Научная статья
УДК 004.56; DOI: 10.61260/2218-13X-2024-4-130-140

# ГАРМОНИЗАЦИЯ НОРМАТИВНЫХ ЦЕЛЕЙ ЗАЩИТЫ СЛУЖЕБНОЙ ИНФОРМАЦИИ В МЧС РОССИИ

✉**Метельков Александр Николаевич.**
**Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия**
✉***metelkov5178@mail.ru***

*Аннотация.* Защита служебной информации в МЧС России с начала 2022 г. обусловлена постоянным ростом кибератак на государственные и иные информационные системы. Все более актуальной становится задача обеспечения конфиденциальности, целостности и доступности информации в ведомственной цифровой информационной инфраструктуре не только от несанкционированного доступа, но и от различных силовых деструктивных дестабилизирующих воздействий и утечки информации по техническим каналам. Технические каналы могут использоваться для сбора необходимых данных для успешного проведения компьютерных атак на информационную инфраструктуру. Появляются ранее не характерные угрозы с использованием скрытых акустических каналов между изолированными системами, неслышимого ухом человека звука как скрытого канала в мобильных устройствах. В связи с появлением новых угроз, связанных с такой утечкой, представляется необходимым гармонизировать подходы к защите информации с учетом обобщения подходов, принятых в различных федеральных органах исполнительной власти и государственных корпорациях. Анализ нормативных правовых актов в различных ведомствах показывает усиление внимания к технической защите информации, поэтому при организации защиты информации ограниченного распространения в МЧС России важным является уточнение внутренних подходов к обеспечению ее безопасности.

*Ключевые слова:* защита, служебная информации, цели, технические каналы, утечка информации, угрозы, требования

**Для цитирования:** Метельков А.Н. Гармонизация нормативных целей защиты служебной информации в МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 4. С. 130–140. DOI: 10.61260/2218-13X-2024-4-130-140.

Scientific article

# HARMONIZATION OF REGULATORY OBJECTIVES FOR PROTECTING OFFICIAL INFORMATION IN THE EMERCOM OF RUSSIA

✉**Metel'kov Alexander N.**
**Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia**
✉***metelkov5178@mail.ru***

*Abstract.* The protection of official information in the EMERCOM of Russia since the beginning of 2022 is due to the constant increase in cyber attacks on government and other information systems. The task of ensuring the confidentiality, integrity and accessibility of information in the departmental digital information infrastructure is becoming increasingly urgent, not only from unauthorized access, but also from various destructive destabilizing effects of force and information leakage through technical channels. Technical channels can be used to collect the necessary data for successful computer attacks on the information infrastructure. Previously unknown threats are emerging with the use of hidden acoustic channels between isolated systems, inaudible to the human ear as a hidden channel in mobile devices. Due to the emergence of new threats associated with such leakage, it seems necessary to harmonize approaches to information protection, taking into account the generalization

of approaches adopted by various federal executive authorities and state corporations. An analysis of regulatory legal acts in various departments shows increased attention to the technical protection of information, therefore, when organizing the protection of information of limited distribution in the EMERCOM of Russia, it is important to clarify internal approaches to ensuring its security.

*Keywords:* protection, service information, goals, technical channels, information leakage, threats, requirements

**For citation**: Metel'kov A.N. Harmonization of regulatory objectives for the protection of official information in the EMERCOM of Russia // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 4. P. 130–140. DOI: 10.61260/2218-13X-2024-4-130-140.

## Введение

В условиях нарастания кибератак на критическую и иную инфраструктуру и включения информационной безопасности в число стратегических национальных приоритетов объективно существует потребность научного обоснования необходимости гармонизации целей защиты служебной информации ограниченного распространения (СИОР) в органах государства, в том числе в системе МЧС России. В литературе обращают внимание на «гармонизацию действующего правового обеспечения взаимодействия всех субъектов правоотношений, совершенствование условий их функционирования во всех режимах и на всех уровнях организации РСЧС»[1, с. 34].

Справедливо отмечает академик Российской академии наук Т.Я. Хабриева, что «нередко цели ведомственных актов не согласуются между собой, что приводит к вредным, не предусмотренным законом последствиям» [2, с. 24].

