Шерешева Марина Юрьевна, д.э.н., профессор

(МГУ имени М.В. Ломоносова)

Малков Павел Борисович

независимый эксперт

**Проблема информационной безопасности и возможности защиты объектов информатизации в государственных органах исполнительной власти Российской Федерации**

Современные реалии общественного развития ставят перед государствами новые задачи. В частности, невозможно отрицать ключевую роль информационных технологий в повышении эффективности работы органов государственного управления.[[1]](#footnote-1) В то же время, быстрая конвергенция информационных и коммуникационных технологий и возникновение вследствие этого сложных информационных инфраструктур создают не только новые возможности, но и проблемы – как в бизнесе, так и в государственном управлении.[[2]](#footnote-2)

Одной из наиболее острых проблем является обеспечение эффективной и безопасной работы государственных органов в условиях трансформации, вызванной растущим распространением интегрированных информационных систем. В условиях стремительной информатизации среда принятия решений в государственном управлении во многом определяется обеспечением информационных процессов, представляющих жизненный цикл информации, от сбора данных, их хранения и обработки до принятия решения на основании полученной информации.[[3]](#footnote-3) На каждом из этих этапов существует опасность случайных или преднамеренных воздействий, способных нанести ущерб обладателям или пользователям информации.[[4]](#footnote-4)

Отсюда, важнейшим условием информатизации органов государственной и муниципальной власти, которая является одной из приоритетных задач руководства нашей страны, является информационная безопасность, под которой понимается защищенность информации и поддерживающей инфраструктуры от соответствующих случайных и преднамеренных воздействий.[[5]](#footnote-5)

Защита информации - достаточно многогранный элемент борьбы с противником, включающей в себя физическую и экономическую сторону, а в современных условиях – также защиту информации, хранящейся на физических носителях, применяемых в электронных вычислительных машинах (ЭВМ), и циркулирующей в вычислительных сетях. Другими словами, вопросы защиты информации касаются любых сведений (сообщений, данных) независимо от формы их представления, включая акустическую (речевую) и видовую информацию, а также информацию, обрабатываемую в информационной системе в виде электрических, электромагнитных, оптических сигналов, а также в виде бит, байт, IP-протоколов, файлов и других логических структур.

В данной статье будут рассмотрены вопросы, касающиеся обеспечения защиты от утечки информации по техническим каналам в государственных органах исполнительной власти.[[6]](#footnote-6)

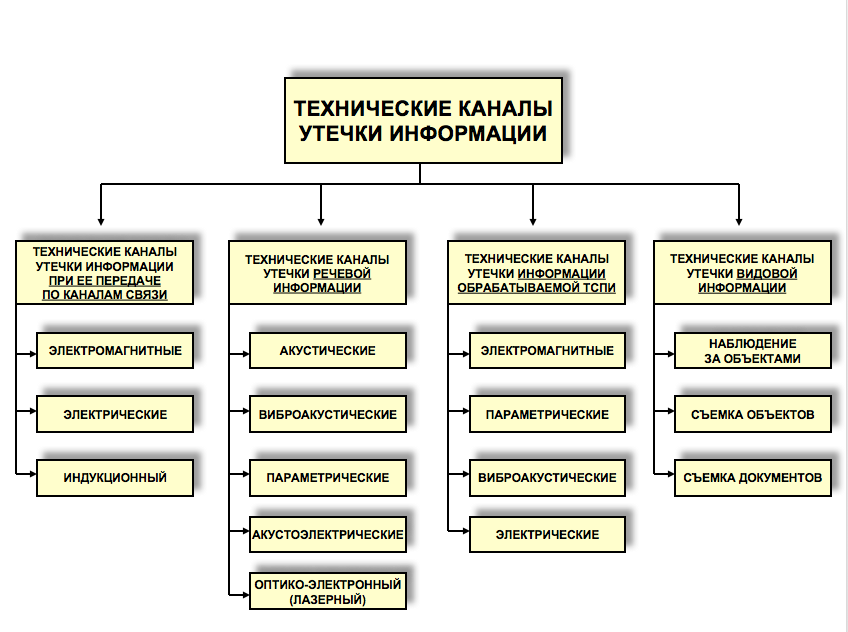
**Моделирование технических каналов утечки информации как основа обеспечения информационной безопасности**

При работе с любой информацией всегда есть процесс передачи информации, в частности, обсуждение чего-либо при встрече союзников, коллег, партнёров. Данный вид передачи информации называется речевой информацией или речевым сигналом. В общем виде речевой сигнал выглядит как волновой процесс (звуковая волна), в результате которого возникают вторичные источники передачи информации (вибрационные), которые, в свою очередь, позволяют услышать конфиденциальную информацию за пределами переговорного помещения.

Защита конфиденциальных переговоров обеспечивается различными мероприятиями, комплексами средств и систем, которые препятствуют распространению конфиденциальной информации за пределами защищаемых помещений и информационных автоматизированных систем (ИАС).

