Приложение № 1 к
документации для
процедуры
запроса предложений

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
На оказание услуг по созданию системы защиты информации на объектах информатизации Некоммерческой организации «Региональный фонд капитального ремонта общего имущества в многоквартирных домах на территории Орловской области»

Термины и сокращения

АС	Автоматизированная система
ГСЗИ	Государственная система защиты информации
ИБ	Информационная безопасность
ИСПДн	Информационная система персональных данных
КСЗПДн	Комплексная система защиты персональных данных
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
СЗКИ	Система защиты конфиденциальной информации
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
ТЗ	Техническое задание
ТЗИ	Техническая защита информации
ФЗ	Федеральный закон
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Термины и определения

Автоматизированная система	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. (ГОСТ 34.003-90)
Автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники. (ФЗ РФ от 27 июля 2006 г. № 152)
Безопасность автоматизированной информационной системы	состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность и целостность, подотчётность и подлинность её ресурсов.(Р 50.1.053-2005)
Блокирование персональных данных	временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных). (ФЗ РФ от 27 июля 2006 г. № 152-ФЗ)
Доступность информации (ресурсов автоматизированной информационной системы)	состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно. (Р 50.1.053-2005)
Доступ к информации в автоматизированной информационной системе	получение возможности ознакомления с информацией, ее обработки и (или) воздействия на информацию и (или) ресурсы автоматизированной информационной системы с использованием программных и (или) технических средств. (Р 50.1.053-2005) Примечание. Доступ осуществляется субъектами доступа, к которым относятся лица, а также логические и физические объекты
Защита информации	деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. (ГОСТ Р 50922-2006)
Информационная система персональных данных	информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. (ФСБ России от 21 февраля 2008 года № 149/54-144)
Конфиденциальность персональных данных	обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом

	требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания. (ФСБ России от 21 февраля 2008 года № 149/54-144)
Обезличивание персональных данных	действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.(ФЗ РФ от 27 июля 2006 года № 152)
Обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.(ФЗ РФ от 27 июля 2006 года № 152)
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. (ФЗ РФ от 27 июля 2006 года № 152-ФЗ)
Персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). (ФЗ РФ от 27 июля 2006 года № 152-ФЗ)
Распространение персональных данных	действия, направленные на раскрытие персональных данных неопределенному кругу лиц. (ФЗ РФ от 27 июля 2006 года № 152-ФЗ)
Система защиты информации	совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации. (ГОСТ Р 50922-2006)
Средство защиты информации	техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации. (ГОСТ Р 50922-2006)
Техническая защита информации	защита (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращение ее утечки по техническим каналам, несанкционированного

	доступа к ней, специальных воздействий на информацию и носители информации в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации. (Р 50.1.053-2005) Примечание. Техническая защита информации при применении информационных технологий осуществляется в процессах сбора, обработки, передачи, хранения, распространения информации с целью обеспечения ее безопасности на объектах информатизации.
Угроза (безопасности информации)	совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и(или) целостности информации. (Р 50.1.053-2005)
Уязвимость (автоматизированной информационной системы)	недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации. (Р 50.1.053-2005)
Уничтожение персональных данных	действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных. (ФЗ РФ от 27 июля 2006 года № 152-ФЗ)
Целостность информации (ресурсов автоматизированной информационной	состояние информации (ресурсов автоматизированной информационной системы), при котором её (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право. (Р 50.1.053-2005)
Эффективность защиты информации	степень соответствия результатов защиты информации поставленной цели. (ГОСТ Р 50922-2006)

1. НАЗНАЧЕНИЕ И ЦЕЛИ РАБОТ

1. Назначение работ: Назначением оказываемых услуг (проводимых работ) является обеспечение безопасности информации ограниченного доступа (конфиденциальной информации и персональных данных), циркулирующей на объектах информатизации.
2. Цели проводимых работ:

Работы проводятся с целью:

– Обследования, подготовки пакета документов для обеспечения организационных мероприятий по защите информации, поставка (приобретение), установка, настройка средств защиты информации от НСД, средств безопасного межсетевого взаимодействия, а так же устройств защиты от утечки информации по техническим каналам предназначенное для защиты объектов ВТ (вычислительной техники) от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств, в случае необходимости.