Под предметом гармонизации нормативных правовых актов в сфере обеспечения информационной безопасности понимаются общественные отношения, регулирование которых осуществляется соответствующими нормами, институтами и отраслями права. В связи со сложностью процесса гармонизации информационного права и широким кругом субъектов права, задействованных в информационной сфере, «важным является вопрос о координации деятельности по сближению систем национального права» [3, с. 39].

Расширение количества институционных механизмов обеспечения гармонизации и унификации нормативных правовых актов приводит к специализации большинства из таких механизмов, развитию различных форм взаимодействия и кооперирования в различных проектах в сфере информационной безопасности, а также дублированию, конкуренции и взаимной несогласованности разрабатываемых организационно-распорядительных документов и нормативных правовых актов.

Решающим фактором обеспечения эффективности гармонизации национального права в информационной сфере является его «единообразное толкование» [4, с. 13] особенно на уровне федеральных органов исполнительной власти при подготовке и утверждении подзаконных нормативных правовых актов. Эффективность гармонизации не всегда достигается в отдельных нормативных правовых актах. Рассмотрим это утверждение на примере защиты СИОР.

## Методы исследования

В работе использованы как общетеоретические методы анализа и синтеза, сравнения, противопоставления, так и частнонаучные междисциплинарные методы исследования, среди которых можно выделить декомпозицию целей как один из эффективных методов целеполагания в организации технической защиты информации ограниченного распространения.

## Организационно-технические аспекты защиты СИОР

Организация защиты СИОР определена приказом МЧС России от 14 октября 2019 г. № 581, в приложении № 4 к которому содержится описание целей защиты таких сведений. Анализ этих целей показывает (табл. 1), что они рассматриваются весьма узко по сравнению с нормами Федерального закона от 27 июля 2006 г. № 149-ФЗ (в ред. от 8 августа 2024 г.) «Об информации, информационных технологиях и о защите информации». Сопоставление с подобными актами ряда федеральных органов исполнительной власти позволяет выделить наиболее адекватную указанному закону формулировку целей защиты СИОР (табл. 2). Результаты анализа показывают, что в МЧС России в организации защиты СИОР из комплексной системы обеспечения безопасности информации выпало направление деятельности по предотвращению ее утечки и хищения по техническим каналам.

Таблица 1

**Сравнительно-правовой анализ целей защиты информации**

| Организация защиты СИОР (приложение № 4 к приказу МЧС России от 14 октября 2019 г. № 581) | Федеральный закон от 27 июля 2006 г. № 149-ФЗ |
|---|---|
| Целями защиты СИОР являются:<br>– предотвращение неправомерного (случайного) доступа неуполномоченных должностных лиц к СИОР;<br>– соблюдение конфиденциальности СИОР;<br>– обеспечение полноты, целостности и достоверности СИОР в системах подготовки, учета, хранения и обработки данных и документов;<br>– сохранение возможности управления процессом обработки и пользования СИОР | Статья 16. Защита информации<br>1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:<br>1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;<br>2) соблюдение конфиденциальности информации ограниченного доступа;<br>3) реализацию права на доступ к информации |

Основными элементами для описания угроз утечки данных по техническим каналам утечки информации (ТКУИ) являются: источник угрозы, среда распространения полезного сигнала и носитель защищаемой информации.

Декомпозиция целей защиты информации позволяет выделить наиболее значимые направления защиты информации (рис. 1).

Анализ показывает, что в МЧС России защиты СИОР направлена на предотвращение неправомерного (случайного) доступа неуполномоченных должностных лиц к СИОР, в то время как в Минюст России, Минтранс России, МВД России, Следственном комитете России и ряде других федеральных органах, Госкорпорации «Росатом» такая защита ориентирована на предотвращение утечки, хищения служебной информации, включая СИОР, по техническим каналам.

Современные методы несанкционированного добывания защищаемых сведений с ТКУИ учитывают характеристики среды распространения (физические препятствия, величина ослабления сигнала на единицу длины, частотные характеристики, вид и мощность помех). ТКУИ, возникающие за счёт наличия преобразовательных акустоэлектрических элементов в цепях различных технических устройств, находящихся в защищаемых помещениях объектов информатизации, представляют серьёзную опасность. Нарушитель может воспользоваться ими без проникновения в контролируемую зону и без установки подслушивающей аппаратуры. Известны способы несанкционированного получения информации об акустике помещения за счёт подсоединения к линии телефонных аппаратов,

линиям диспетчерской или громкоговорящей связи, вторичной часофикации и т.п. Подобные же каналы утечки информации могут быть созданы некоторыми устройствами охранной сигнализации на основе акустоэлектрических преобразователей.

