Приложение № 2

Утверждено
Постановлением Администрации
муниципального округа
от «20»05.2021 г. № 456

РУКОВОДСТВО
по защите информации от технических разведок и от её утечки по техническим каналам в Администрации Пограничного муниципального округа.

1. Общие положения

1.1. Руководство по защите информации от технических разведок и от её утечки по техническим каналам в Администрации Пограничного муниципального округа разработано в соответствии с Федеральными законами от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 21 июля 1993 г. N 5485-1 "О государственной тайне".

1.2. Руководство определяет основные меры по защите информации, типовые обязанности сотрудников Администрации Пограничного муниципального округа.

1.3. Требования Руководства являются обязательными для сотрудников Администрации Пограничного муниципального округа.

Руководство регламентирует вопросы защиты конфиденциальной информации.

При возникновении в Администрации Пограничного муниципального округа информации, содержащей государственную тайну, к средствам вычислительной техники (далее - СВТ), автоматизированным системам (далее - АС) и сотрудникам постоянно действующая техническая комиссия Администрации Пограничного муниципального округа (далее - ПДТК) будет предъявлять дополнительные требования, в соответствии с законодательством РФ.

При приёме на службу (работу) сотрудники, которые будут допущены к сведениям конфиденциального характера, должны быть под расписку ознакомлены с требованиями настоящего Руководства, в части их касающейся, а также с ответственностью за их нарушение.

1.4. В Руководстве используются термины и их определения, установленные законодательством РФ и приведённые в Приложении к данному Руководству.

2. Существующие угрозы информационной системе Администрации Пограничного муниципального округа

2.1. Информационной системе Администрации Пограничного муниципального округа характерны следующие особенности:

- возрастающий удельный вес автоматизированных процедур в общем объёме процессов обработки данных в Администрации Пограничного муниципального округа;
- нарастающая важность и ответственность решений, принимаемых в автоматизированном режиме и на основе автоматизированной обработки информации;
- увеличивающаяся концентрация в АС информации, зачастую носящей конфиденциальный характер;
- накопление на технических носителях значительных объемов информации, для многих видов которой становится всё более трудным (и даже невозможным) изготовление немашинных аналогов (дубликатов);
- отсутствие в единых базах данных информации различного назначения и различной принадлежности;

- долговременное хранение информации на машинных носителях;
- отсутствие одновременного доступа к ресурсам (в том числе и к информации) большого числа сотрудников;
- незначительная (малая) циркуляция информации между АС.

В связи с этим существует необходимость в обеспечении сохранности и защиты используемой информации, циркулирующей и обрабатываемой в АС Администрации Пограничного муниципального округа.

2.2. В Администрации Пограничного муниципального округа на основе требований настоящего Руководства могут быть разработаны в необходимом объеме и с учетом их особенностей инструкции и организационно распорядительные документы по защите информации для всех категорий должностных лиц, допущенных к информации ограниченного доступа.

2.3. Угрозы для информации, циркулирующей в АС, могут исходить от утечки по техническим каналам, от внедренных специальных электронных устройств, от специальных программ-вирусов, от несанкционированного доступа (далее - НСД).

2.4. К основным способам НСД к информации относятся:
- непосредственное обращение к объектам доступа (СВТ, АС);
- воздействие на АС программными и техническими средствами, позволяющими выполнить обращение к объектам доступа в обход средств защиты.

2.5. Несанкционированный доступ к информации, находящейся в АС Администрации Пограничного муниципального округа, может быть косвенным - без физического доступа к элементам АС и прямым - с физическим доступом.

Существуют следующие косвенные пути НСД к информации:
- применение подслушивающих устройств;
- дистанционное фотографирование;
- перехват электромагнитных излучений;
- хищение информации;
- считывание данных в массивах других пользователей;
- копирование носителей информации;
- несанкционированное использование терминалов;
- маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
- использование программных ловушек;
- получение защищаемых данных с помощью серии разрешённых запросов;
- использование недостатков языков программирования и операционных систем;
- преднамеренное включение в библиотеки программ специальных блоков типа "троянских коней";
- незаконное подключение к аппаратуре или линиям связи информационной системы;
- злоумышленный вывод из строя механизмов защиты.