– Обеспечения защиты от несанкционированного доступа (далее НСД) к информации ограниченного доступа (конфиденциальной информации и персональных данных), обрабатывающейся на автоматизированных рабочих местах (далее АРМ).

– Проведение объектовых специальных исследований линий связи локальных вычислительных сетей (ЛВС) стандарта 100BASE-TX от утечки по каналам побочных электромагнитных излучений;

– Обеспечение безопасного межсетевого взаимодействия и обнаружения уязвимостей при подключении локальной вычислительной сети к сетям международного информационного обмена;

– Проведение аттестационных испытаний автоматизированных систем **(АС),** информационных систем персональных данных **(ИСПДн)** по требованиям безопасности информации и защищаемых помещений **(ЗП)** в которых циркулирует акустическая информация конфиденциального характера;

– Проведение **Обучения** «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Заказчик – Некоммерческая организация «Региональный фонд капитального ремонта общего имущества в многоквартирных домах на территории Орловской области».

4. Исполнитель – определяется по результатам проведения процедуры запроса предложений.

5. Требования к организации исполнителя:

– действующая лицензия **ФСТЭК России** на деятельность по технической защите конфиденциальной информации со следующими видами работ:

- контроль защищенности конфиденциальной информации от утечки по техническим каналам в средствах и системах информатизации;
- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- аттестационные испытания и аттестация на соответствие требованиям по защите информации средств и систем информатизации;
- установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищенности информации);

– или лицензия **ФСТЭК России** на деятельность по технической защите конфиденциальной информации (выданной до вступления в силу постановления Правительства РФ от 03.02.2012 N 79.).

– **лицензия ФСБ России** на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), в части выполнения и оказания следующих работ и услуг, составляющих лицензируемую деятельность: № 12, 13, 14, 15, 20, 21, 22, 23, 24, 25, 26, 28 перечня выполняемых работ и оказываемых услуг составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 года № 313.

2. СВЕДЕНИЯ ОБ ОБЪЕКТАХ РАБОТ

2.1. Объектами являются:

- **АС и ИСПДн (АИС) «Региональный фонд капитального ремонта»:**

2.1.1. В АИС «Региональный фонд капитального ремонта» установлено 24 (двадцать четыре) рабочих станций и 1 (один) Сервер, входящие в состав общей корпоративной локальной вычислительной сети подключенной к информационно-телекоммуникационной сети Интернет. Количество рабочих станций и Серверов, на которых производится обработка информации ограниченного доступа – персональные данные, служебная информация и другая конфиденциальная информация (за исключением государственной тайны) составляет 15 (Пятнадцать) АРМ и Серверов.

2.1.2. В процессе обследования информационной системы определяется точное количество рабочих мест и в случае необходимости, за свой счёт и своими силами необходимо закупить всё недостающее оборудование и другие, необходимые для проведения работ устройства и материалы, предварительно согласовав характеристики поставляемого оборудования и материалов с Заказчиком.

В процессе обследования информационных систем определяется точное количество рабочих мест и в случае необходимости, за свой счёт и своими силами закупить всё недостающее оборудование и другие необходимые для проведения работ устройства и материалы, предварительно согласовав характеристики поставляемого оборудования и материалов с Заказчиком.

2.2. Место оказания услуг (Фактический адрес расположение – АИС). Точки выхода в сети общего пользования АИС.

2.2.1 Российская Федерация, Орловская обл., г. Орел, ул. Московская, д. 159.

Информационные системы имеют выход за пределы контролируемой зоны. В случае необходимости, за свой счёт и своими силами организовать каналы криптографической защиты передачи информации ограниченного доступа по локальной вычислительной сети между зданиями, сертифицированными по требованиям ФСБ России средствами криптографической защиты информации (Наличие у Исполнителя сертификатов и (или) лицензий на указанные средства обязательно). Уточняется в процессе обследования.

3. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ПРОВЕДЕНИЯ ОБСЛЕДОВАНИЯ ОИ

3.1. Основными задачами по обследованию являются АИС:

– установка необходимости обработки персональных данных и конфиденциальной информации (далее – КИ и ПДн);

– определение перечня информации, подлежащих защите от несанкционированного доступа (далее - НСД);

– определение конфигурации и топологии ИС в целом и ее отдельных компонентов, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения;

– определение технических средств и систем, предполагаемых к использованию в ИС, условий их расположения, общесистемных и прикладных программных средств, имеющихся и предлагаемых к использованию;

– определение режима обработки информации в ИС в целом и в отдельных компонентах;

– уточнение степени участия персонала в обработке информации, характер их взаимодействия между собой;

– определение используемых средств защиты информации;

– определение существующей организационно-распорядительной базы по обеспечению безопасности информации;

– проведение объектовых специальных исследований линий связи локальных вычислительных сетей (ЛВС) стандарта **100BASE-TX от утечки по каналам побочных электромагнитных излучений;**

– проведение **инструментального контроля защищенности информации в линиях связи ЛВС стандарта 100BASE-TX от утечки по каналам побочных электромагнитных излучений** в ходе аттестационных испытаний;

– **проведение контроля защищенности информации**, обрабатываемой на объектах ВТ, от утечки по каналам побочных электромагнитных излучений и наводок **(ПЭМИН)** с целью уточнения угроз безопасности и минимизации затрат применительно к следующим каналам:

- побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны, в том числе на цепи заземления и электропитания;
- параллельного пробега линий связи ОТСС с иными линиями и коммуникациями;
- изменений тока потребления, обусловленных обрабатываемыми техническими средствами информативными сигналами;
- радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств.

– приведение в полное соответствие с нормами Федерального закона от 26 июля 2006 года № 152 ФЗ «О персональных данных» автоматизированных рабочих мест, на которых обрабатываются персональные данные;

– обеспечение защиты от несанкционированного доступа (далее НСД) к конфиденциальной информации, обрабатывающейся на автоматизированных рабочих местах (далее АРМ);

– обеспечение автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированной локальной вычислительной сети;

– обеспечение безопасного межсетевого взаимодействия при подключении локальной вычислительной сети к сетям международного информационного обмена;

– *обеспечение (при необходимости) криптографической защиты канала передачи информации ограниченного доступа по локальной вычислительной сети между зданиями, сертифицированными по требованиям ФСБ России средствами криптографической защиты информации (Наличие у Исполнителя сертификатов и (или) лицензий на указанные средства обязательно);*

– оценка соответствия объекта требованиям стандартов и других нормативных документов по безопасности информации, утвержденных (согласованных) ФСТЭК (Гостехкомиссией) России.

Основными направлениями проведения мероприятий по обследованию являются:

– анализ информационных ресурсов АИС;

– анализ технических и эксплуатационных характеристик АИС;

– анализ имеющихся мер и средств защиты информации (далее - СЗИ);

– анализ существующей организационной структуры и организационно-распорядительной документации по обеспечению безопасности информации;

– мероприятия по обследованию объекта информатизации;

– приобретение, установка и ввод в эксплуатацию средств от несанкционированного доступа к информации, средств безопасного межсетевого взаимодействия;

– *приобретение в случае необходимости программного обеспечения (Операционные системы, офисное ПО, серверное ПО, ПО для работы с Базами Данных и т.д.) для функционирования средств защиты информации и средств вычислительной техники-Локальной вычислительной сети (ЛВС);*

– создание системы защиты межсетевого взаимодействия;

– проведение аттестационных испытаний.

3.2. Основными задачами по обследованию являются ЗП:

– Определение наиболее подходящих для проведения аттестационных испытаний помещения и подбор необходимых сертифицированных по требованиям безопасности информации средств защиты информации.

– Рекомендации по исключению неиспользуемых технических средств из помещения, или технических средств, создающих предпосылки к нарушению информационной безопасности.

4. ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ РАБОТ ПО ПРОВЕДЕНИЮ ОБСЛЕДОВАНИЯ

4.1. Требования к анализу информационных ресурсов АИС

В процессе проведения анализа информационных ресурсов определить:

– необходимость обработки информации в АИС;
– состав;
– содержание и местонахождение информации, подлежащих защите;
– произвести оценку выполнения обязанностей по обеспечению безопасности информации.