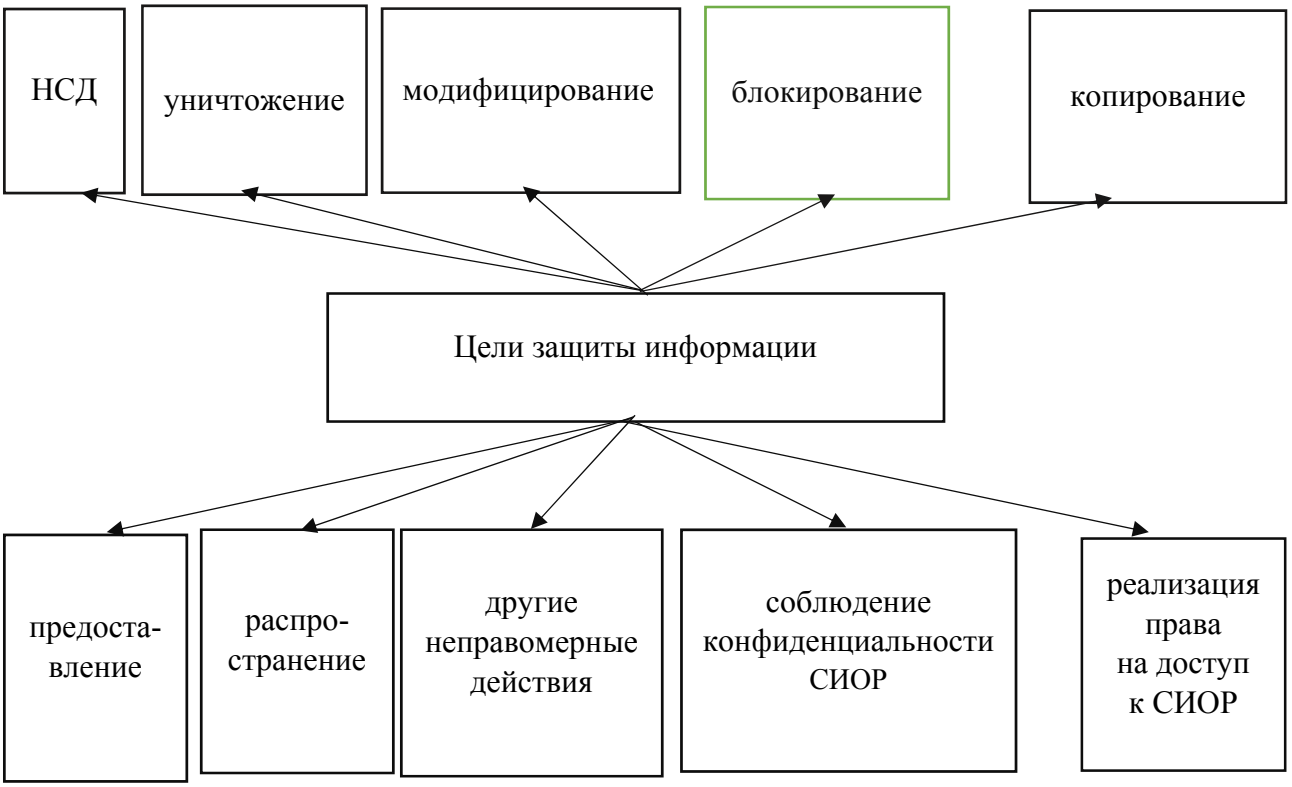


Рис. 1. **Декомпозиция целей защиты СИОР по критерию угроз (НДС – несанкционированный доступ)**

Определение наличия акустоэлектрических преобразователей в схеме и устройстве охранных (охранно-пожарных) извещателей свидетельствует о возможности создания канала утечки акустической информации из помещения, где расположены подобные извещатели. Результаты измерений извещателей (отечественных – ВМ-12, «Стекло-1», а также импортных DAM GS-360, Ademco 998L, Ademco 192SD/T) показали возможность создания ТКУИ из помещений. Очевидно, обеспечение противопожарной безопасности объектов не должно идти вразрез с их защитой от утечки речевой информации по акустопреобразовательному, а также электромагнитному каналу. При проведении мероприятий по защите информации необходимо учитывать и блокировать подобные ТКУИ [5, с. 111].