3. Основные направления и методы защиты информации

3.1. Обеспечение надёжной защиты информации является одной из важнейших обязанностей ПДТК и сотрудника, ответственного за защиту информации в Администрации Пограничного муниципального округа.

3.2. Организацию работ по защите информации, методическое руководство проведением мероприятий по защите информации в Администрации Пограничного муниципального округа, а также контроль за эффективностью предусмотренных мер защиты проводит ПДТК.

3.3. Сотрудник, ответственный за защиту информации в Администрации Пограничного муниципального округа, контролирует выполнение установленных общих требований по организации работы АС и предусмотренных мер по защите информации.

3.4. Сотрудники Администрации Пограничного муниципального округа, контролируют в пределах своей компетенции состояние защиты информации АС на своих рабочих местах с целью своевременного выявления и предотвращения утечки информации по техническим каналам, несанкционированного доступа к ней, преднамеренных программно-технических воздействий на информацию и оценки ее защищённости.

3.5. Отчеты о состоянии защиты информации по итогам года сотрудник, ответственный за защиту информации в Администрации Пограничного муниципального округа, предоставляет Постоянно действующей технической комиссии Администрации Пограничного муниципального округа.

3.6. В целях предотвращения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации (далее - ТСПИ), их хищения и нарушения работоспособности организуется охрана объектов информатизации по средствам видеонаблюдения за помещениями и контрольно-пропускной системы Администрации Пограничного муниципального округа.

3.7. Защита информации в АС и СВТ предусматривает комплекс организационных, программных и технических мероприятий по защите информации при ее автоматизированной обработке, хранении и передаче по каналам связи.

В качестве программных средств используются специальные программы, предназначенные для выполнения функций, связанных с защитой информации.

К техническим средствам защиты информации относятся различные электрические, электромеханические и электронные устройства, которые подразделяются на аппаратные средства - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с СВТ по стандартному интерфейсу и физические средства - автономные устройства (электронно-механическое оборудование охранной сигнализации и наблюдения, запоры и решётки на окнах).

3.8. На объекты информатизации, задействованные в обработке конфиденциальной информации, составляются технические паспорта, согласно СТР-К, и они должны быть аттестованы по требованиям безопасности информации в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации, утверждённым Гостехкомиссией при Президенте Российской Федерации 25.11.1994 г.

3.9. Защите подлежат все компоненты информационной структуры Администрации Пограничного муниципального округа: документы, сети связи, ТСПИ, персонал и т.д.

3.10. Защита информации в АС Администрации Пограничного муниципального округа осуществляется по следующим основным направлениям:

- от утечки по техническим каналам;
- от внедренных специальных электронных устройств;
- от специальных программ-вирусов;
- от несанкционированного доступа;
- от несанкционированного воздействия;

- от непреднамеренного воздействия;
- от разглашения;

3.11. В качестве основных мер защиты информации в Администрации Пограничного муниципального округа сотрудниками, осуществляющими эксплуатацию объектов информатизации, должны выполняться:

а) соблюдение Положения о порядке обращения с конфиденциальной информацией в Администрации Пограничного муниципального округа;

б) разграничение доступа сотрудников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

в) ограничение посторонних лиц в защищаемые помещения и помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;

г) учёт и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;

д) резервирование технических средств, дублирование массивов и носителей информации;

е) использование сертифицированных серийно выпускаемых в защищённом исполнении технических средств обработки, передачи и хранения информации;

ж) использование технических средств, удовлетворяющих требованиям стандартов по электромагнитной совместимости;

з) использование сертифицированных средств защиты информации;

и) размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от её границ;

к) защита цепей электропитания объектов информации:

- использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);
- развязка цепей электропитания объектов защиты с помощью сетевых помехоподавляющих фильтров, блокирующих (подавляющих) информативный сигнал;

л) использование защищённых каналов связи;

м) размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

н) организация физической защиты помещений и собственно технических средств обработки информации с использованием технических средств охраны, предотвращающих или существенно затрудняющих проникновение в Администрации Пограничного муниципального округа посторонних лиц, хищение документов и носителей информации, самих средств информатизации;

о) предотвращение внедрения в АС программ-вирусов, программных закладок.