Одним из первых шагов на пути обеспечения информационной безопасности объекта является изучение и моделирование *технических каналов утечки информации* (ТКУИ).[[7]](#footnote-7) Они делятся на четыре типа: ТК утечки информации при ее передаче по каналам связи, ТК утечки речевой информации, ТК утечки видовой информации, ТК утечки информации, обрабатываемой ТСПИ[[8]](#footnote-8). В свою очередь, каждый из этих типов можно условно разделить на подтипы (рис. 1 - 4).

При разработке комплекса мер по обеспечению защиты от утечки информации необходимо учитывать все типы ТКУИ для обеспечения максимальной защиты информации при проведении работ в защищаемом помещении.



**Рис. 1. Технические каналы утечки информации**

Источник: составлено автором



**Рис. 2. Технические каналы утечки акустической информации**

Источник: составлено автором

****

**Рис. 3. Технические каналы утечки, обрабатываемые ТСПИ.**

Источник: составлено автором



**Рис. 4. Наглядный вид технических каналов утечки информации, обрабатываемой ТСПИ.**

Источник: составлено автором

**Модель угроз и реализация методов защиты на объекте информатизации**

Для точного определения методов и способов защиты информации необходимо иметь частную модель угроз.

При определении угроз безопасности конфиденциальной информации и формировании частной модели угроз актуальными являются:

* угрозы утечки акустической речевой информации;
* угрозы утечки видовой информации;
* угрозы утечки информации по каналам ПЭМИН[[9]](#footnote-9).

*Защита акустической речевой информации*

При передаче акустической речевой информации по каналам связи необходимо исключить передачу информации по открытым проводным каналам связи, выходящим за пределы контролируемой зоны, и открытым радиоканалам. Для обеспечения режима защиты необходимо как минимум использовать защищенные линии связи.

В случае необходимости проведении звуко- и видеозаписи конфиденциальной информации рекомендуется:

* производить данные работы только в защищённом помещении;
* после окончания звуко- и видеозаписи конфиденциальной информации все носители информации необходимо учитывать и хранить в установленном порядке, в соответствии с классом защиты информации;
* назначить должностное лицо, ответственное за хранение и использование аппаратуры записи информации;
* обеспечить хранение и использование этой аппаратуры, исключающее несанкционированный доступ к ней.

*Защита видовой информации*

Для обеспечения данного вида угроз необходимо исключить возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей данные ограниченного распространения. Для чего необходимо правильное размещение устройств вывода информации СВТ[[10]](#footnote-10), информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИС.

*Методы и средства защиты от ПЭМИН:*

* использование технических средств в защищенном исполнении;
* использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
* размещение объектов защиты в соответствии с предписанием на эксплуатацию;
* размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
* обеспечение развязки цепей электропитания ОТСС[[11]](#footnote-11) с помощью защитных фильтров, блокирующих информативный сигнал;
* обеспечение электромагнитной развязки между линиями связи и другими цепями ВТСС, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Для обеспечения защиты информации от утечки по ТКУИ разработаны специальные технические средства, позволяющие блокировать или вносить помехи в линию связи. Список этих средств является достаточно обширным, конкретные средства и системы определяются при построении системы активной защиты в защищаемом помещении (ЗП).

Все работы по защите ЗП (на этапах проектирования, строительства или реконструкции, монтажу оборудования и аппаратуры защиты информации, аттестации ЗП) осуществляют организации, имеющие лицензию на деятельность в области защиты информации - в частности, лицензию ТЗКИ[[12]](#footnote-12), выдаваемую Федеральной службой по техническому и экспортному контролю  (ФСТЭК).[[13]](#footnote-13) Исключение составляют работы, проводимые для собственных нужд организации, однако при этом специалисты, проводящие данные работы, должны обладать соответствующими знаниями по защите информации.

Применяемое оборудование и программное обеспечение должно соответствовать требованиям руководящих документов РФ по защите информации и иметь соответствующие сертификаты по безопасности.

При вводе защищаемого помещения в эксплуатацию должна проводиться его аттестация по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.[[14]](#footnote-14) Периодически, не реже одного раза в год, должно проводиться его специальное обследование.

*Пользователями объекта информатизации* являются субъекты доступа ‑ сотрудники органа исполнительной власти Российской Федерации.

В качестве *информационных ресурсов* рассматриваются:

* двоичные и текстовые данные, содержащие информацию о состоянии объектов и субъектов в виде файлов-контейнеров или сетевых пакетов;
* двоичные и текстовые данные, содержащие информацию об управлении объектами и субъектами в виде сетевых пакетов;
* прочие материальные объекты, в том числе физические поля, в которых информация (сведения) находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

В качестве владельца информационных ресурсов рассматривается субъект доступа должностное лицо или организация, создавший информационный ресурс или получивший его от другого субъекта доступа.