Канал утечки данных образуется в физической среде, в которой распространение СИОР не контролируется. Любая организация, использующая компьютеры, серверные стойки, сети, имеет ТКУИ. С их помощью злоумышленник может получить доступ к охраняемой государством и организацией тайне. Баланс мер защиты и угроз определяют безопасность информации в информационных системах.

Исследователями анализируются угрозы утечки данных из изолированных от внешнего мира компьютеров посредством шума вентиляторов, через светодиоды клавиатуры, с использованием скрытых акустических каналов между изолированными системами.

Одним из подходов к защите СИОР может служить так называемый «воздушный зазор» (air gap), с использованием которого осуществляется физическая изоляция сети от внешних сетей. Такие сети защищены от ряда сетевых угроз (удаленная эксплуатация,

заражение вредоносным программным обеспечением (ВПО), фишинговые атаки), минимизируются риски несанкционированного доступа и утечки данных.

Сети с воздушным зазором применяются для защиты критической информации в таких отраслях, как здравоохранение, финансы и оборона и др. Воздушный зазор позволяет предотвратить попытки киберпреступников получить удаленный доступ или организовать кибератаки на эти изолированные системы через сеть. Данная мера включает строгий контроль над обменом информацией между изолированными системами и окружающей средой, как правило, с использованием зашифрованных средств передачи данных (например, флеш-накопителей, оптических дисков и т.п.). Воздушный зазор нередко применяется для защиты информации в критически важной инфраструктуре для защиты систем управления от разрушительного воздействия компьютерных атак. Одновременно может быть запрещено или ограничено использование съемных носителей в сети и подключение к LAN или WAN. Для предотвращения несанкционированного доступа к информации в таких системах с воздушным разделением может применяться жесткий контроль доступа, например, биометрическая аутентификация и видеонаблюдение.

Сотрудником кафедры разработки программного обеспечения и информационных систем лаборатории Air-Gap Университета имени Бен-Гуриона (Израиль) М. Гури был представлен [6] новый тип атаки на системы с воздушным зазором, содержащие или обрабатывающие СИОР. Для обхода защиты воздушного зазора и формирования канала утечки данных через звук злоумышленники могут использовать компьютерные динамики. С целью защиты конфиденциальных данных от этой угрозы может быть введен «аудиоразрыв» – запрет на использование громкоговорителей или аудиооборудования. В статье «Атака PIXHELL: утечка конфиденциальной информации из компьютеров с воздушным зазором с помощью «поющих пикселей»» М. Гури продемонстрировал атаку по скрытому каналу, позволяющему злоумышленникам собирать утечки информации через шум, создаваемый без аудиооборудования или громкоговорителей пикселями на экране. ВПО в компьютерах с воздушным зазором и аудиоразрывом генерирует созданные пиксельные шаблоны, создающие помехи в диапазоне от 0 до 22 кГц. ВПО использует звук, возбуждаемый конденсаторами и катушками, для управления исходящими от экрана частотами. Акустические сигналы могут кодировать и передавать конфиденциальную информацию. Ученым представлена модель состязательной атаки, обсуждена генерация растровых изображений и коррелированных акустических сигналов с реализацией процессов модуляции и демодуляции, дана оценка скрытого канала и показаны итоги тестирования компьютеров с различными видами данных, а также сделаны выводы о возможных мерах защиты. Тестирование с использованием PIXHELL продемонстрировало возможность добывания полезной информации из автономных электронно-вычислительных систем на расстоянии 2 м с использованием модулированного с жидкокристаллических экранов звука. Для получения доступа к конфиденциальной информации в изолированных информационных системах злоумышленники используют методы обхода воздушного зазора с помощью социальной инженерии, физического внедрения, сбора и передачи акустических сигналов, использования работающего в режиме «воздушного зазора» ВПО [7], создания каналов утечки конфиденциальных данных из изолированных машин посредством перехвата скрытого шума вентиляторов графического процессора [8], утечка данных из защищенных клетками Фарадея изолированных компьютеров с помощью магнитных полей [9].

