УДК 004.056.5

Вестник УрФО № 4(38) / 2020, с. 5–21

Поршнев С.В., Беляев Д.О.

DOI: 10.14529/secur200401

СКРЫТЫЕ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ: АНАЛИЗ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ

В процессе функционирования средств вычислительной техники (СВТ) возникают технические каналы утечки информации (ТКУИ). Сегодня перечень ТКУИ, а также методы и средства с борьбы с утечками по данным техническим каналам регламентируются действующей нормативной документа-цией в области технической защиты информации (ТЗИ). Однако оказывается, что также существует целый ряд ТКУИ, мер противодействия, которым не предусмотрено действующими нормативными документами в области ТЗИ. Для краткости данный тип ТКУИ назван скрытыми техническими каналами утечки информации (СКТУИ).

Примерами СКТУИ, используемыми для передачи данных, обрабатываемых в СВТ, являются:

– линии электропередач, в которых зависимость потребления электро-энергии от времени определяется нагрузкой центральных процессоров (CPU) СВТ, управляемых предустановленной специальной программой;

– акустический ультразвуковой канал, 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.

Принимая во внимание реальную опасность несанкционированного доступа к данным, обрабатываемым в СВТ, понятна необходимость научных исследований СТКУИ с

целью разработки методик оценивания угроз безопасности информации и разработки научно-обоснованных методов и средств защиты от утечки информации по данным ТКУИ.

В статье проведен обзор открытых научных публикаций, посвященных исследованиям СТКУИ, в том числе рассмотрены механизмы передачи информации по СТКУИ и экспериментальные результаты, подтверждающие работоспособность данных механизмов.

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

Porshnev S.V., Belyaev D.O.

REVIEW OF RESEARCH RESULTS ON HIDDEN TECHNICAL CHANNELS OF INFORMATION LEAKAGE PROCESSED BY COMPUTER TECHNOLOGY

In the process of functioning of computer equipment, technical channels of information leakage arise. Today, the list of technical channels of information leakage, as well as methods and means to combat leaks through these technical channels are regulated by the current regulatory documentation in the field of technical information protection. However, it turns out that there are also a num-ber of technical channels of information leakage, measures to counteract which are not provided for by the current regulatory documents in the field of technical information protection. For the sake of brevity, this type of technical information leakage channels is called hidden technical information leakage channels.

Examples of hidden technical channels of information leakage used to transmit data processed in a computer tool are:

– power lines in which the dependence of electricity consumption on time is determined by the load of the central processing units (CPUs) of the computer tool, controlled by a pre-installed special program;

– acoustic ultrasonic channel formed by passive speakers and headphones without using a microphone;

– low-frequency magnetic vibrations that occur during the operation of the CPU of computer equipment;

– radio emission 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 of thermal radiation of the computer equipment housing;

– acoustic radiation generated by disk drives in the process of writing and reading information;

– electromagnetic radiation that occurs during access to various devices via the USB port;

– optical radiation of led indicators means of computing technology, etc.

Taking into account the real danger of unauthorized access to data pro-cessed in a computer tool, it is clear that there is a need for scientific research of hidden technical channels of

information leakage in order to develop methods for assessing threats to information security and develop scientifically based meth-ods and means of protection against information leakage using these technical channels of information leakage.

The article reviews open scientific publications devoted to the research of hidden technical channels of information leakage, including the mechanisms of information transmission through hidden technical channels of information leak-age and experimental results confirming the operability of these mechanisms.

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

Введение

Техническим каналом утечки информации (ТКУИ) называется совокупность источник информации (передатчик – объект разведки), линия связи (протяженная физическая среда), по которой распространяется информационный сигнал (собственно, канал передачи), а также средство приёма (пере-хвата) 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]. Перечень объективных и субъективных факторов (внутренних и внешних), воздействующих на защищаемую информацию, обрабатываемую средствами вычислительной техники, которые непосредственно формируют ТКУИ выделен в [4].

Однако оказывается, что также существуют ТКУИ, наличие которых обусловлено факторами, не предусмотренных в действующих нормативно-правовых документах в области технической защиты информации (например, акустические эманации, возникающие при отображении визуальной информации на экране, параметры которых определяются законом формирования изображения [5] и др.), которые для краткости будем называть далее «скрытыми техническими каналами утечки информации» (СТКУИ). (При этом мы сознательно не даем в данной статье точного определения понятия СТКУИ, так как для это потребуется провести детальный анализ действующей отечественной и зарубежной нормативно-правой базы в области технической защиты информации, который является предметом отдельной статьи).

В статье проводится обзор открытых публикаций, в которых обсуждаются результаты исследований скрытых технических каналов утечки информации, обрабатываемой средствами вычислительной техники.

Анализ результатов изучения СТКУИ физически изолированных средств вычислительной техники

В настоящее время зарубежными специалистами в области обеспечения информационной безопасности проводятся активные исследования нерегламентированных ТКУИ, связанных с тематикой возможности извлечения информации и управления техническими средствами обработки информации с использованием скрытых технических каналов. Данный вывод подтверждает результаты информационного поиска открытых зарубежных публикаций за последние 15 лет, приведенные ниже.

1. **Цель исследования**: подтверждение гипотезы о возможности обнаружения и извлечения информации, выводимой на экран ЖК монитора, по акустическим излучениям, сопровождающим процесс отображения инфор-мации на экране ЖК монитора, с использованием тест-сигнала типа «зебра» и экранных клавиатур [5].

Результаты исследования:

– установлено, что при визуализации отдельных пикселей генерируются акустические сигналы, частоты которых зависят от цвета отдельного пикселя (например, черного или белого);

– описан механизм утечки информации, установлена зависимость формы и характеристик (частота, амплитуда) акустического сигнала от формы отображаемой информации, описаны механизмы извлечения информативной составляющей (в том числе и использованием специально разработанного приложения для смартфона) на стороне злоумышленника;

– определены источники акустического излучения в ЖК мониторе;

– доказана возможность извлечения информации о коде нажатой клавиши экранной клавиатуры из акустических сигналов, создаваемых экраном;

– для доказательства возможности распознавания символов и слов в акустическом сигнале, перехваченном по данному ТКУИ, разработано мобильное приложение, функционирующее на основе сверхточных нейронных сетей.

2. **Цель исследования**: исследование возможности регистрации сигнала, представляющего собой низкочастотное магнитное поле, генерируемое ядрами процессоров компьютера, помещенного в клетку Фарадея, па-раметры которого определяются операциями, выполняемыми ядрами про-цессоров, и извлечение информации из низкочастотного магнитного поля о выполняемых операциях [6, 7].

Результаты исследования:

– Разработана следующая модель угроз защищаемой информации:

• на атакуемом компьютере, установлено вредоносное программное обеспечение, которое собирает информацию, представляющую интерес для злоумышленника (текстовые данные, ключи шифрования, маркеры учетных данных или пароли и т.д.);

• вредоносная программа в заданное время кодирует собранную информацию, блокирует выполнение других программ и нагружает центральный процессор таким образом, что генерируется низкочастотное магнитное поле на заданной частоте, модулированное по амплитуде соответствующим бинарным сигналом, таким образом, магнитное поле оказывается носителем информации, являющейся целью нарушителя;

• на некотором удалении от компьютера установлен магнитометрический датчик, регистрирующий в установленное время магнитное поле, создаваемое компьютером;

• декодирование сигнала, зарегистрированного с выхода магнитометрического датчика.