3.12. Объём принимаемых мер защиты информации, в зависимости от возможного ущерба в случае ее утечки, определяет ПДТК**.**

4. Защита информации от утечки по техническим каналам

4.1. При выявлении технических каналов утечки информации технические средства обработки, хранения и передачи информации рассматриваются как система, включающая основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ТСПИ и их элементами), распределительные и коммуникационные устройства, системы электропитания, системы заземления.

4.2. Отдельные технические средства или группа технических средств, предназначенных для обработки информации, вместе с помещениями, в которых они размещаются, составляют объект ТСПИ. Под объектами ТСПИ понимаются также выделенные помещения, предназначенные для проведения конфиденциальных мероприятий.

Наряду с ТСПИ, в помещениях могут находиться вспомогательные технические средства и системы (далее - ВТСС), не применяемые в обработке информации, но используемые совместно с ТСПИ и находящиеся в зоне электромагнитного поля, создаваемого ими. К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, электробытовые приборы и т.д.

4.3. В качестве канала утечки информации основное внимание необходимо уделять ВТСС, имеющим выход за пределы контролируемой зоны.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками.

4.4. Основные способы защиты информации от утечки по техническим каналам:

- использование сертифицированных по требованиям защиты информации основных технических средств и систем, предназначенных для передачи, обработки и хранения конфиденциальной информации (далее - ОТСС) и ВТСС;
- использование сертифицированных технических средств защиты информации;
- размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ;
- документальное оформление перечня защищаемых помещений (далее - ЗП) и лиц, ответственных за их эксплуатацию;
- выполнение рекомендованных мероприятий по оборудованию ЗП: стены, полы и потолки не должны быть смежными с помещениями других организаций; окна закрываются шторами (жалюзи);
- проведение специальных проверок помещений;
- применение при необходимости активных средств защиты речевого сигнала (генераторы шума и т.п.);
- выполнение требований по монтажу и применению ВТСС в ЗП согласно Специальным требованиям и рекомендациям по технической защите конфиденциальной информации;
- проведение на объектах защиты специальных исследований специализированными организациями, имеющими лицензии на проведение работ по защите информации.

5. Защита информации от внедрённых специальных электронных устройств

5.1. Информация, обрабатываемая в ТСПИ, может сниматься путём установки в них электронных устройств перехвата информации - закладных устройств (минипередатчики, излучение которых модулируется информационным сигналом).

5.2. Выявление внедренных на объекты электронных устройств перехвата информации достигается специальными проверками, которые проводятся при аттестации помещений, предназначенных для ведения секретных и конфиденциальных переговоров. Для помещений, предназначенных для ведения секретных переговоров, аттестация является обязательной, а для ведения конфиденциальных переговоров - по усмотрению Постоянного представителя.

5.3. Специальные проверки проводятся также с целью выявления и изъятия специальных электронных устройств перехвата информации, внедрённых в ОТСС и ВТСС. Специальные проверки должны проводить специалисты организаций, имеющих лицензии, выданные уполномоченными органами.

В зависимости от целей, задач и используемых средств устанавливаются следующие виды специальных проверок:

- специальное обследование объектов защиты;
- визуальный осмотр ЗП;
- комплексная специальная проверка ЗП;
- визуальный осмотр и специальная проверка новых предметов (подарков, предметов интерьера, бытовых приборов и т.п.) и мебели, размещаемых или устанавливаемых в ЗП;
- специальная проверка применяемой радиоэлектронной аппаратуры;
- периодический радиоконтроль (радиомониторинг) ЗП;
- специальная проверка проводных линий;
- проведение тестового "прозвона" всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Периодичность и виды проверок помещений в целях выявления в них закладных устройств зависят от степени важности помещений и порядка допуска в них посторонних лиц.