Нарушителем может быть осуществлено извлечение данных из изолированных компьютеров с помощью вибраций, с использованием скрытых акустических каналов между изолированными системами, за счет скрытой утечки данных с использованием световых и энергетических каналов, с применением методов извлечения данных из изолированных компьютеров с помощью вибраций, скрытых каналов между изолированными системами и находящимися рядом смартфонами, с использованием связи между динамиками и гироскопом, с помощью генерируемых процессором магнитных полей, утечка

конфиденциальных данных из изолированных от внешнего мира и звука систем путем превращения источников питания в динамики.

22 апреля 2023 г. в блоге компании Positive Technologies «На «воздушный зазор» надейся, а сам не плошай: история о радикальных мерах кибербезопасности» исследователи из Школы кибербезопасности Корейского университета в г. Сеуле описали новый вид атаки под названием «CASPER», осуществляемой по скрытому каналу. Атака позволяет передавать данные с компьютеров без внешних подключений. В качестве канала передачи данных используется подключенный к материнской плате компьютерный динамик. С помощью программного обеспечения внутренний спикер генерирует не слышимый человеком закодированный высокочастотный звук, способный транслироваться на внешний принимающий микрофон до полутора метров. При этом принимающий микрофон может находиться в смартфоне или ноутбуке. Для атаки нарушитель должен обладать физическим доступом к компьютеру и заразить его через USB-флеш-накопитель ВПО, которое автономно исследует файловую систему цели, находит файлы или типы файлов, которые его интересуют, и передает их на принимающее устройство. Из-за физических ограничений природы звука скорость передачи данных низкая: 8-символьный пароль передается примерно за три секунды, 2048-битный ключ RSA – за 100 сек., а на передачу документа Microsoft Word размером 10 КБ, в идеальных условиях без прерываний потребуется свыше часа. Одним из способов защиты от атаки является удаление внутреннего динамика из критически важных компьютеров и внедрение в них фильтров высоких частот для ограничения генерируемых частот в пределах слышимого звукового диапазона. В результате происходит блокирование передачи ультразвуковых сигналов. Потенциальные жертвы могут услышать процесс похищения их данных злоумышленником. В истории уже были резонансные инциденты с реализацией подобных «CASPER» атак, когда нарушители взламывали защиту и преодолевали «воздушный зазор» (червь Stuxnet, нацеленный на иранский завод по обогащению урана в г. Натанзе; вредоносная программа Agent.BTZ., заразившая военную базу США; модульный бэкдор Remsec, который ряд лет тайно собирал информацию из закрытых правительственных сетей в разных странах Европы). Вместе с тем применение «воздушного зазора» по-прежнему является одним из эффективных методов обеспечения кибербезопасности, так как для получения доступа к изолированным системам киберпреступникам необходимо преодолеть физические барьеры, препятствующие возможности проведения удаленных атак и снижению риска утечки информации через сетевые каналы [10].

В п. 2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (ГИС), утвержденных приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) России от 11 февраля 2013 г. № 17 установлены обязательные требования для федеральных органов исполнительной власти к обеспечению защиты информации ограниченного доступа от утечки по ТКУИ в ГИС. Поэтому в связи с распространением информационных технологий в территориальных органах, организациях и учреждениях МЧС России на основе знаний конкретных ТКУИ, обрабатываемой в информационной системе (ИС), необходимо применять в меры защиты от утечки по техническим каналам. Среди ТКУИ выделяют электромагнитные (перехват побочных электромагнитных излучений (ПЭМИ), перехват излучений на частотах работы высокоточных генераторов, перехват излучений на частотах возбуждения усилителей низкой частоты), параметрический (перехват информации путем высокочастотного облучения), электрические (съем информационных сигналов с линий электропитания (ТСПИ), цепей заземления основных (ОТСС) и вспомогательных (ВТСС) технических средств и систем, съем наводок с соединительных линий ВТСС и посторонних проводников с помощью аппаратных закладок).