– для реального существования предложенной модели угроз безопас-ности информации авторы разработали программу «ODINI» для стационар-ных компьютеров, а также программу «MAGNETO» для смартфонов, кото-рые могут управлять низкочастотными магнитными полями, излучаемыми зараженным вычислительными средствами за счет изменения нагрузку на ядра процессоров, при этом, не требуя специальных привилегий (например, root);

– получено экспериментальное подтверждение работоспособности исследованного ТКУИ: в заданные моменты времени были зарегистрированы сигналы с выхода магнитометрического датчика, удаленного на расстояние до 50 см от ноутбуков, до 100 см от настольных ПК и до 150 см от сервера, содержащие закодированную информацию, интересующую нарушителя;

– доказано, что клетка Фарадея в данном случае оказалась абсолютно неэффективной.

3. **Цель исследования:** подтверждение гипотезы о том, что оптическое излучение светодиодных индикаторов состояния, устанавливаемых на различных устройствах вычислительной техники, которое может быть зарегистрировано с помощью видеокамер, смартфонов и смартчасов, является ТКУИ операциях, выполняемых данным вычислительным устройством (например, светодиодная панель клавиатуры) и подтверждение гипотезы о возможности реализации вредоносного ПО, обеспечивающего передачу похищаемой информации с помощью амплитудной и частотной модуляции оптического излучения [8].

Результаты исследования:

– экспериментально обнаружена связь между характеристиками мгновенной яркости мерцания светодиодов и нажимаемой в данный момент клавишей, цифровой код которой представляет собой некоторую последовательность нулей и единиц;

– дано объяснение обнаруженному эффекту, который обусловлен тем, что в процессе передачи той или иной двоичной последовательности в процессор вычислительного устройства из-за изменения нагрузки процессора и, соответственно, потребляемой им электрической мощности, что приводит к возникновению амплитудной и частотной модуляции оптического излучения светодиодов индикаторной панели с характерным периодом несколько микросекунд, что делает их незаметным для человеческого глаза;

– экспериментально подтверждена возможность регистрации оптического излучения светодиодов клавиатуры светочувствительными датчиками, удаленными от источника излучения на расстояние до 50 метров, в том числе камерами смартфонов и смартчасов, оснащенных соответствующими светофильтрами, даже при незначительном освещении;

– продемонстрирована возможность увеличения периода амплитудной и частотной модуляции оптического излучения светодио-

дов индикаторных панелей вычислительных устройств помощью специально разработанного программного обеспечения;

– предложен алгоритм анализа параметров амплитудной и частотно-модулированной составляющих оптического излучения светодиодов индикаторных панелей вычислительных устройств, обеспечивающий идентификацию кода нажатой на клавиатуре клавиши.

4. **Цель исследования:** исследование возможности утечки информации из высокозащищенных и/или изолированных компьютерных сетей по оптическому каналу, создаваемому светодиодами, используемыми в сетевом оборудования (коммутаторами локальной сети, маршрутизаторами и т.д.) [9].

Результаты исследования:

– предложена следующая модель угроз безопасности информации:

• в изолированную компьютерную сеть внедрен вредоносный код, функционирующий в коммутаторе или маршрутизаторе локальной сети, который получил полный контроль и управление над индикаторами состояния сети;

• вредоносный программный код имеет доступ к информации, передаваемой в защищенной компьютерной сети;

• вредоносный программный код кодирует информацию, передаваемую в защищенной компьютерной сети, и использует для ее для модуляции соответствующими кодами оптического излучения индикаторов состояния сети;

• модулированное оптическое излучение индикаторов состояния сети регистрируется оптическим датчиком выбранного типа и затем декодируется.

– представлены схемы модуляции и кодирования данных, а также разработанный протокол передачи данных;

– проведен анализ двух типов атак:

• на уровне микропрограммного обеспечения, в которых вредоносное программное обеспечение устанавливается на микропрограммном уровне сетевого коммутатора или маршрутизатора;

• вредоносный программный код имеет доступ к информации, передаваемой в защищенной компьютерной сети;

• атаки на уровне программного обеспечения, в которых вредоносный код управляет светодиодами с зараженного компьютера через стандартные каналы удаленного управления (например, SSH и telnet) или используя определенных уязвимостей компьютерной сети, при этом не требуется наличие вредоносной прошивки у маршрутизатора.

5. Цель исследования: подтверждение гипотезы о возможности несанкционированного доступа к информации об операциях, выполняемых накопителями на жестких магнитных дисках (НЖМД) на основе регистрации оптического излучения светодиодных индикаторов состояния НЖМД [10].

Результаты исследования:

– результаты исследования аналогичны результатам, полученным в [8] (см. п.3).

6. **Цель исследования:** исследование возможности несанкционированного доступа к цифровой информации в процессе ее чтения с накопителей на жестких магнитных дисках записи и, соответственно, записи на основе анализа возникающих при этом акустических излучений (акустических эманаций) [11, 12].

Результаты исследования:

– проведен анализ реальных акустических сигналов, зарегистрированных в различных режимах работы НЖМД, и выявлена связь между их количественными характеристиками и выполняемыми операциями;

– для использования в научных целях разработана вредоносная программа «Disk Filtration», устанавливаемая на скомпрометированном компьютере, которая обеспечивает генерацию акустического излучения на выбранных звуковых частотах путем управления движением рычага привода жесткого диска;

– предложен возможный механизм утечки информации, в соответствие с которым перехватываемая цифровая информация используется для преобразования несущего акустического сигнала в амплитудно-манипулированный сигнал, регистрируемый ближайшим приемником (например, смартфоном, умными часами, ноутбуком и т. д.);

– предложена модель угроз безопасности информации, соответствие с которой:

• вредоносная программа, установленная на компьютере, собирает данные для извлечения (например, пароли или ключи шифрования), а затем передает их с помощью акустических сигналов, излучаемых жестким диском;

• для амплитудной модуляции акустического излучения жесткого диска вредоносная программа преднамеренно выполняет опе-

рации поиска информации на диске, которые заставляют рычаг привода жесткого диска совершать механические движения, за счет которых обеспечивается амплитудная акустического излучения;

• ближайший приемник принимает и декодирует акустический сигнал, и предоставляет доступ злоумышленнику к извлеченной информации.

7. **Цель исследования:** исследование возможности утечки аудиоинформации за счет принудительного переключения динамиков мультимедийного компьютера в режим микрофона [13].