5.4. Специальное обследование и визуальный осмотр ЗП проводятся, как правило, без применения технических средств. Остальные же виды проверок требуют использования тех или иных специальных средств контроля.

Специальные обследования помещений проводятся после окончания строительства объекта или после проведения капитального ремонта в них, а также периодически. Для проведения специальных обследований должны привлекаться соответствующие специалисты.

Визуальный осмотр помещений проводится перед началом и после завершения служебных совещаний, а также в начале и после завершения рабочего дня. Если проверка проводится вечером, то после ее завершения помещение должно быть закрыто. Данный вид проверки кабинетов руководящего состава целесообразно поручать их секретарям. Проверку помещений для проведения служебных совещаний целесообразно поручать сотруднику, ответственному за защиту информации в Администрации Пограничного муниципального округа.

При проведении визуального осмотра ЗП особое внимание уделяется местам, куда можно быстро и скрыто установить закладное устройство. Этот вид контроля позволяет выявить закладки, оставляемые посетителями в легко доступных местах: под столешницами, под сидениями стульев, в различных щелях, за картинами, за батареями, за мебелью, за шторами и т.д.

5.5. Специальная проверка радиоэлектронной аппаратуры, в том числе ПЭВМ и телефонных аппаратов, проводится после их закупки или ремонта. Специальная проверка проводных линий осуществляется после окончания строительства объекта или после проведения его капитального ремонта, а также периодически в целях обнаружения несанкционированных подключений к линиям средств съема информации. Для проведения проверки должны привлекаться соответствующие специалисты.

5.6. Радиоконтроль выделенных помещений проводится в целях обнаружения активных радиозакладок с использованием сканерных приемников или программноаппаратных комплексов контроля. Он организуется периодически при проведении наиболее важных мероприятий (совещаний, заседаний и т.п.) или непрерывно (постоянно).

5.7. Тестовый "прозвон" телефонных аппаратов проводится при установке нового телефонного аппарата или телефонного аппарата после ремонта, а также периодически. "Прозвон" необходимо проводить с радиотелефона или телефонного аппарата, установленного в другом помещении. При наборе номера проверяемого телефонного аппарата осуществляется контроль (на слух) прохождения всех вызывных сигналов АТС. Если обнаружено подавление (непрохождение) одного - двух вызывных звонков у контролируемого телефонного аппарата, то, возможно, что в его корпусе или

телефонной линии установлено закладное устройство, и необходимо проводить специальную проверку телефонной линии и телефонного аппарата.

5.8. Комплексная специальная проверка помещений проводится после окончания строительства объекта или после проведения капитального ремонта в них, при проведении аттестации помещений, а также периодически. Это наиболее полный вид проверки. Для проведения таких специальных проверок используется весь арсенал технических средств контроля.

6. Защита информации от специальных программ-вирусов

6.1. В целях съёма информации, её разрушения, нарушения нормального функционирования СВТ и АС создаются специальные программы-вирусы.

6.2. Пути проникновения вирусов в СВТ и АС:

- проникновение вирусов на рабочие станции при использовании на рабочей станции инфицированных файлов с переносимых источников (флоппи-диски, компактдиски и т.п.);
- заражение вирусами с помощью инфицированного программного обеспечения, полученного из сети «Интернет»;
- заражение вирусами с удалённого сервера, подсоединенного к ЛВС и обменивающегося инфицированными данными с её серверами;
- распространение электронной почты, содержащей в приложениях файлы Excel и Word, инфицированные макровирусами.

6.3. Организация антивирусной защиты информации на объектах информатизации достигается путём:

- внедрения и применения средств антивирусной защиты информации;
- обновления баз данных средств антивирусной защиты информации;
- спланированных действий должностных лиц при обнаружении заражения информационных ресурсов программными вирусами.