Техническая защита информации путем перекрытия ТКУИ при ее обработке в ИС осуществляется с применением пассивных и активных методов. Пассивные методы направлены на:

– снижение ПЭМИ на границе контролируемой зоны объекта информатизации до безопасных величин, то есть до таких значений, при достижении которых исключается возможность выделения полезного сигнала средствами технической разведки;

– уменьшение наводок ПЭМИ в посторонних проводниках и соединительных линиях, выходящих за пределы контролируемой зоны, до безопасных величин;

– исключение или ослабление просачивания информационных сигналов в цепи электропитания, выходящих за пределы контролируемой зоны, до безопасных величин с помощью сетевых помехоподавляющих фильтров, устанавливаемых в сетях электропитания.

Пассивными методами технической защиты информации являются экранирование (электростатическое, магнитостатическое, электромагнитное), заземление и фильтрация (локализации) опасных сигналов. Среди пассивных методов защиты акустической информации выделяют звукоизоляцию.

Активные методы направлены на создание маскирующих пространственных электромагнитных помех. С помощью таких помех осуществляется снижение отношения сигнал/шум на границе контролируемой зоны или в посторонних проводниках и соединительных линиях с целью минимизации отношения сигнал/шум на границе контролируемой зоны до безопасных величин. В числе активных методов защиты информации применяется зашумление (маскирование информационного сигнала помехами, близкими по спектру к полезному сигналу). Для защиты СИОР используются средства активной защиты информации от утечки за счет наводок информационного сигнала по цепи заземления и электропитания (например, «Соната-РС3» и др.), по цепи электропитания 220 В и для противодействия несанкционированному съему информации по каналам ПЭМИ (например, ЛГШ-505) путем создания широкополосной шумовой электромагнитной помехи.

Источниками угроз утечки информации по техническим каналам являются субъекты, не имеющие доступа к ИС, а также зарубежные спецслужбы или террористические организации, криминальные группировки, осуществляющие перехват информации техническими средствами. Утечка информации может быть в документированной, телекоммуникационной, акустической (речевой) форме ее представления.

Следует подчеркнуть, что в научной и учебной технической литературе нет единства взглядов на названия одних и тех же каналов. Например, А.А. Хорев канал, образуемый при облучении лазерным лучом в ИК-диапазоне вибрирующих в акустическом поле тонких отражающих поверхностей (например, стекол), называет акустооптическим или лазерным [11]. Горбатов В.С., Зайцев А.П., Королев В.И., Малюк А.А., Мещеряков Р.В., Шелупанов А.А. и другие специалисты именуют «канал утечки информации, образуемый путем облучения лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей … оптико-электронным» [12].

ТКУИ представляют собой совокупность носителя информации, физической среды распространения информативного сигнала и средств добывания защищаемой информации. Классификация ТКУИ представлена на рис. 2. Среда распространения информативного сигнала может быть однородной (воздушная среда, металлоконструкции) и неоднородной (при переходе сигнала из одной среды в другую).

Результаты измерений пожарных извещателей показали «возможность создания технических каналов утечки информации из помещений, к которых они установлены» [4, с. 12]. При этом комплекс мер по обеспечению противопожарной безопасности должен коррелировать с принятием мер по технической защите информации, включая меры по защиты от утечки речевой информации по акустопреобразовательному и электромагнитному каналам.

Таблица 2

**Цели защиты СИОР (сравнительный анализ выделенных направлений)**

| Приложение № 4 к приказу МЧС России от 14 октября 2019 г. № 581 | Приложение № 4 к приказу Минюста Российской Федерации от 7 октября 2010 г. № 250 | Приложение к приказу МВД России от 9 ноября 2018 г. № 755 | Приложение № 4 к приказу Минобрнауки России от 13 июня 2023 г. № 598 |
|---|---|---|---|
| В качестве цели предотвращение утечки, хищения СИОР по техническим каналам не указано | Предотвращение утечки, хищения служебной информации по техническим каналам | Предотвращение утечки, хищения СИОР по техническим каналам | Предотвращение утечки, хищения служебной информации по техническим каналам |

В руководящем документе ФСТЭК России под утечкой информации по техническим каналам понимается «неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации. Классификация таких угроз включает угрозы утечки информации по техническим каналам и угрозы утечки речевой информации, угрозы утечки визуальной информации, угрозы утечки информации по каналам ПЭМИ и наводок» [13].