Результаты исследования:

– разработан метод перехвата аудиоинформации, основанный на принудительном переключении динамиков мультимедийного компьютера в режим микрофона с помощью вредоносного ПО, использующего соответствующую функцию аудиочипа, и регистрацию генерируемого звукового сигнала с помощью аудиосистемы удаленного компьютера;

– подтверждена работоспособность предложенного метода несанкционированного доступа к аудиоинформации, в том числе приведены экспериментальные результаты, подтверждающие возможность перехвата в ультразвуковом диапазоне звуковых сигналов, в том числе продемонстрирована возможность перехвата аудиоинформации по исследуемому ТКУИ, компьютером, удаленным от атакуемого компьютера на расстояние до 9 м;

– установлено, что максимальная чувствительность динамиков и наушников, используемые пользователями мультимедийных компьютеров, находится в ближнем ультразвуковом диапазоне звуковых волн (от 18 кГц до 24 кГц);

– подтверждена возможность прямой передачи на расстояниях до 3 м скрытой связи между наушниками атакуемого компьютера и компьютером атакующего и передачи по данному ТКУИ аудиоинформации в ультразвуковом диапазоне.

8. Цель исследования: исследование возможности использования инфракрасного излучения для установления скрытой двусторонней связи между внутренней сетью организации и удаленным компьютеров злоумыш-ленника для реализации утечки данных из компьютерной сети передачи и проникновение в компьютерную сеть [14].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере:

• на атакуемом компьютере размещен вредоносный программный код, имеющий доступ к камерам видеонаблюдения, оснащенных инфракрас-ными светодиодами (IR LED), а также доступ к информации, представляющей интерес для нарушителя (конфиденциальные данные, ПИН-коды, пароли и ключи шифрования), которая далее преобразуется в двоичные коды;

• далее полученные двоичные коды используются вредоносносным ПО для модуляции оптического излучения инфракрасного диода API-видеокамеры;

• регистрация излучения инфракрасного диода API-видеокамеры, с помощью ИК-видеокамеры, используемой атакующей стороной, и декодирование двоичных кодов в смысловой вид;

– экспериментальна подтверждена возможность реализации следующего сценария атаки, целью которой является перехват управления атакуемым компьютером:

• на атакуемом компьютере размещен вредоносный программный код, имеющий доступ к камерам видеонаблюдения, оснащенных инфракрасными светодиодами (IR LED);

• атакующий компьютер, используя инфракрасные светодиоды, излучает модулированное кодами команд управления атакуемого компьютера;

• вредоносное ПО через ИК-видеокамеру атакуемого компьютера извлекает их выходного видеопотока соответствующий информационный сигнала, далее декодирует информационный сигнал и выполняет полученную команду;

– установлено, что утечка информации по исследованному ТКУИ возможна между удаленными друг от друга компьютерами на расстояниях от 10 до 100 м, при этом скорость передачи данных достигает 20 бит/сек, скорость приема данных – 100 бит/сек;

– продемонстрировано, что описанные способы атаки, названные авторами технологией «aIR-Jumper», при соответствующей модификации, может быть использована для несанкционированного доступа к «умными» дверными звонками и другими устройствам

Интернета-вещей, которые укомплектованы инфракрасными LED.

9. **Цель исследования:** исследование возможности использования силовых кабелей (кабелей электропитания) для извлечения данных [15].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере с помощью вредоносного ПО «PowerHammer», реализующего следующую модель утечки информации:

• целевой компьютер заражается вредоносной программой, которая регулирует уровень загрузки ресурсов процессоров, выбирая из них ядра, не занятые в данный момент пользовательскими операциями, и загружая их собственными задачами;

• в результате изменения загрузки процессоров соответствующим образом изменяется потребление энергии компьютером, при этом, организовав соответствующим образом изменения потребления электроэнергии, можно реализовать кодирование и передачу информации с атакуемого компьютера;

– при практической реализации описанной атаки предложено и измерять вариации мощности электрических сигналов, передаваемых в силовых сетях, используя для этого трансформатор тока, который имеется в свободной продаже.

10. **Цель исследования:** исследование возможности скрытой передачи информации из физически изолированных средств вычислительной техники на частотах стандарта GSM [16].

Результаты исследования:

– описана вредоносная программа «GSMem», которая может извлекать и передавать данные через воздушный зазор на частотах стандарта GSM. Для реализации алгоритма модуляции B-ASK использовался набор команд Streaming SIMD Extension (SSE), имеющийся в процессорах Intel и AMD, в качестве передатчика использовался процессов ПЭВМ и шина памя-ти;

– продемонстрировано, что вредоносное программное обеспечение на зараженном целевом компьютере модулирует и передает электромагнитные сигналы на выше упомянутых частотах, используя многоканальную архитектуру памяти для усиления передачи;

– показано, что передаваемые сигналы могут быть приняты и демодулированы руткитом, помещенным в базовую прошивку соседнего сотового телефона;

– реализация прототипа Gamemaker, состоящего из передатчика и приемника, оценка его производительности и ограничений при использовании;

– демонстрация эффективности и осуществимости СТКУИ: эффективная дальности передачи с использованием стандартного мобильного телефона составляет 1 – 5,5 метра;

– установлено, что при использовании специального, но доступного для приобретения аппаратного приемника эффективная дальность канала связи ТКУИ достигает более 30 метров.

11. **Цель исследования:** проверка гипотезы о возможности использования акустических сигналов, возникающих при нажатии на клавиши клавиатуры средств вычислительной техники (в том числе, ноутбуков, мобиль-ных телефонов и банкоматов и т.д.) в качестве ТКУИ, по которому нарушитель может получить информацию о том, какие клавиши и в какой последовательности были нажаты пользователем [17].

Результаты исследования:

– продемонстрировано, что исследованная атака может быть эффективной, если нарушителю удается установить соответствие между кодом нажатой клавиши и спектром перехваченного акустического сигнала, используя для этого, например, соответствующим образом обученную нейронную сеть;

– построена модель акустического сигнала утечки информации, основанная на предположении о том, что амплитуды генерируемых акустических колебаний при нажатии на различные клавиши различны и проведены экспериментальные исследования, результаты которых подтвердили адекватность предложенной модели;

– продемонстрировано, что нейронная сеть, обученная на клавиатурном почерке конкретного пользователя, может решать задачи распознавания и классификации акустических сигналов, возникающих при нажатии на клавиши данной клавиатуры другим пользователем;

– установлено, что влияние стиля набора текста на клавиатуре (клавиатурного почерка) на качество классификации акустических сигналов, генерируемых при нажатии на клавиши, не значительно.

12. **Цель исследования:** экспериментальная проверка возможности реализации атаки, которая позволяет восстановить выводимый на печать текст на основе записи звука, который издает матричный принтер в процессе печати текста, с помощью акустического микрофона, установленного на расстоянии 10 см от принтера [18].

Результаты исследования:

– доказано, что при отсутствии априорных знаний о тексте, выводимом на печать, было правильно распознано около 72% напечатанных слов;

– доказано, что при наличии априорных сведений о тексте, выводимом на печать, было правильно распознано около 95 % напечатанных слов.

13. **Цель исследования:** исследование излучения в побочном электромагнитном канале устройства цифровой подписи ECDSA, использующего стандартную криптографическую библиотеку ОС Android [19].

Результаты исследования:

– доказано, что при использовании эллиптических кривых над простыми полями удается достаточно эффективно восстанавливать секретный ключ на смартфонах, функционирующих по управлением ОС Android, используя боковой (побочный) канал;

– впервые продемонстрирована возможность различения операций удвоения и сложения, выполняемых при использовании кривых Коблица. реализуемых в многоядерном процессоре с тактовой частотой более гига-герца.