6.4. Система антивирусной защиты должна разрабатываться с учётом особенностей конкретных ЛВС и, в общем случае, должна включать в себя:

- антивирусную защиту рабочих станций;
- антивирусную защиту серверов;
- возможность автоматического обновления антивирусных баз и версий.

6.5. Организация работ по антивирусной защите информации возлагается на сотрудника, ответственного за защиту информации Представительства, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на ПДТК.

6.6. Порядок применения средств антивирусной защиты устанавливается с учётом необходимости выполнения следующих требований:

- периодическая проверка жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка используемых в работе гибких магнитных дисков перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка магнитных носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса;
- обязательный входной контроль на отсутствие программных вирусов всех поступающих на объект информатизации машинных носителей информации, информационных массивов, программных средств общего и специального назначения;
- восстановление работоспособности программных средств и информационных массивов в случае их повреждения программными вирусами.

6.7. К использованию допускаются только лицензированные антивирусные средства. Порядок установки и использования средств антивирусной защиты определяется инструкцией по установке и руководством по эксплуатации конкретного антивирусного программного продукта.

6.8. При обнаружении программных вирусов пользователь обязан прекратить все работы на ПЭВМ, поставить в известность сотрудника, ответственного за защиту информации Администрации Пограничного муниципального округа, который должен принять меры по локализации и удалению вирусов.

При функционировании ПЭВМ в качестве рабочей станции вычислительной сети производится её отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

7. Защита информации от несанкционированного доступа

7.1. Существуют два относительно самостоятельных направления защиты информации от НСД: направление, связанное с СВТ, и направление, связанное с АС.

Защита СВТ обеспечивается комплексом программно-технических средств. Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

7.2. Организационные меры в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесённую к категории секретной, должны осуществляться в соответствии с требованиями Специальных требований и рекомендаций по защите информации, составляющей государственную тайну, от утечки по техническим каналам, утвержденными Решением Государственной технической комиссии при Президенте Российской Федерации от 23 мая 1997 г. N 55.

7.3. При обработке или хранении в АС конфиденциальной информации для её защиты проводятся следующие организационные мероприятия:

- документальное оформление конфиденциальной информации в виде перечня сведений, подлежащих защите;
- определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;
- установление и оформление правил разграничения доступа, т.е. совокупности правил доступа субъектов к данным;
- ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая АС, путём технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение СВТ, информационных носителей, а также НСД к СВТ и линиям связи;
- выбор класса защищённости АС в соответствии с особенностями обработки информации и уровнем её конфиденциальности;
- разработка системы защиты информации от НСД, включая соответствующую организационно-распорядительную документацию.

7.4. Защита доступа к компьютеру осуществляется программными, программноаппаратными средствами и чисто аппаратными комплексами. Это обеспечивает:

- наличие в компьютерах Представительства только той информации и тех программ, которые необходимы сотрудникам для повседневной деятельности
- постоянный контроль за конфиденциальной информацией, всегда можно узнать, кто и когда к ней обратился;

7.5. Основные мероприятия по предотвращению НСД к информации:

а) разграничение доступа к информации;

б) управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

в) идентификация пользователей (сотрудников) и подтверждение их права на работу с запрашиваемой информацией;

г) очистка оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

8. Защита информации от несанкционированного и непреднамеренного воздействия

Защита информации от несанкционированного и непреднамеренного воздействия осуществляется по следующим направлениям:

а) соблюдение порядка разработки, ввода в действие и эксплуатации объектов информатизации;

б) определение условий размещения объекта информатизации относительно границ контролируемой зоны;

в) контроль, техническое обслуживание и обеспечение установленных режимов работы ТСПИ в целях предупреждения их сбоев, аварий, неисправностей;

г) применение постоянно обновляемого антивирусного программного обеспечения;

д) защита от природных и техногенных явлений и стихийных бедствий (пожары, наводнения, землетрясения, грозовые разряды, грызуны и т.п.);

е) предупреждение передачи конфиденциальной информации по открытым линиям связи и её обработки в незащищенных АС;

ж) организация ПДТК эффективного контроля за выполнением предусмотренных мер защиты информации;

9. Защита информации от разглашения

9.1. С увеличением масштабов распространения и использования ПЭВМ и информационных систем усиливается роль различных факторов, способствующих возможности разглашения информации. К ним относятся несанкционированные и злоумышленные действия сотрудников, а также их ошибки.