Уровень доступа (гриф секретности), обрабатываемой на объекте информатизации, определяется субъектами доступа в соответствии с законодательством Российской Федерации.[[15]](#footnote-15)

***Типы нарушителей безопасности информации***

Нарушителем безопасности информации комплекса средств автоматизации (КСА) объекта информатизации могут являться лицо или группа лиц, имеющие своей целью нанесение ущерба владельцам информационных ресурсов путем преодоления (нарушения) целевых функций средств защиты информации, для нарушения конфиденциальности, целостности, доступности и достоверности информации.

Модель нарушителя для КСА базируется на следующих принципах:

* все информационные ресурсы рассматриваются, как имеющие уровень доступа – «Для служебного пользования»;
* безопасность данных в КСА обеспечивается организационными мерами, средствами защиты информации (СЗИ), средствами криптографической защиты информации (СКЗИ), а также используемыми информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям к КСА по защите информации;
* СЗИ и СКЗИ не могут обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (то есть защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

Нарушитель безопасности КСА может преследовать следующие цели:

* получение акустической информации, содержащей информацию, передаваемую при обсуждении сведений конфиденциального характера;
* получение видовой информации с дисплеев КСА;
* получение информационного содержания КСА (файлов, томов, СУБД) - как полного, так их части;
* искажение (замена, уничтожение) информационного содержания КСА (файлов, томов, СУБД) - как полностью, так частично;
* нарушение функционирования КСА.

Все физические лица, имеющие доступ к КСА, могут быть отнесены к двум категориям:

* Категория I - лица, не имеющие права доступа в контролируемую зону КСА;
* Категория II - лица, имеющие право постоянного или разового доступа в контролируемую зону КСА.

К лицам категории II относятся:

* лица, являющиеся пользователями КСА;
* лица, не являющиеся пользователями КСА, но имеющие право постоянного или разового доступа в помещения, с целью выполнения своих должностных обязанностей. К данной категории относится персонал, обслуживающий помещения в которых располагаются КСА (уборщицы, электрики, охранники и т.п.), сотрудники организаций, обеспечивающие установку и эксплуатацию средств связи, сотрудники экстренных служб (пожарные и т.п.) работники учреждений, осуществляющих сервисное обслуживание и ремонт КСА;
* иные лица (посетители).

Все потенциальные нарушители подразделяются на *внешних нарушителей*, осуществляющих атаки из-за пределов контролируемой зоны объектов размещения КСА, и *внутренних нарушителей*, осуществляющих атаки, находясь в пределах контролируемой зоны.

Внешними нарушителями могут быть как лица категории I, так и лица категории II, находящиеся в момент проведения атаки за пределами контролируемой зоны. Внутренними нарушителями могут быть только лица категории II.

***Внутренний нарушитель*** скрывает свои несанкционированные действия. Его возможности существенным образом зависят от ограничительных факторов, действующих в пределах контролируемой зоны, из которых основными являются организационно-технические меры, направленные на:

* предотвращение и пресечение несанкционированных действий;
* допуск физических лиц в контролируемую зону КСА;
* контроль порядка проведения работ;
* подбор, расстановку и обучение кадров.

Внутренние нарушители *первого типа* - лица, являющиеся пользователями КСА. Их действия строго регламентированы инструкциями и сопровождаются регистрацией в системных и электронных журналах.

Персонал, обслуживающий КСА и допущенный к КСА после оформления соответствующих допусков, наделяется правами и обязанностями в соответствии с законодательством Российской Федерации и организационно-распорядительной документацией. Указанные лица обладают всеми необходимыми навыками и не должны совершать непреднамеренные действия, представляющие собой угрозу конфиденциальности и достоверности информации.

Кроме того, возможное непреднамеренное нарушение прав доступа пользователями КСА к защищаемой информации исключается реализованным комплексом организационно-технических мер защиты (в том числе с использованием общесистемного и прикладного программного обеспечения, прошедшего исследования на отсутствие недекларированных возможностей).

В обязанности указанных лиц включены требования по соблюдению или обеспечению правил работы с информационными ресурсами органа исполнительной власти.

Таким образом, пользователи КСА не рассматриваются как нарушители безопасности информации.

Внутренние нарушители *второго типа* - физические лица (группа лиц), находящиеся внутри помещений, в которых размещается КСА, но не являющиеся пользователями КСА и не имеющие санкционированного доступа к КСА. Нарушитель данного типа самостоятельно создаёт методы и средства реализации атак, и реализует их.

Доступ в помещения с КСА и к самим СЗИ строго ограничен и осуществляется только в присутствии и под контролем пользователей КСА.

Внутренние нарушители *третьего типа* - работники учреждений, осуществляющих сервисное обслуживание и ремонт КСА.

Внутренние нарушители *четвертого типа* – иные лица (посетители, соискатели на должности, представители иных организаций).

Данные лица не имеют доступ к КСА. Нахождение лиц данной категории в контролируемой зоне осуществляется под постоянным наблюдением сопровождающих. Соответственно, лица данной категории не рассматриваются в качестве нарушителей безопасности информации.