14. **Цель исследования:** исследование возможности распознавания и восстановления вводимых с клавиатуры символов по акустическим сигналам, генерируемым при нажатии и возвращения клавиш в исходное положение [20].

Результаты исследования:

– выявлена связь между характеристиками акустического сигналом, генерируемого в процессе ввода текстовой информации с клавиатуры, и процессом ввода текста с клавиатуры, в том числе установлено, что характеристики акустических сигналов клавиатуры зависят от координат мест расположения клавиш, физическим расположением на клавиатуре;

– продемонстрирована возможность улучшения качества распознавания вводимой текстовой информации на основе идентификации не нажимаемых клавиш, но набираемых слов, что позволяет использовать дополнитель-но к свойствам акустического сигнала статистическую информацию о свойства языка;

– предложна модель атаки, основанная на использовании акустических сигналов, генерируемых в процессе ввода текстовой информации;

– предложен алгоритм анализа акустического сигнала утечки, основанный на совместном использовании методов ЦОС методов анализа данных;

– продемонстрирована возможность реконструкции отдельных слов, состоящих из 7-13 символов;

– обнаружено, что точность идентификации слов, состоящих более из 10 букв и более, составляет 90%.

– доказано, что факторами, определяющими успешность данного типа атаки, являются длина слова и количество одинаковых символов в слове.

15. **Цель исследования:** проверка гипотезы о возможности приема акустических сигналов, генерируемых при нажатии на клавиши клавиатуры, с помощью программного обеспечения VoIP и распознавания вводимых символов по их известным акустическим образам в условиях, когда у атакующего отсутствует какая-либо дополнительная информация об источнике акустического сигнала [21].

Результаты исследования:

– предложена модель угроз безопасности информации, соответствие с которой во время VoIP телефонного разговора между нарушителем жертвой, последний набирает на клавиатуре атакуемого устройства какой-либо текст (например, например, текст сообщения электронной почты или пароль), что сопровождается акустическими эманациями клавиатуры, автоматически регистрируемые микрофоном телефона жертвы и передающиеся на телефон атакующего по VoIP;

– обоснованы условия реализации изучаемой угрозы безопасности информации:

• наличие у злоумышленника информации о модели используемой клавиатуры и клавиатурном почерке жертвы;

• наличие у злоумышленника инструментов анализа акустических сигналов, в которых реализованы соответствующие методы, не требующие априорной информации об источнике акустического сигнала.

– продемонстрировано, что вероятность утечки информации по исследуемому ТКУИ

возрастает при увеличении числа символов набираемого жертвой текста.

16. **Цель исследования:** подтверждение гипотезы о возможности перехвата акустических сигналов, генерируемых клавиатурой компьютера во время использования программного обеспечения GnuPG, реализующего дешифровку текстов, зашифрованных с помощью алгоритма RSA, и извлече-ния из них значений 4096-битных ключей [22].

Результаты исследования:

– экспериментально подтверждена возможность перехвата исследуемых акустических сигналов с помощью обычного мобильного телефона, расположенного в непосредственной близости к целевому компьютеру, или более чувствительного микрофона, расположенного на расстоянии до 10 метров от целевого компьютера;

– продемонстрирована возможность определения полных значений 4096-битных секретных ключей RSA основе анализа перехваченных мобильным телефоном акустических сигналов, генерируемых клавиатурой компью-тера во время использования программного обеспечения в течение одного часа.

17. **Цель исследования:** доказательство возможности идентификации нажимаемых клавиш клавиатуры на основе анализа, генерируемых при этом акустических сигналов, излучениям клавиатуры, зарегистрированным с помощью микрофона мобильного телефона [23].

Результаты исследования:

– предложен метод идентификации нажимаемых клавиш клавиатуры, основанный на анализе временных задержек акустических сигналов, гарнируемых при последовательном нажатии на клавиши, а также анализе харак-теристик акустических сигналов с целью идентификации нескольких нажатий одной и той же клавиши, который не требует использования маркированных обучающих данных, а также лингвистического контекста;

– получены оценки качества идентификации нажатых клавиш на клавиатурах трех типов смартфонов, свидетельствующие о том, что точность разработанного авторами метода анализа перехваченных акустических сигналов составила 94%.

18. **Цель исследования:** исследование возможности извлечения информации из источников оптического сигнала, установленных компьютерах и стандартном сетевом оборудовании (сетевых картах, маршрутизаторах и т.д.), о реализуемых на них операциях (например, записи и чтения файлов и т.д.) [24].

Результаты исследования:

– экспериментально подтверждена возможность извлечения информации об операциях, выполняемых компьютером из оптических излучений интерфейсов WAN, расположенных на задней панели корпоративных маршрутизаторов, находящихся в сетевых стойках.

19. **Цель исследования:** исследование возможности восстановления данных на основе анализа оптического излучения светодиодных индикаторов, встроенных в технические средства обработки, хранения и передачи информации [25].

Результаты исследования:

– реализован программный компонент с использованием библиотеки OpenCV 3.0 (Itseez, 2015), который обеспечивает регистрацию оптического излучения светодиодных индикаторов, встроенных в технические средства обработки информации, идентификацию источников оптического излучения, а также анализ вариаций яркости оптических источников;

– экспериментально подтверждена возможность кодирования похищаемой информации и ее передачи по оптическому каналу, а также декодирования оптического излучения светодиодных индикаторов и сохранении далее извлеченной информации на веб-сервер через мобильное соединение смартфона или компьютерную сеть;

– разработан алгоритм обнаружения и определения местоположения светодиодов, который основан на поиске различий между двумя последовательными кадрами.

20. **Цель исследования:** теоретическое исследование проблемы извлечения информации при использовании программно-управляемых скрытых каналами утечки информации [26].

Результаты исследования:

– разработана концептуальная модель перехвата информации по программно-управляемым техническим каналам, а также манипулирования информационными ресурсами специальным программным обеспечением.

21. **Цель исследования:** исследование возможности использования для несанкционированного доступа к аудиоинформации за счет использования ультразвуковых моде-

мов, установленных на мобильных устройствах связи [27].

Результаты исследования:

– продемонстрирована возможность реализации ТКУИ за счет использования ультразвукового модема мобильного устройства связи (Android), которое осуществляет принудительную регистрацию и передачу перехваченных акустических сигналов на мобильное устройство нарушителя;

– обосновано, что на расстоянии до 100 метров от источника излучения вероятность перехвата информации составляет 0,9–1.

22. **Цель исследования:** исследование возможности утечки звуковой информации при несанкционированном доступе к звуковой карте компьютера, находящегося в компьютерной сети [28].

Результаты исследования:

– продемонстрирована возможность перехвата аудиоинформации с помощью штатных средств звукозаписи и звуковоспроизведения персонального компьютера типа ноутбук (возможность перехвата аудиоинформации с помощью звуковой карты стационарного компьютера подтверждена в [29]).

23. **Цель исследования:** проверка гипотезы о возможности использования теплового излучения систем отопления, вентиляции и кондиционирования, подключенных к сети Интернет, для получения управления над изолированной корпоративной компьютерной сетью [30].