9.2. Разглашение может происходить по формальным и неформальным каналам распространения информации.

К формальным каналам относятся деловые встречи, совещания, переговоры и тому подобные формы общения, а также обмен официальными деловыми и научными документами с использованием средств передачи официальной информации (почта, телефон, телеграф и др.).

Неформальные каналы включают:

- личное общение (встречи, переписка и др.);
- выставки, семинары, конференции и другие массовые мероприятия;
- средства массовой информации (печать, газеты, интервью, радио, телевидение и др.).

9.3. Условиями, способствующими неправомерному доступу к конфиденциальной информации, могут являться также отсутствие трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа по сплочению коллектива Администрации Пограничного муниципального округа.

9.4. Предупреждение противоправных действий с конфиденциальной информацией обеспечивается различными мерами и средствами, начиная с создания климата осознанного отношения работников к проблеме безопасности и защиты информации.

9.5. Причиной разглашения конфиденциальной информации, как правило, является недостаточное знание работниками правил её защиты и непонимание (или недопонимание) необходимости их тщательного соблюдения.

9.6. Правовой основой работы с работниками, допущенными к конфиденциальной информации, являются:

- наличие в служебном контракте пункта о работе со сведениями, составляющими конфиденциальную информацию;
- наличие в должностном регламенте работника пункта о том, что он работает с конфиденциальной информацией и несёт ответственность за её разглашение;
- наличие перечня сведений конфиденциального характера, с которыми должен быть ознакомлен работник;
- создание работникам условий для работы с информацией ограниченного доступа.

Термины и их определения

Приложение

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аттестация - комплекс организационно-технических мероприятий, в результате которых посредством специального документа - "Акта соответствия" подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Абонентский пункт информационной сети общего пользования (АП ИВС ОП) - автоматизированная система, подключаемая к информационной сети общего пользования (Интернет) с помощью коммутационного оборудования и предназначенная для работы абонентов.

Безопасность информации - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системой от внутренних или внешних угроз.

Доступ к информации - возможность получения информации и ее использования.

Закладное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защищаемые помещения - помещения (служебные кабинеты, актовые, конференц- залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

Информация - сведения (сообщения, данные), независимо от формы их представления.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная инфраструктура - совокупность систем обработки и анализа информации, каналов информационного обмена и телекоммуникаций, линий связи, систем и средств защиты информации.

Информация ограниченного доступа - информация, для которой установлен специальный режим сбора, хранения, обработки, распространения и использования.

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств, технических и иных материальных средств.

Локальная вычислительная сеть - совокупность основных технических средств и систем, осуществляющих обмен информацией между собой и с другими информационными системами, в том числе с ЛВС, через определенные точки входа/выхода информации, которые являются границей ЛВС.

Несанкционированный доступ - доступ к информации, нарушающий правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Непреднамеренное воздействие на информацию - воздействие ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированное воздействие на информацию - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящее к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате.

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора права разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Пользователь информации - субъект, обращающийся к информационной системе за получением необходимой ему информации и пользующийся ею.

Разглашение - умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с информацией.

Система защиты информации - комплекс организационных мер и программнотехнических средств обеспечения безопасности информации в автоматизированных системах.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность объекта технической разведки, физической среды распространения информационного сигнала и средств, которыми добывается защищаемая информация.

Технические средства приема, обработки, хранения и передачи информации - технические средства, непосредственно обрабатывающие информацию, к средствам относятся: электронно-вычислительная техника, режимные АТС, системы

оперативнокомандной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.