Учитывая состав обрабатываемой информации в органе исполнительной власти, в качестве ***внешнего нарушителя*** могут выступать как отдельные физические лица, действующие в личных интересах и самостоятельно осуществляющие создание способов атак, их подготовку и проведение, так и группы лиц, с привлечением научно-исследовательских организаций и групп специалистов, а также специальных служб иностранных государств.

Внешний нарушитель не имеет непосредственного доступа к КСА. Этот нарушитель может осуществлять атаки только с территории, расположенной вне контролируемой зоны и по каналам связи. Он может осуществлять атаки на каналы связи, выходящие за пределы контролируемой зоны, посредством:

* перехвата информации и последующего ее анализа;
* уничтожения, модификации и блокирования информации;
* навязывания ложной информации;
* реализации попыток преодоления средств защиты.

Предполагается, что нарушитель обладает всей информацией, необходимой для подготовки и проведения атак на КСА, за исключением информации, доступ к которой со стороны нарушителя исключается СЗИ КСА, а также применением комплекса организационно-технических мер. К такой информации может относиться парольная, аутентифицирующая и ключевая информация.

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

В качестве исходной информации нарушитель располагает:

* данными об организации работы, структуре и используемом оборудовании КСА;
* сведениями об открытой информации (характерные особенности информационного обмена, форматы сообщений, протоколы информационного обмена, статистические свойства информации и потока сообщений) в объемах, приведенных в открытых источниках и в эксплуатационной документации на КСА;
* описанием используемых в КСА алгоритмов;
* доступными в свободной продаже СЗИ с технической и эксплуатационной документацией к ним.

## ***Виды угроз безопасности информации***

1. *Угрозы утечки информации по техническим каналам*

С учётом различного состава оборудования для разных вариантов комплектования КСА, угрозы утечки акустической (речевой) информации будут актуальны при применении средств телефонной связи, видеоконференцсвязи, или при проведении совещаний. Угрозы утечки информации от ПЭМИН будут всегда при применении не специализированных персональных ЭВМ и КСА.

1. *Угрозы несанкционированного доступа (НСД)[[16]](#footnote-16)*

Угрозы НСД в КСА с применением программных и программно-аппаратных средств реализуется при осуществлении НСД, в том числе случайного, в результате которого осуществляется нарушение конфиденциальности (копирование, несанкционированное распространение), целостности (уничтожение, изменение) или доступности (блокирование) информации. Сюда включаются угрозы внедрения (в том числе по сети) вредоносных программ, и угрозы НСД, связанные с действиями нарушителей, имеющих доступ к программно-техническим средствам КСА (ПТС КСА), реализующих угрозы непосредственно в КСА.[[17]](#footnote-17)

Исходя из модели угроз, система обеспечения безопасности информации должна решать следующие задачи:

* обеспечение безопасности информации при передаче (обсуждении) конфиденциальных сведений, в защищаемых помещениях (акустическую информацию);
* обеспечение безопасности информации при обработке конфиденциальных сведений (видовую информацию);
* обеспечение безопасности информации при её передаче по каналам связи;
* обеспечение безопасности функционирования средств передачи данных, систем управления, средств и систем защиты информации.

Обеспечение информационной безопасности в защищаемом помещении предусматривает оснащение помещения средствами активной защиты, системами контроля доступа и дополнительными средствами защиты в соответствии с СТР-К[[18]](#footnote-18).

Как уже отмечено выше, пользователи КСА (нарушители первого типа) не являются нарушителями безопасности информации. Для обеспечения безопасности от нарушителей второго типа применяются меры защиты от преднамеренных воздействий и включают административные и технические меры. В частности, организация режима посещения контролируемой зоны в виде ограничения доступа физических лиц в помещения в которых размещается оборудование КСА и проводятся конфиденциальные переговоры.

На объекте органа исполнительной власти должна быть издана организационно-распорядительная документация, регламентирующая допуск лиц в контролируемую зону.

Противодействие перехвату информации с носителей конфиденциальной информации, в виде сигналов (электромагнитных излучений) от оборудования должно осуществляться за счет его размещения, с учетом размеров зон, указанных в предписаниях на эксплуатацию оборудования, а также с применением средств активной защиты.

Все нарушения, выявленные при реализации функций защиты информации, должны фиксироваться в журналах, для последующего принятия мер по ликвидации источника угроз и последствий нарушения.

***Организационные мероприятия по защите информации от утечки по техническим каналам***

К основным организационным мероприятиям по защите речевой информации от утечки по техническим каналам относятся:

* выбор помещений для ведения конфиденциальных переговоров
* категорирование ЗП
* использование в ЗП сертифицированных ОТСС и ВТСС[[19]](#footnote-19)
* установление контролируемой зоны вокруг ЗП
* организация режима и контроля доступа в ЗП
* отключение при проведении конфиденциальных переговоров незащищенных ВТСС
* При необходимости производится демонтаж незадействованных ВТСС, их соединительных линий и посторонних проводников в ЗП

Работы по подготовке помещения должны быть проведены в соответствии с СТР-К раздел 4. «Требования и рекомендации по защите речевой конфиденциальной информации»[[20]](#footnote-20), и учитывать локальные нормативные акты органа исполнительной власти.