Результаты исследования:

– экспериментально подтверждена возможность реализации следующего сценария атаки, целью которой является несанкционированный доступ к информации в атакуемом компьютере:

• имеется изолированная корпоративная компьютерная сеть, зараженная вредоносным ПО;

• вредоносное ПО получило права управления хостами корпоративной компьютерной сети, а также права доступа к установленным в каждом компьютере тепловых датчиках, предназначенных для измерения температуры центрального процессора и передачи ее значений в BIOS;

• вредоносное ПО перехватило управление датчиками температуры и перевело их в режим измерения температуры окружающего воздуха;

• параллельно корпоративной компьютерной сети организации, охватывающей здание, в здании имеется система отопления, вентиляции и кондиционирования (HVAC), чей центр управления имеет выход в Интернет;

• злоумышленники реализовали успешную атаку и получили доступ к управлению системой HVAC;

• используя доступ к управлению системой HVAC, злоумышленник реализует изменение температуры воздуха в выбранном помещении в соответствие с кодами команды, передаваемой вредоносному ПО по тепловому каналу;

• вредоносное ПО получает сигнал с выхода теплового датчика, находящегося под его управлением, и далее, декодировав полученное сообщение, получает переданную злоумышленником команду.

– для подтверждения работоспособности обсуждаемого сценария атаки создано вредоносное программное обеспечение «HVACKer», предназначенное в том числе, для перехвата управления тепловыми датчиками, установленных в средствах вычислительной техники и их переключения в режим измерения температуры окружающей среды и разработан соответствующий line-encoding протокол, который позволяет передавать команды посредством изменения температуры;

– получены оценки скорости передачи данных по тепловому каналу, составляющие $\approx$ 40 бит/сек, что оказывается вполне достаточно для управления внедренным кодом;

– установлено, что ПО «HVACKer» можно использовать только для передачи команд в зараженную компьютерную сеть, но не для извлечения для извлечения из нее информации, так как точность тепловых датчиков, используемых в HVAC-устройствах, оказывается недостаточной для декодирования информации, передаваемой по тепловому каналу из компьютерной сети нарушителю.

24. **Цель исследования:** исследование возможности восстановления текста, набираемого на клавиатуре, основанного анализе на видеозаписи процесса набора текста пользователем. Разработка методов для отслеживания движения рук пользователей, реконструкции предложений и исправления ошибок, т.е. автоматическое восстановление текста, набранного пользователем, начинающееся с видеозаписи сеанса набора текста [31].

Результаты исследования:

– разработан программный инструмент, обеспечивающий автоматическое отслежи-

вание на видеозаписях процесса набора текста движений рук пользователей и восстановление набираемого текста, («ClearShot»), и прове-дено его тестирование в условиях близких к реальным;

– экспериментально подтверждена возможность реконструкции значительную часть набранного текста с помощью («ClearShot»);

– разработан алгоритм анализа результатов функционирования инструмента в типичной офисной среде, состоящий из двух этапов:

• 1 этап – анализ видеоинформации, записанной камерой с использованием методов компьютерного зрения (для каждого кадра видео компьютерный анализ зрения вычисляет набор клавиш, которые, вероятно, были нажаты, набор клавиш, которые, безусловно, не были нажаты, и положение пробелов);

• 2 этап – анализ и корректировка введенного текста с помощью языковых и контекстно-зависимых методов.

– в качестве доказательства работоспособности исследуемого метода представлен реконструированный текст, где каждое его слово представлено списком возможных слов-кандидатов, ранжированных по вероятности.

25. **Цель исследования:** получение оценки пропускной способности скрытых тепловых каналов утечки информации [32].

Результаты исследования:

– предложен эмпирический метод оценивания реальных (и ранее неизвестных) мощностей тепловых СТКУИ;

– обнаружено (на примерах сценариев с различными промежуточны-ми хостами и различными уровнями температурной индукции и шума), что скорость передачи информации в исследуемом канале может достигать ≈ 20,5 бит/час;

– установлено, что пропускная способность канала уменьшается почти вдвое (до 10,3 бит/час) при повышении уровня шума или более эффективном охлаждении на промежуточном хосте компьютерной сети.

26. **Цель исследования:** исследование возможности использования бытовых роботов-пылесосов в качестве средств акустической речевой разведки за счет перепрофилирования встроенных лазерных датчиков (лидаров) в систему дистанционного зондирования бытовых предметов, выступающих в роли источников вибрационных сигналов [33].

Результаты исследования:

– представлен программно-аппаратный механизм «LidarPhone», перепрофилирующий встроенный в робот-пылесос лидар в лазерный микрофон, который может воспринимать звуки от тонких вибраций, индуцированных на близлежащих объектах;

– модель угроз для данного вида атак схожа с моделью угроз, реализуемой с использованием систем дистанционного лазерного зондирования поверхностей остекления оконных проемов, за исключением того, что технология LidarPhone использует для записи отраженных сигналов внутреннюю память бытового устройства.

– установлено, что время функционирования разработанной технологии составляет порядка 19 часов непрерывного времени;

– продемонстрировано, что в условиях применения методов глубокого обучения с использованием сверточных нейронных сетей разработанная технология достигает точности классификации и распознавания акустических образов информативных символов порядка 90%, произнесенных в течение 10-20 секунд на расстоянии порядка 20 см;

– установлено, что значительными ограничивающими факторами эффективной реализации приведенной атаки являются уровень акустического давления, создаваемого в точке перехвата, и расстояние от источника сигнала до приемника, как следствие, влияющие на значение отношения «сигнал/шум».

27. **Цель исследования:** проверка гипотезы о возможности использования сенсорных датчиков технических средств интернет-вещей (IoT) в качестве устройств перехвата и восстановления акустической речевой информации [34].

Результаты исследования:

– представлен механизм «PitchIn», реализующий перехват и восстановление акустических сигналов с точностью порядка 79% от различных устройств со встроенными датчиками акселерометрного, гироскопического и микрофонного типа, расположенным на расстоянии до 1,5 метров от источника речи;

– также, как и в исследовании, приведенном в п.26, установлено, что значительными ограничивающими факторами эффективной реализации приведенной атаки являются уровень акустического давления, создаваемого в точке перехвата, и расстояние от источника сигнала до приемника, как следствие, влияющие на значение отношения «сигнал/шум».

28. **Цель исследования:** исследование возможности использования гироскопа современного смартфона в качестве средства перехвата акустической информации [35].

Результаты исследования:

– представлено разработанное мобильное приложение «Gyrophone», использующее обработку сигналов, воздействующих на гироскоп смартфона, и машинное обучение для идентификации информации говорящего и для анализа речи;

– показано, что гироскопы достаточно чувствительны для измерения акустических колебаний. Это приводит к возможности восстановления речи по показаниям гироскопа, а именно к использованию гироскопа в качестве микрофона;

– показано, что частота дискретизации гироскопа достигает 200 Гц, что охватывает часть слышимого диапазона. Это повышает вероятность подслушивания речи в непосредственной близости от телефона без доступа к реальному микрофону;

– установлено, что, поскольку частота дискретизации гироскопа ограничена, невозможно полностью восстановить перехваченную речь по измерениям одного гироскопа. Поэтому в случае использования гироскопа в качестве скрытого устройства перехвата информации необходимо прибегать к автоматическому распознаванию речи путем машинного обучения;

– показано, что в случае ограничения небольшим словарным запасом, состоящим исключительно из цифровых произношений ("один", "два", "три",...) возможно достижение успеха распознавания речи порядка 65%;

– показано, что при комбинации сигналов от двух или более смартфонов возможно увеличение эффективной частоты дискретизации акустического сигнала, при этом злоумышленник достигает более высокой скорости распознавания речи и более высокого процента (77%) успешного распозна-вания речевого контента.

