 25.07.2020).
11. Банк данных угроз безопасности информации. – URL: <https://bdu.fstec.ru/ubi/threat/view/id/530> – (дата обращения: 25.07.2020).
12. ГОСТ Р 53113.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.
13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: <https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf> – (дата обращения: 27.03.2020).
14. A Guide to Understanding Covert Channel Analysis of Trusted Systems, National Computer Security Center. NCSC-TG-030. - Ver. 1, 1993 – URL: <https://fas.org/irp/nsa/rainbow/tg030.htm> – (дата обращения: 10.07.2020).
15. Federal Information Processing Standard Publication 140-2 – URL: <https://csrc.nist.gov/publications/fips/140/2/final> – (дата обращения: 15.06.2020).
16. Federal Information Processing Standard Publication 140-3 – URL: <https://csrc.nist.gov/publications/fips/140/3/final> – (дата обращения: 15.06.2020).
17. Yong Bin Zhou, Deng Guo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China, 2006. – URL: <http://eprint.iacr.org/2005/388.pdf> – (дата обращения: 15.06.2020).
18. Common Vulnerabilities and Exposures. – URL: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4576> – (дата обращения: 12.06.2020).

References

1. Buzov, G. A. Zashchita informacii ogranichenogo dostupa ot utechki po tekhnicheskim kanalom: Spravochnoe posobie / Buzov G.A. – М.: Goryachaya liniya-Telekom, 2015.
2. Zajcev, A. P. Tekhnicheskie sredstva i metody zashchity informacii. Uchebnik dlya vuzov – 7-e izd., ispr. / A.P. Zajcev, R.V. Meshcheryakov, A.A. Shelupanov. – М.: Goryachaya Liniya-Telekom, 2018.
3. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i opredeleniya.
4. OST R 51275-2006. Zashchita informacii. Ob'ekt informatizacii. Faktory, vozdeystvuyushchie na informaciyu. Obshchie polozheniya.
5. Special'nye trebovaniya i rekomendacii po tekhnicheskoy zashchite konfidencial'noj informacii. Utverzhdeny prikazom Gostekhkomissii Rossii ot 30 avgusta 2002 g.
6. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels. 2019 IEEE Symposium on Security and Privacy (SP), 2019. P. 853-869. – URL: <https://ieeexplore.ieee.org/abstract/document/8835386> – (дата обращения: 15.10.2019).
7. Porshnev, S.V., Belyaev, D.O. Obzor rezul'tatov issledovaniy skrytykh tekhnicheskikh kanalov utechki informacii, obrabatyvaemoj sredstvami vychislitel'noj tekhniki. 2020, V : Vestnik UrFO. Bezopasnost' v informacionnoj sfere.
8. Lamson, B. W. A Note on the Confinement Problem A Note on the Confinement Problem, Communications of the ACM, 16, 10 (Oct. 1973), pp 613-615.
9. GOST R 53113.1-2008. Informacionnaya tekhnologiya. Zashchita informacionnykh tekhnologij i avtomatizirovannykh sistem ot ugroz informacionnoj bezopasnosti, realizuemykh s ispol'zovaniem skrytykh kanalov. CHast' 1. Obshchie polozheniya.
10. Банк данных угроз безопасности информации. – URL: <https://bdu.fstec.ru/ubi/threat/view/id/526> – (дата обращения: 25.07.2020).
11. Банк данных угроз безопасности информации. – URL: <https://bdu.fstec.ru/ubi/threat/view/id/530> – (дата обращения: 25.07.2020).
12. GOST R 53113.2-2009. Informacionnaya tekhnologiya. Zashchita informacionnykh tekhnologij i avtomatizirovannykh sistem ot ugroz informacionnoj bezopasnosti, realizuemykh s ispol'zovaniem skrytykh kanalov. CHast' 2. Rekomendacii po organizacii zashchity informacii, informacionnykh tekhnologij i avtomatizirovannykh sistem ot atak s ispol'zovaniem skrytykh kanalov.
13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise. arXiv preprint arXiv:1608.03431, 2016. – URL: <https://arxiv.org/ftp/arxiv/papers/1608/1608.03431.pdf> – (дата обращения: 27.03.2020).

14. A Guide to Understanding Covert Channel Analysis of Trusted Systems, National Computer Security Center. NCSC-TG-030. - Ver. 1, 1993 – URL: <https://fas.org/irp/nsa/rainbow/tg030.htm> – (data obrashheniya: 10.07.2020).

15. Federal Information Processing Standard Publication 140-2 – URL: <https://csrc.nist.gov/publications/fips/140/2/final> – (data obrashheniya: 15.06.2020).

16. Federal Information Processing Standard Publication 140-3 – URL: <https://csrc.nist.gov/publications/fips/140/3/final> – (data obrashheniya: 15.06.2020).

19. Yong Bin Zhou, Deng Guo Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China, 2006. – URL: <http://eprint.iacr.org/2005/388.pdf> – (data obrashheniya: 15.06.2020).

17. Common Vulnerabilities and Exposures. – URL: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4576> – (data obrash-heniya: 12.06.2020).

ПОРШНЕВ Сергей Владимирович, доктор технических наук, профессор, директор Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: sergey_porshnev@mail.ru

БЕЛЯЕВ Дмитрий Олегович, старший преподаватель Учебно-научного центра «Информационная безопасность», Институт радиоэлектроники и информационных технологий – РтФ, Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина». 620002, г. Екатеринбург, ул. Мира, 19. E-mail: belyaev-urfu@yandex.ru

PORSHNEV Sergey, Dr.Sc., Professor, head of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University. B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: sergey_porshnev@mail.ru

BELIAEV Dmitry, Senior Lecturer of Educational and research center «Information security», Institute of radio electronics and information technologies – RTF, Ural Federal University. B. N. Yeltsin. 620002, Ekaterinburg, Mira street, 19. E-mail: belyaev-urfu@yandex.ru