При подготовке помещения допускается установка однорамных шумозащитных двухкамерных сертифицированных стеклопакетов по ГОСТ 24866-99, оборудованных средствами активной защиты от утечки речевой информации по акустическому и вибрационному каналам (при необходимости), сертифицированными по требованиям безопасности информации в ФСТЭК России, а также шторами (жалюзи), не пропускающими свет и закрывающими оконные проемы. Для обеспечения необходимых звуко- и виброизолирующих свойств окон не допускается нарушение их конструкции, в том числе установка оконных кондиционеров.

Средства вычислительной техники, устанавливаемые в защищаемом помещении, должны соответствовать требованиям руководящих документов в соответствии с установленным классом ЗП. Телефонные аппараты, устанавливаемые в ЗП, должны быть отечественного производства из состава рекомендованных к применению, либо соответствовать одному из требований:

* наличие сертификата соответствия требованиям безопасности информации;
* пройти специальные исследования с целью определения их возможности установки в защищаемых помещениях соответствующей категории.

Телефонные аппараты иностранного (совместного) производства, кроме того, должны пройти специальную проверку на наличие возможно внедренных устройств перехвата (уничтожения) информации в организациях, имеющих лицензии ФСБ России.

В помещении должна быть обеспечена защита оконечных устройств телефонной связи, линии которых имеют прямой выход за пределы контролируемой зоны, путем установки на их линиях сертифицированных устройств защиты. В качестве устройств защиты могут быть использованы устройства защиты, имеющие сертификат ФСТЭК России на право использования их для защиты телефонных аппаратов, установленных в защищаемых помещениях соответствующей категории.

При использовании фальшстен, подвесных потолков, систем вентиляции, ниш для межкомнатных коммуникаций и т.п. должна обеспечиваться невозможность проникновения в помещение при их использовании путем установки внутренних стальных решеток, аналогично оконным.

По результатам подготовки помещений должен быть документально определен перечень защищаемых помещений и лиц, ответствен­ных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на эти помещения.

***Пример применения средств защиты информации***

План-схема размещения помещения и границы контролируемой зоны приведены на рис. 5 (на рисунке красными линиями показано здание с ЗП, синим цветом показана граница контролируемой зоны). План помещения показан на рис. 6. Защищаемое помещение находится в пределах контролируемой зоны, на четвёртом этаже девятиэтажного офисного здания. Здание и контролируемая территория принадлежат одной организации. Окна ЗП выходят на фасад здания ориентированный на проезжую часть. Окна оборудованы жалюзи. Вокруг контролируемой зоны расположены другие здания и сооружения, этажностью от 3-х то 12-ти. От границы фасада здания до границы контролируемой зоны расстояние составляет 10 метров. ЗП по периметру имеет границу с соседним кабинетом и коридором. В помещении установлен кондиционер (индивидуальная сплит-система), системы охранно-пожарной сигнализации, система звукового оповещения. Помещение оборудовано системой центрального отопления. В кабинете установлена мебель, сейф, организовано рабочее место должностного лица с персональными ЭВМ и телефонами. На одной из стен помещения расположен кабель‑канал для организации ввода‑вывода кабелей в общую систему кабель‑каналов для организации Структурированной Кабельной Сети (далее - СКС) предприятия. Система электропитания в кабинете выполнена с применением одного ввода. Стены и перекрытия выполнены из железобетона толщиной 200 мм.

В результате обследования предполагаемого помещения для выполнения работ по обеспечению защиты от утечки по ТКУИ можно сделать вывод, что строительная подготовка помещения соответствует требованиями СТР-К.