29. **Цель исследования:** исследование возможности использования виброгенератора мобильного телефона в качестве микрофона [36].

Результаты исследования:

– представлено программное средство «VibraPhone», реализованное посредством преобразования механических колебаний, возникающих при воздействии акустического сигнала на виброгенератор (вибромотор) смартфона, и позволяющее использовать методы машинного обучения для распознавания информативных символов;

– установлено, что средняя точность распознавания речи составляет порядка 88% при условии расположения источника акустического сигнала на расстоянии 2 метров от смартфона и воспроизведении акустической информации при интегральном звуковом давлении 80 дБ;

– установлено, что при снижении уровня звукового давления с 80 до 60 дБ процент распознанной речи падает до 60%.

30. **Цель исследования:** исследование возможности извлечения акустической информации из параметров радиосигнала, изменяющихся за счет вибраций акустических излучателей (колонки, громкоговорители и т.д.), которые механически воздействуют на радиосигнал или на расположенные в непосредственной близости радиопередатчики [37].

Результаты исследования:

– установлено, что модель угроз, представленная в данном виде атак, концептуально схожа с механизмом, лежащем в основе лазерного радара (LADAR), который обычно используется для проверки устойчивости строительных конструкций;

– смоделирована процедура возмущения радиоволн звуковыми колебаниями: в качестве модели процесс воздействия механических колебаний на электромагнитные колебания рассмотрен как процедура низкоскоростной амплитудно-фазовой модуляции;

– с помощью разработанной модели спроектирован демодулятор в частотной области, изолирующий несущественные компоненты радиосигнала и позволяющий экстраполировать звуковые сигналы, проецировать их во временную область, которая в конечном итоге становится воспринимаемой злоумышленником;

– установлено, что в случае приема радиосигнала на фоне шумов при пиковом отношении «сигнал/шум» превышающем 15 дБ, тестеры обычно могут распознавать контент с точностью, близкой к 100%. Данное условие достигается при наблюдении радиосигнала на расстоянии от 2 до 4 метров от его источника (при этом источник радиосигнала – радиопередатчик – расположен на расстоянии до 1 метра от вибрирующего технического средства звуковоспроизведения);

– показано, что нижний СВЧ-диапазон (в

экспериментах использовали Wi-Fi – передатчики) обеспечивает более высокое значение пикового отношения «сигнал/шум» в задаче восстановления звука, колеблющееся в диапазоне от 7 до 9 дБ в экспериментах со звукоизолирующей стеной или звуконепроницаемым окном между передатчиком и приемником;

– установлено, что большие габариты устройства звуковоспроизведения обеспечивает более высокое значение пикового отношения «сигнал/шум» ввиду большего коэффициента вибрации.

Заключение

Проведенный анализ открытых публикаций, посвященных анализу результатов исследования СТКУИ, позволяет сделать следующие выводы.

1. Для создания СКТУИ и получения доступа к информации обрабатываемой средствами вычислительной техники, нарушитель может использовать тепловые, акустические и электромагнитные поля, а также внедренное в процессе эксплуатации или предустановленное специальное программное обеспечение на объекте вычислительной техники, которое не распознается программно-аппаратными средствами как вредоносное ПО, используя для этого, например, методы социальной инженерии, методы программного скрытия кода и иные известные методы.

2. Необходимо отметить высокую активность зарубежных ученых в исследованиях СТКУИ, в которых для получения доступа к информации, обрабатываемой средствами вычислительной техники, используются физические поля различной природы.

3. Принимая во внимании непрерывное совершенствование методов и средств защиты информации, средств вычислительной техники от утечки по «классическим» ТКУИ, требуется проведение целенаправленных отечественных исследований СКТУИ с целью выявления новых механизмов утечки информации по данным каналам, разработки моделей атак, адекватных методов и средств противодействия утечкам информации по СТКУИ, а также разработки соответствующей нормативно-правовой и методической базы по противодействию данным СТКУИ и проведения независимой проверки ре-зультатов зарубежных ученых с целью выявления возможных фактов использования открытых научных журналов с целью дезинформации.

Литература

1. Бузов Г.А. Защита информации ограниченного доступа от утеч-ки по техническим каналам: Справочное пособие / Бузов Г.А. – М.: Горячая линия-Телеком, 2015.

2. Зайцев, А. П. Технические средства и методы защиты информа-ции. 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 информатиза-ции. Факторы, воздействующие на информацию. Общие положения.

5. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthe-sia: 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).

6. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. IEEE Transactions on Information Forensics and Security, 2019. P. 1190-1203. – URL: https://ieeexplore.ieee.org/abstract/document/8820015 – (дата обращения: 18.10.2019).

7. Mordechai Guri, Andrey Daidakulov, Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. February 7, 2018 – URL: https://arxiv.org/abs/1802.02317 – (дата обращения: 21.10.2019).

8. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019. P. 801-810. – URL: https://ieeexplore.ieee.org/abstract/document/8754078 – (дата обращения: 12.02.2020).

9. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018. P. 1-12.

10. Mordechai Guri, Boris Zadov, Yuval Elovici. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED. DIMVA 2017. Detection of Intrusions and Malware, and

Vulnerability Assess-ment - 14th International Conference, 2017. P. 161-184. – URL: https://arxiv.org/ftp/arxiv/papers/1702/1702.06715.pdf – (дата обращения: 24.04.2020).

11. 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).

12. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. arXiv preprint arXiv:1606.05915, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf – (дата обращения: 19.03.2020).

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. MOSQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Com-puters Using Speaker-To-Speaker Communication. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. P. 1-8. – URL: https://ieeexplore.ieee.org/abstract/document/8625124 – (дата обращения: 15.05.2020).

14. Mordechai Guri, Dima Bykhovsky, Yuval Elovici. aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Computers & Security, vol. 82. P. 15-29. – URL: https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf – (дата обращения: 11.05.2020).

15. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. PowerHammer: Exfiltrating data from air-gapped computers through power lines. IEEE Transactions on Information Forensics and Security, vol 15, 2019. P. 1879-1890. – URL: https://arxiv.org/pdf/1804.04014.pdf – (дата обращения: 26.04.2019).

16. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yuval Elovici. GSMem: Data Exfiltration from Air-Gapped Computers over {GSM} Frequencies. 24th {USENIX} Security Symposium ({USENIX} Se-curity 15), 2015. P. 849-864. – URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-guri.pdf – (дата обращения: 08.07.2020).

17. Dmitri Asonov, Rakesh Agrawal. Keyboard Acoustic Emanations. IEEE Symposium on Security and Privacy, 2004. – URL: https://ieeexplore.ieee.org/abstract/document/1301311 – (дата обращения: 17.09.2020).

18. Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, Caroline Sporleder. Acoustic Side-Channel Attacks on Printers. USENIX Security symposium, 2010. P. 307-322. – URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf – (дата обращения: 18.09.2020).

19. Pierre Belgarric, Pierre-Alain Fouque, Gilles Macario-Rat, Mehdi Ti-bouchi. Side-channel analysis of Weierstrass and Koblitz curve ECDSA on An-droid smartphones. Cryptographers'Track at the RSA Conference, 2016. P. 236-252. – URL: https://eprint.iacr.org/2016/231.pdf – (дата обращения: 03.09.2020).

20. Yigael Berger, Avishai Wool, Arie Yeredor. Dictionary attacks using keyboard acoustic emanations. Proceedings of the 13th ACM conference on Computer and communications security, 2006. P. 245-254.

21. Alber to Compagno, Mauro Conti, Daniele Lain, Gene Tsudik. Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017. P. 703-715. – URL: https://arxiv.org/pdf/1609.09359.pdf – (дата обращения: 16.09.2020).

22. Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Advances in Cryptology–CRYPTO 2014, 2014. P. 444-461

23. Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, Marco Gruteser. Snooping Keystrokes with mm-level Audio Ranging on a Single Phone. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015. P. 142-154.

24. Joe Loughry. Optical TEMPEST. 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018. P. 172-177. – URL: https://arxiv.org/pdf/1808.07175.pdf – (дата обращения: 21.09.2020).

25. Arthur Costa Lopes, Diego F Aranha. Platform-agnostic Low-intrusion Optical Data Exfiltration. 3rd International Conference on Information Systems Security and Privacy (ICISSP), 2017. P. 474-480. – URL: https://www.scitepress.org/Papers/2017/62115/62115.pdf – (дата обращения: 27.09.2020).

26. J.-P. Power: Mind the gap: are air-gapped systems safe from breach-es? Symantec. 2015. – URL: http://www.symantec.com/connect/blogs/mind-gap-are-air-gapped-systems-safe-breache – (дата обращения: 09.09.2020).

27. Luke Deshotels. Inaudible Sound as a Covert Channel in Mobile De-vices. 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014. – URL: https://www.usenix.org/system/files/conference/woot14/woot14-deshotels.pdf – (дата обращения: 09.09.2020).

28. Michael Hanspach, Michael Goetz. On Covert Acoustical Mesh Net-works in Air. Journal of Communications, vol. 8, no. 11. P. 758-767, 2013. – URL: https://arxiv.org/abs/1406.1213 – (дата обращения: 10.10.2020).

29. Беляев, Д.О., Волчков, Д.Н., Поршнев, С.В. О возможности ис-пользования персонального ком-

пьютера как устройства несанкционирован-ного доступа к речевой информации. 2019, В : Вестник УрФО. Безопасность в информационной сфере. 3 (33), стр. 5-11.

30. Yisroel Mirsky, Mordechai Guri, Yuval Elovici. HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System. arXiv preprint arXiv:1703.10454, 2017 – URL: https://arxiv.org/ftp/arxiv/papers/1703/1703.10454.pdf – (дата обращения: 11.05.2020).

31. Davide Balzarotti, Marco Cova, Giovanni Vigna. Clearshot: Eaves-dropping on keyboard input from video. 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008. P. 170-183. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.9871&rep=rep1&type=pdf – (дата обращения: 20.10.2020).

32. Sebastian Zander, Philip Branch, Grenville Armitage. Capacity of temperature-based covert channels. IEEE communications letters, vol 15. P. 82-84. – URL: https://researchrepository.murdoch.edu.au/id/eprint/34937/1/capacity.pdf – (дата обращения: 17.09.2020).

33. .Sriram Sami, Sean Rui, Xiang Tan, Yimin Dai, Nirupam Roy, Jun Han. LidarPhone: acoustic eavesdropping using a lidar sensor. Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems, 2020. P. 701-702 – URL: www.cs.umd.edu/~nirupam/images/2_publication/posters_demo/writeup /LidarPhone_poster_SenSys20_nirupam.pdf – (дата обращения: 23.11.2020).

34. Jun Han, Albert Jin Chung, and Patrick Tague. Pitchln: eavesdrop-ping via intelligible speech reconstruction using non-acoustic sensor fusion. Pro-ceedings of the 16th ACM/IEEE International Conference on Information Pro-cessing in Sensor Networks, 2017. P. 181-192. – URL: https: //doi.org/10.1145/3055031.3055088 – (дата обращения: 25.11.2020).

35. Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Rec-ognizing Speech from Gyroscope Signals. 23rd USENIX Security Symposium (USENIX Security 14), 2014. P. 1053-1067.

36. Nirupam Roy and Romit Roy Choudhury. Listening through a Vibra-tion Motor. Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, 2016. P. 57-69. – URL: https://doi.org/10.1145/2906388.2906415 – (дата обращения: 30.11.2020).

37. Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. Acoustic eaves-dropping through wireless vibrometry. Proceedings of the 21st Annual Interna-tional Conference on Mobile Computing and Networking, 2015. P. 130-141.

References

1. Buzov G. A. Zashchita informacii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam: Spravochnoe posobie / Buzov G.A. – M.: 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. SHelu-panov. – M.: Goryachaya Liniya–Telekom, 2018.

3. GOST R 50922-2006. Zashchita informacii. Osnovnye terminy i op-redeleniya.

4. OST R 51275-2006. Zashchita informacii. Ob'ekt informatizacii. Faktory, vozdejstvuyushchie na informaciyu. Obshchie polozheniya.

5. Daniel Genkin, Mihir Pattani, Roei Schuster, Eran Tromer. Synesthe-sia: 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 – (data obrashheniya: 15.10.2019).

6. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. ODINI: Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. IEEE Transactions on Information Forensics and Security, 2019. P. 1190-1203. – URL: https://ieeexplore.ieee.org/abstract/document/8820015 – (data obrashheniya: 18.10.2019).

7. Mordechai Guri, Andrey Daidakulov, Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. February 7, 2018 – URL: https://arxiv.org/abs/1802.02317 – (data obrashheniya: 21.10.2019).

8. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. CTRL-ALT-LED: Leaking Data from Air-Gapped Computers via Keyboard LEDs. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), 2019. P. 801-810. – URL: https://ieeexplore.ieee.org/abstract/document/8754078 – (data obrashheniya: 12.02.2020).

9. Mordechai Guri, Boris Zadov, Andrey Daidakulov, Yuval Elovici. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018. P. 1-12.

10. Mordechai Guri, Boris Zadov, Yuval Elovici. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED. DIMVA 2017. Detection of Intrusions and Malware, and Vulnerability Assess-ment - 14th International Conference, 2017. P. 161-184. – URL: https://arxiv.org/ftp/arxiv/papers/1702/1702.06715.pdf – (data obrashheniya: 24.04.2020).

11. 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 – (data obrashheniya: 27.03.2020).

12. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. arXiv preprint arXiv:1606.05915, 2016. – URL: https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf – (data obrashheniya: 19.03.2020).

13. Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici. MOSQUITO: Covert Ultrasonic Transmissions Between Two Air-Gapped Com-puters Using Speaker-To-Speaker Communication. 2018 IEEE Conference on Dependable and Secure Computing (DSC), 2018. P. 1-8. – URL: https://ieeexplore.ieee.org/abstract/document/8625124 – (data obrashheniya: 15.05.2020).

14. Mordechai Guri, Dima Bykhovsky, Yuval Elovici. aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR). Computers & Security, vol. 82. P. 15-29. – URL: https://arxiv.org/ftp/arxiv/papers/1709/1709.05742.pdf – (data obrashheniya: 11.05.2020).

15. Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici. PowerHammer: Exfiltrating data from air-gapped computers through power lines. IEEE Transactions on Information Forensics and Security, vol 15, 2019. P. 1879-1890. – URL: https://arxiv.org/pdf/1804.04014.pdf – (data obrashheniya: 26.04.2019).

16. Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, Yuval Elovici. GSMem: Data Exfiltration from Air-Gapped Computers over {GSM} Frequencies. 24th {USENIX} Security Symposium ({USENIX} Se-curity 15), 2015. P. 849-864. – URL: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-guri.pdf – (data obrashheniya: 08.07.2020).

17. Dmitri Asonov, Rakesh Agrawal. Keyboard Acoustic Emanations. IEEE Symposium on Security and Privacy, 2004. – URL: https://ieeexplore.ieee.org/abstract/document/1301311 – (data obrashheniya: 17.09.2020).

18. Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, Caroline Sporleder. Acoustic Side-Channel Attacks on Printers. USENIX Security symposium, 2010. P. 307-322. – URL: https://www.usenix.org/legacy/event/sec10/tech/full_papers/Backes.pdf – (data obrashheniya: 18.09.2020).

19. Pierre Belgarric, Pierre-Alain Fouque, Gilles Macario-Rat, Mehdi Ti-bouchi. Side-channel analysis of Weierstrass and Koblitz curve ECDSA on An-droid smartphones. Cryptographers'Track at the RSA Conference, 2016. P. 236-252. – URL: https://eprint.iacr.org/2016/231.pdf – (data obrashheniya: 03.09.2020).

20. Yigael Berger, Avishai Wool, Arie Yeredor. Dictionary attacks using keyboard acoustic emanations. Proceedings of the 13th ACM conference on Computer and communications security, 2006. P. 245-254.

21. Alber to Compagno, Mauro Conti, Daniele Lain, Gene Tsudik. Don't Skype & Type! Acoustic Eavesdropping in Voice-Over-IP. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017. P. 703-715. – URL: https://arxiv.org/pdf/1609.09359.pdf – (data obrashheniya: 16.09.2020).

22. Daniel Genkin, Adi Shamir, and Eran Tromer. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. Advances in Cryptology–CRYPTO 2014, 2014. P. 444-461

23. Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, Marco Gruteser. Snooping Keystrokes with mm-level Audio Ranging on a Single Phone. Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, 2015. P. 142-154.

24. Joe Loughry. Optical TEMPEST. 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), 2018. P. 172-177. – URL: https://arxiv.org/pdf/1808.07175.pdf – (data obrashheniya: 21.09.2020).

25. Arthur Costa Lopes, Diego F Aranha. Platform-agnostic Low-intrusion Optical Data Exfiltration. 3rd International Conference on Information Systems Security and Privacy (ICISSP), 2017. P. 474-480. – URL: https://www.scitepress.org/Papers/2017/62115/62115.pdf – (data obrashheniya: 27.09.2020).

26. J.-P. Power: Mind the gap: are air-gapped systems safe from breach-es? Symantec. 2015. – URL: http://www.symantec.com/connect/blogs/mind-gap-are-air-gapped-systems-safe-breache – (data obrashheniya: 09.09.2020).

27. Luke Deshotels. Inaudible Sound as a Covert Channel in Mobile De-vices. 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014. – URL: https://www.usenix.org/system/files/conference/woot14/woot14-deshotels.pdf – (data obrashheniya: 09.09.2020).

28. Michael Hanspach, Michael Goetz. On Covert Acoustical Mesh Net-works in Air. Journal of Communications, vol. 8, no. 11. P. 758-767, 2013. – URL: https://arxiv.org/abs/1406.1213 – (data obrashheniya: 10.10.2020).

29. Belyaev, D.O., Volchkov, D.N., Porshnev, S.V. O vozmozhnosti ispol'-zovaniya personal'nogo komp'yutera kak ustrojstva nesankcionirovannogo dostupa k rechevoj informacii. 2019, V : Vestnik UrFO. Bezopasnost' v infor-macionnoj sfere. 3 (33), str. 5-11.

30. Yisroel Mirsky, Mordechai Guri, Yuval Elovici. HVACKer: Bridging the Air-Gap by Attacking the Air

Conditioning System. arXiv preprint arXiv:1703.10454, 2017 – URL: https://arxiv.org/ftp/arxiv/papers/1703/1703.10454.pdf – (data obrashheniya: 11.05.2020).

31. Davide Balzarotti, Marco Cova, Giovanni Vigna. Clearshot: Eaves-dropping on keyboard input from video. 2008 IEEE Symposium on Security and Privacy (sp 2008), 2008. P. 170-183. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.413.9871&rep=rep1&type=pdf – (data obrashheniya: 20.10.2020).

32. Sebastian Zander, Philip Branch, Grenville Armitage. Capacity of temperature-based covert channels. IEEE communications letters, vol 15. P. 82-84. – URL: https://researchrepository.murdoch.edu.au/id/eprint/34937/1/capacity.pdf – (data obrashheniya: 17.09.2020).

33. Sriram Sami, Sean Rui, Xiang Tan, Yimin Dai, Nirupam Roy, Jun Han. LidarPhone: acoustic eavesdropping using a lidar sensor. Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems, 2020. P. 701-702 – URL: www.cs.umd.edu/~nirupam/images/2_publication/posters_demo/writeup /LidarPhone_poster_SenSys20_nirupam.pdf – (data obrashheniya: 23.11.2020).

34. Jun Han, Albert Jin Chung, and Patrick Tague. Pitchln: eavesdrop-ping via intelligible speech reconstruction using non-acoustic sensor fusion. Pro-ceedings of the 16th ACM/IEEE International Conference on Information Pro-cessing in Sensor Networks, 2017. P. 181-192. – URL: https: //doi.org/10.1145/3055031.3055088 – (data obrashheniya: 25.11.2020).

35. Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Rec-ognizing Speech from Gyroscope Signals. 23rd USENIX Security Symposium (USENIX Security 14), 2014. P. 1053-1067.

36. Nirupam Roy and Romit Roy Choudhury. Listening through a Vibra-tion Motor. Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services, 2016. P. 57-69. – URL: https://doi.org/10.1145/2906388.2906415 – (data obrashheniya: 30.11.2020).

37. Teng Wei, Shu Wang, Anfu Zhou, and Xinyu Zhang. Acoustic eaves-dropping through wireless vibrometry. Proceedings of the 21st Annual Interna-tional Conference on Mobile Computing and Networking, 2015. P. 130-141.

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

BELYAEV 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