В зависимости от физической природы сигналы распространяются в материальных средах. Например, между двумя близкорасположенными электроцепями могут возникать нежелательные электромагнитные связи, наличие которых приводит к появлению наводок сигналов, циркулирующих как в цепи источника, так и в цепи рецептора наводки. Такие связи возникают за счет электромагнитного поля, ближних электрического и магнитного полей, а также соединительные провода, кабели и волноводы, цепей электропитания, заземления и других токоведущих компонентов.


Рис. 2. **Классификация ТКУИ**
**(СВТ – средства вычислительной техники)**

На небольших расстояниях возможно появление всех видов нежелательной связи. Увеличение расстояния приводит к ослаблению и исчезновению связи через ближнее электрическое и магнитное поля, а на больших расстояниях также через электромагнитное поле излучения.

С точки зрения технической разведки информативными носителями являются акустические сигналы, источниками которых являются органы речи, а вторичными – преобразователи (микрофоны, телефоны и др.), а также электромагнитное, радиоактивное излучения, а также химические выбросы в различные среды при функционировании объектов технической разведки.

## Заключение

Использование специальных технических средств и методов для несанкционированного доступа к защищаемой информации предполагает применение технических каналов утечки информации. Технические каналы утечки информации ограниченного распространения и доступа в современных условиях требуют реализации мер по их выявлению и перекрытию с применением организационных и технических средств. К числу основных объектов защиты информации ограниченного доступа относятся информационные ресурсы, основные и вспомогательные технические средства и системы, а также помещения, в которых они размещены и где обрабатывается такая информация.

Резюмируя изложенное, можно утверждать, что предотвращение утечки, хищения СИОР по техническим каналам является актуальным направлением защиты информации, на котором следует сконцентрировать ведомственные усилия в МЧС России.

***Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России НИР «Разработка принципов, методологии и элементов технологии решения прикладных задач гармонизации нормативной правовой базы в части требований информационной и кибербезопасности в интересах МЧС России» (НИР «Гармония»).***

**Список источников**

1. Гордиенко А.Н. Конституционные основы предотвращения чрезвычайных ситуаций // Право. Безопасность. Чрезвычайные ситуации. 2024. № 2. С. 27–38.

2. Хабриева Т.Я. Избранные труды: в 10 т. Т. 6: Теория толкования права. Теория правотворчества. Концепции развития законодательства. М., 2018. 472 с.

3. Бахин С.В. Сотрудничество государств по сближению национальных правовых систем (унификация и гармонизация права): автореф. дис. ... д-ра юрид. наук. СПб., 2003. 46 с.

4. Халяпин Д.Б., Терентьев Е.Б. Технические каналы утечки речевой информации через извещатели охранно-пожарной сигнализации // Известия ЮФУ. Технические науки. 2003. № 4. С. 110–111.

5. License: arXiv.org perpetual non-exclusive license arXiv:2409.04930v1 [cs.CR] 07 Sep 2024 // https://arxiv.org/html/2409.04930v1.

6. Guri M., Elovich Y. Bridgeware: Air-gapped malware. Commun. ACM, March 2018. № 61 (4). P. 74–82.

7. Guri M. Gpu-fan: Leaking sensitive data from isolated machines via hidden GPU fan noise. In Nordic Conference on Secure IT Systems, Springer, 2022. P. 194–211.

8. На «воздушный зазор» надейся, а сам не плошай: история о радикальных мерах кибербезопасности. Блог компании Positive Technologies. 22 апреля 2023 г. URL: https://smart-lab.ru/company/positive-technologies/blog/897260.php (дата обращения: 18.11.2024).

9. Guri M., Zadov B., Elovich Y. Odiny: Leaking sensitive data from isolated Faraday cage computers using magnetic fields // IEEE. Transactions on Information Forensics and Security, 2019. Vol. 15. P. 1190–1203.

10. Хорев А.А. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники // Специальная Техника. № 2. 2010. С. 39–57.

11. Технические средства и методы защиты информации: учеб. для вузов / А.П. Зайцев [и др.]; под ред. А.П. Зайцева, А.А. Шелупанова. М.: ООО Изд-во «Машиностроение», 2009. 507 с.