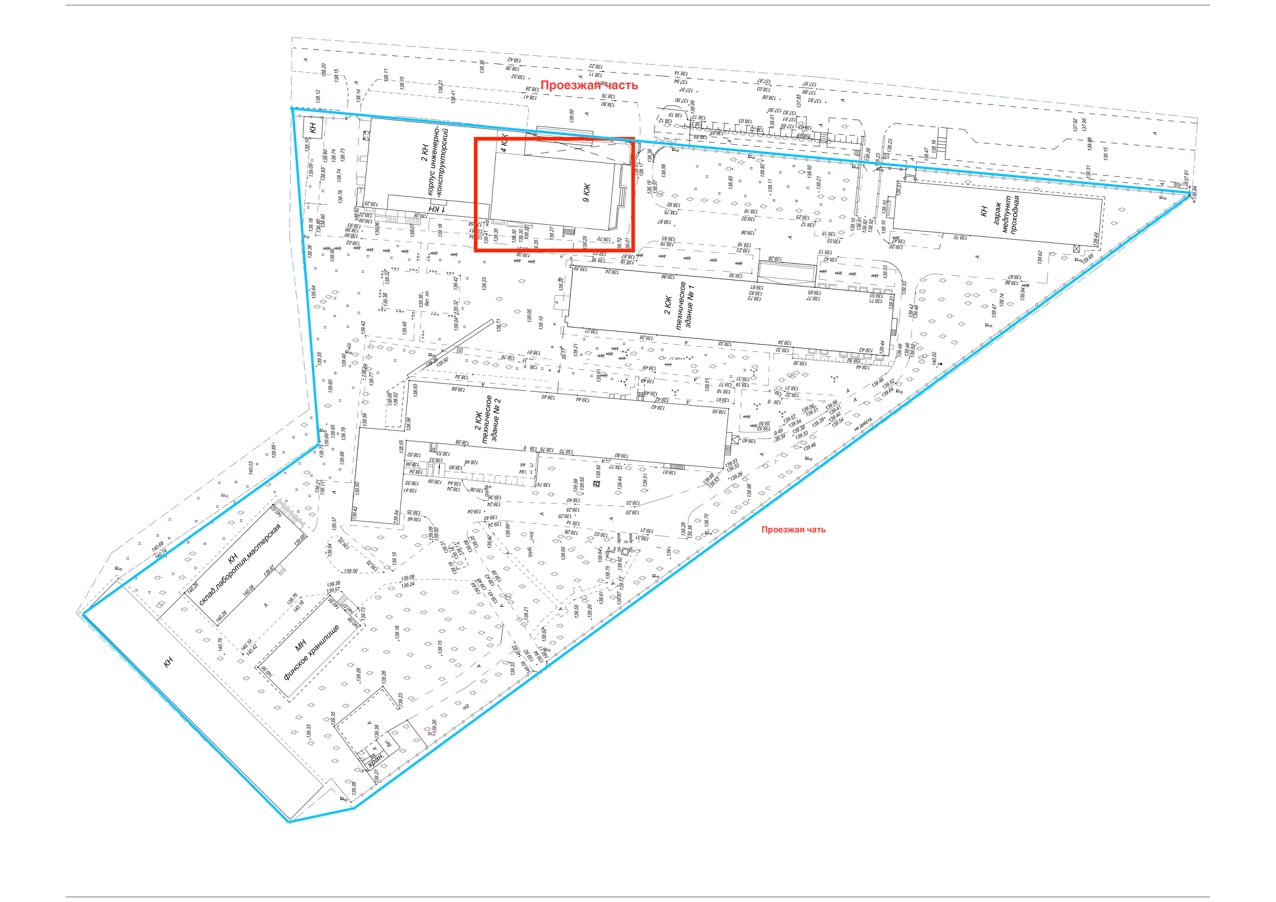


Рис. 5. План размещения и границы контролируемой зоны.

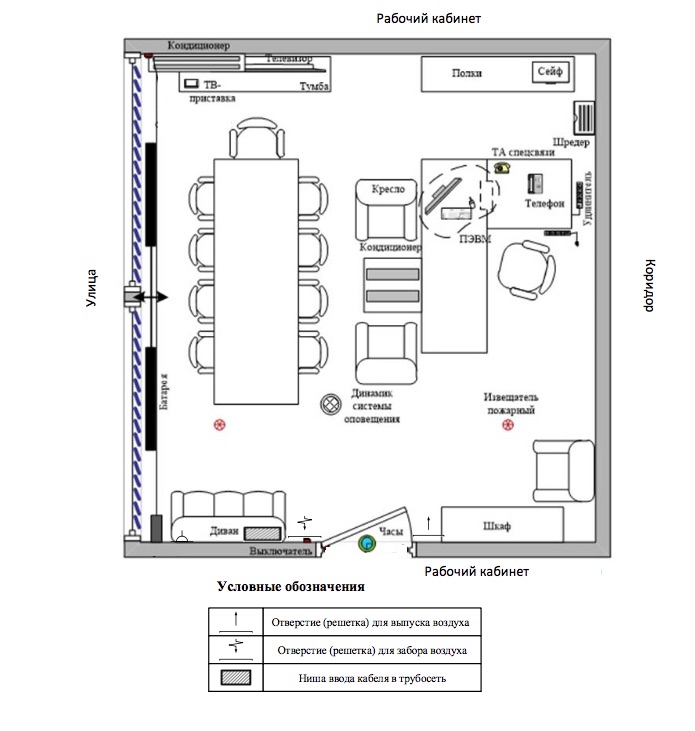
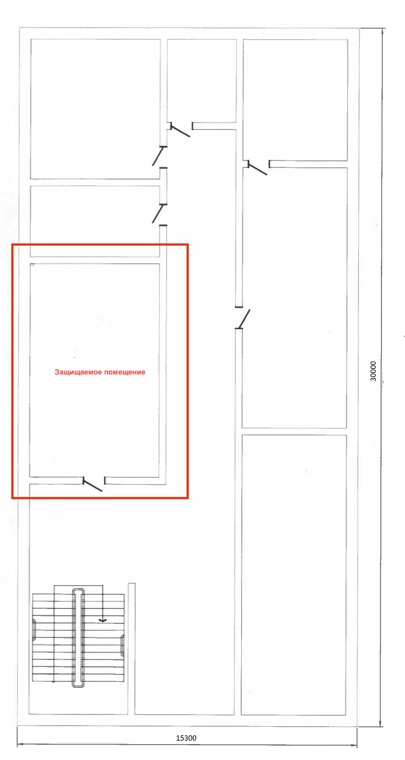


Рис. 6. Поэтажный план и план кабинета

Учитывая модель угроз и схему расположения помещения, для защиты информации от утечки по техническим каналам в защищаемом помещении, принимается решение об использовании системы активной защиты (рис.7).

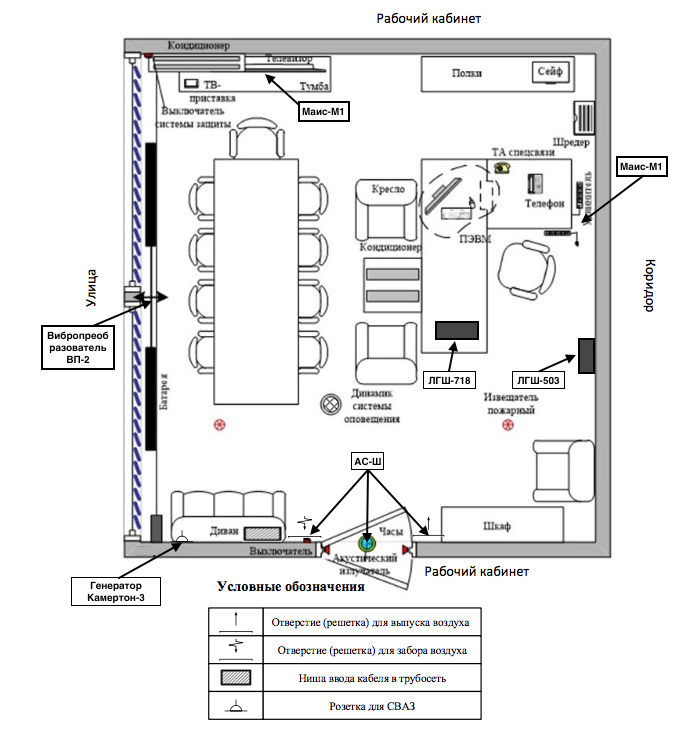


Рис. 7. Места установки системы активной защиты.

## 

## Оценка уровней защищенности для отдельных технических средств и каналов утечки информации производится в соответствии с методикой оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустичекому каналам, и необходима для аттестации помещений на соответствие требованиям защищенности.

# **Заключение**

В этой связи в данной работе были рассмотрены основные методы и средства, позволяющие защищать информацию различного уровня важности, и предложен комплекс мер по защите информации от утечек по техническим каналам в помещениях органов исполнительной власти Российской Федерации.

Было показано, что для этого необходимо четко понимать, каковы возможные каналы утечки и возможности несанкционированного доступа в то или иное помещение, применение средств активной защиты информации от утечки по техническим каналам при подготовке помещений для проведения работ с информацией, содержащей конфиденциальные данные. Это касается проведения переговоров, использования персональных ЭВМ для видеоконференцсвязи и обработки информации с меткой «Для Служебного Пользования».

# **Литература**

1. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 5 декабря 2016 г. № 646).
2. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992.
3. Положение по аттестации объектов информатизации по требованиям безопасности информации (Приказ Председателя Гостехкомиссии России от 25 ноября 1994).
4. Козлова О.Н., Соломахин А.Н., Шахворостов Г.И. Особенности применения информационной политики как инструмента повышения эффективности государственного и муниципального управления // Регион: государственное и муниципальное управление. 2016. № 2(06). С.1-20. URL: <http://regiongmu.ru/wp-content/uploads/2016/07/RegionGMU020604.pdf>
5. Куприяновский В.П., Аленьков В.В., Соколов И.А., Зажигалкин А.В., Климов А.А., Степаненко А.В., Синягов С.А., Намиот Д.Е. Умная инфраструктура, физические и информационные активы, Smart Cities, BIM, GIS и IoT // International Journal of Open Information Technologies. 2017. Vol. 5. № 10. С. 55-86.
6. Лугачев М.И. Информационные революции, экономика и экономическое образование // Вестник Московского университета. Серия 6. Экономика. 2017. № 4. С. 142-160.
7. Шаньгин В. Защита информации в компьютерных системах и сетях. М.: Litres, 2017.
8. Шерешева М.Ю. Информационная инфраструктура розничных сетей в России // Российский журнал менеджмента. 2005. Т. 3. № 1. С. 53-74.
9. Merkow M.S., Breithaupt J. Information security: Principles and practices. Pearson Education, 2014.
10. Peltier T.R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press. 2016.
11. Указ Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти». URL: https://rg.ru/2004/03/11/federel-dok.html
12. Федеральный Закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
13. Федеральный Закон от 4.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
14. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