12. Введение в информационную безопасность: учеб. пособие / А.А. Малюк [и др.]; под ред. В.С. Горбатова. М.: Горячая линия – Телеком, 2018. 288 с.

13. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка), утв. заместителем директора ФСТЭК России 15 февраля 2008 г. URL: http://https://normativ.kontur.ru/document?moduleId=1&documentId=204882 (дата обращения: 28.12.2024).

**References**

1. Gordienko A.N. Konstitucionnye osnovy predotvrashcheniya chrezvychajnykh situacij // Pravo. Bezopasnost'. Chrezvychajnye situacii. 2024. № 2. S. 27–38.

2. Khabrieva T.Ya. Izbrannye trudy: v 10 t. T. 6: Teoriya tolkovaniya prava. Teoriya pravotvorchestva. Koncepcii razvitiya zakonodatel'stva. M., 2018. 472 s.

3. Bakhin S.V. Sotrudnichestvo gosudarstv po sblizheniyu nacional'nykh pravovykh sistem (unifikaciya i garmonizaciya prava): avtoref. dis. ... d-ra yurid. nauk. SPb., 2003. 46 s.

4. Khalyapin D.B., Terent'ev E.B. Tekhnicheskie kanaly utechki rechevoj informacii cherez izveshchateli okhranno-pozharnoj signalizacii // Izvestiya YuFu. Tekhnicheskie nauki. 2003. № 4. S. 110–111.

5. License: arXiv.org perpetual non-exclusive license arXiv:2409.04930v1 [cs.CR] 07 Sep 2024 // https://arxiv.org/html/2409.04930v1.

6. Guri M., Elovich Y. Bridgeware: Air-gapped malware. Commun. ACM, March 2018. № 61 (4). R. 74–82.

7. Guri M. Gpu-fan: Leaking sensitive data from isolated machines via hidden GPU fan noise. In Nordic Conference on Secure IT Systems, Springer, 2022. R. 194–211.

8. Na «vozdushnyj zazoR» nadejsya, a sam ne ploshaj: istoriya o radikal'nykh merakh kiberbezopasnosti. Blog kompanii Positive Technologies. 22 aprelya 2023. URL: https://smart-lab.ru/company/positive-technologies/blog/897260.php (data obrashcheniya: 18.11.2024).

9. Guri M., Zadov B., Elovich Y. Odiny: Leaking sensitive data from isolated Faraday cage computers using magnetic fields // IEEE. Transactions on Information Forensics and Security, 2019. Vol. 15. R. 1190–1203.

10. Khorev A.A. Tekhnicheskie kanaly utechki informacii, obrabatyvaemoj sredstvami vychislitel'noj tekhniki // Special'naya Tekhnika. № 2. 2010. S. 39–57.

11. Tekhnicheskie sredstva i metody zashchity informacii: ucheb. dlya vuzov / A.P. Zajcev [i dr.]; pod red. A.P. Zajceva, A.A. Shelupanova. M.: OOO Izd-vo «MashinostroeniE», 2009. 507 s.

12. Vvedenie v informacionnuyu bezopasnost': ucheb. posobie / A.A. Malyuk [i dr.]; pod red. V.S. Gorbatova. M.: Goryachaya liniya – Telekom, 2018. 288 s.

13. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informacionnykh sistemakh personal'nykh dannykh (vypiska), utv. zamestitelem direktora FSTEHK Rossii 15 fevralya 2008 g. URL: http://https://normativ.kontur.ru/document?moduleId=1&documentId=204882 (data obrashcheniya: 28.12.2024).

**Информация о статье:**
Статья поступила в редакцию: 08.12.2024; одобрена после рецензирования: 22.12.2024;
принята к публикации: 26.12.2024
**Information about the article:**
The article was submitted to the editorial office: 08.12.2024; approved after review: 22.12.2024;
accepted for publication: 26.12.2024

*Сведения об авторах*:
**Метельков Александр Николаевич**, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат юридических наук, e-mail: metelkov5178@mail.ru, https://orcid.org/0000-0002-6113-8981, SPIN-код: 5990-6833

*Information about the authors:*
**Metelkov Alexander N.**, associate professor of the department of applied mathematics and information technologies Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of law, e-mail: metelkov5178@mail.ru, https: //orcid.org/0000-0002-6113-8981, SPIN: 5990-6833