1. Козлова О.Н., Соломахин А.Н., Шахворостов Г.И. Особенности применения информационной политики как инструмента повышения эффективности государственного и муниципального управления // Регион: государственное и муниципальное управление. 2016. № 2(06). С.1-20; Ларин А.А. Информационные технологии и эффективность государственного управления. Вестник Нижегородского университета им. Н.И. Лобачевского. 2010. № 2 (1). С. 251-255. [↑](#footnote-ref-1)
2. Куприяновский В.П., Аленьков В.В., Соколов И.А., Зажигалкин А.В., Климов А.А., Степаненко А.В., Синягов С.А., Намиот Д.Е. Умная инфраструктура, физические и информационные активы, Smart Cities, BIM, GIS и IoT // International Journal of Open Information Technologies. 2017. Vol. 5. № 10. С. 55-86. [↑](#footnote-ref-2)
3. Лугачев М.И. Информационные революции, экономика и экономическое образование // Вестник Московского университета. Серия 6. Экономика. 2017. № 4. С. 142-160. [↑](#footnote-ref-3)
4. Peltier T.R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press. 2016. [↑](#footnote-ref-4)
5. Шаньгин В. Защита информации в компьютерных системах и сетях. М.: Litres, 2017; Merkow M.S., Breithaupt J. Information security: Principles and practices. Pearson Education, 2014. [↑](#footnote-ref-5)
6. Органами исполнительной власти в Российской Федерации являются Правительство РФ и министерства различных направлений (Министерство связи, Министерство промышленности и торговли, Министерство обороны и др.). [↑](#footnote-ref-6)
7. *Технический канал утечки информации* - совокупность объекта технической разведки (источника сигнала или передатчика), физической среды распространения информативного сигнала (линии связи) и средств, которыми добывается защищаемая информация (приемника). [↑](#footnote-ref-7)
8. *Технические средства приема, обработки, хранения и передачи информации* (ТСПИ) - это технические средства, непосредственно обрабатывающие конфиденциальную информацию, к которым относятся: электронно-вычислительная техника; АТС для ведения конфиденциальных переговоров; системы оперативно-командной и громкоговорящей связи; системы звукоусиления, звукового сопровождения и звукозаписи, и т.д. [↑](#footnote-ref-8)
9. Побочные электромагнитные излучения и наводки (ПЭМИН) ‑ утечки информации через разного рода демаскирующие и побочные излучения электронного оборудования. [↑](#footnote-ref-9)
10. СВТ (средства вычислительной техники) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем. [↑](#footnote-ref-10)
11. Основные технические средства и системы (ОТСС) – это технические средства информационной системы (ИС), включающие в себя средства вычислительной техники; информационно-вычислительные комплексы и сети; средства и системы передачи, приема и обработки; программные средства; средства защиты информации в ИС. [↑](#footnote-ref-11)
12. Техническая защита конфиденциальной информации (ТЗКИ) ‑ это защита информации некриптографическими методами, направленными на предотвращение утечки защищаемой информации по техническим каналам, от несанкционированного доступа к ней и от специальных воздействий на информацию в целях ее уничтожения, искажения или блокирования. [↑](#footnote-ref-12)
13. ФСТЭК России - специальный орган по лицензированию создана в соответствии с Указом Президента Российской Федерации от 09 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей до этого Государственной технической комиссии при Президенте РФ. См. также Федеральный Закон от 4.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». [↑](#footnote-ref-13)
14. Положение по аттестации объектов информатизации по требованиям безопасности информации (Приказ Председателя Гостехкомиссии России от 25 ноября 1994). [↑](#footnote-ref-14)
15. О перечне сведений конфиденциального характера (от 6.03.1997 г. № 188); Закон РФ № 5485-I от 21 июля 1993 г. "О государственной тайне" (с изменениями и дополнениями). [↑](#footnote-ref-15)
16. Угрозы НСД в КСА в данной статье не рассматриваются. Предполагается, что все КСА, установленные в защищаемых помещениях государственного органа исполнительной власти, обладают необходимыми СЗИ и сертификатами, позволяющими обрабатывать информацию, категорированную в соответствии с требованиями законов и руководящих документов РФ и внутренними распорядительными документами органа исполнительной власти. [↑](#footnote-ref-16)
17. Угрозы НСД, связанные с действиями нарушителей, имеющих доступ к ПТС КСА, могут быть реализованы нарушителем в случае получения физического доступа к ПТС КСА. [↑](#footnote-ref-17)
18. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Приказ Председателя Гостехкомиссии России № 282 от 30.08.2002). [↑](#footnote-ref-18)
19. Вспомогательные средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы. [↑](#footnote-ref-19)
20. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Приказ Председателя Гостехкомиссии России № 282 от 30.08.2002). [↑](#footnote-ref-20)