4.2. Требования к анализу технических и эксплуатационных характеристик АИС

В ходе проведения анализа технических и эксплуатационных характеристик АИС должны быть определены следующие данные:

– территориальное размещение АИС;
– конфигурация и топология АИС в целом и ее отдельных компонент;
– физические связи АИС, в том числе с сетями общего пользования;
– функциональные и технологические связи как внутри АИС, так и с другими системами различного уровня и назначения;
– технические средства и системы АИС, условия их расположения;
– общесистемные и прикладные программные средства, используемые (планируемые к использованию) в АИС;
– режимы обработки информации в АИС и ее в компонентах;

Инструментально-контрольное обследование процессов автоматизированной обработки персональных данных:

– инвентаризация информационных систем персональных данных с использованием специализированных программных, программно-аппаратных средств контроля защищенности (сканер безопасности, анализатор уязвимости): определение архитектуры, конфигурации и топологии систем в целом и их отдельных компонент; составление схемы существующей сети с выделением участков, входящих в различные информационные системы;
– определение перечня серверов информационных систем персональных данных и функциональных требований, предъявляемых к ним;
– полное сканирование всех портов TCP/UDP для определения списка запущенных сервисов информационных систем персональных данных;
– сканирование при помощи специализированных технических средств обследуемых объектов информационных систем, задействованных в обработке персональных данных, на наличие открытых портов, установленных обновлений безопасности ОС и подверженности известным уязвимостям;
– определение работающих сервисов и их проверки на предмет обнаружения известных уязвимостей;
– выборочное тестирование на проникновение с составлением отчета о выявленных уязвимостях;

– выборочная запись и анализ трафика в информационных системах персональных данных на предмет передачи информации в открытом виде, осуществления недокументированной и вредоносной активности;

– выявление угроз несанкционированного доступа к персональным данным, реализуемых с применением программных и программно-аппаратных средств;

– аудит паролей (выявление слабых путем подбора по словарю и прямым перебором) для отдельных серверов приложений. Перечень серверов согласовывается с Заказчиком;

– оценка принятых контрмер (по результатам инструментального анализа и теста на проникновение) и соответствия средств защиты информации требованиям законодательства РФ по обеспечению безопасности персональных данных;

– подготовка рекомендаций по принятию технических мер, направленных на обеспечение безопасности персональных данных;

– разработка технического отчета по результатам инструментального обследования процесса автоматизированной обработки персональных данных;

– инструментально-контрольное обследование должно проводиться лицензионными программными (ПО) и (или) программно-аппаратными средствами;

– инструментальный контроль защищенности информационных систем должен проводиться сертифицированными средствами контроля защищенности.

Инструментально-контрольное обследование, инструментальный контроль, а также иные виды работ проводятся инструментально-контрольными средствами, инструментальными средствами контроля защищенности информационных систем и иными средствами Исполнителя.

Наличие у Исполнителя сертификатов и (или) лицензий на указанные средства обязательно.

Количество и тип средств вычислительной техники (сервера, рабочие станции и др.) по каждой информационной системе в соответствии с их размещением на объектах, необходимо получить Исполнителю контракта при проведении инвентаризация информационных систем, обрабатывающих (определение архитектуры, конфигурации и топологии систем в целом и их отдельных компонент) при экспертно-документальном обследовании процессов автоматизированной обработки информации и инструментально-контрольном обследование процессов автоматизированной обработки информации.

4.3. Требования к анализу имеющихся мер и средств защиты информации

В процессе проведения анализа, имеющихся средств защиты информации в АИС, должны быть получены следующие данные:

– наличие мер и средств защиты информации от физического доступа к ним;

– наличие мер и средств защиты информации от утечки информации по техническим каналам;

– наличие мер и средств защиты информации от несанкционированного доступа;

– наличие мер и средств защиты информации от программно-математических воздействий;

– наличие мер и средств защиты информации от электромагнитных воздействий.

4.4. Требования к анализу существующей организационной структуры и организационно-распорядительной документации по обеспечению безопасности информации.

В процессе проведения анализа должны быть получены следующие данные:

– наличие организационной структуры по обеспечению безопасности информации в АИС;

– наличие и состав документов, регламентирующих процесс обработки информации в АИС (регламенты, соглашения по организации информационного взаимодействия, положения о конфиденциальности и т.п.);

– наличие и содержание должностных инструкций лиц, администрирующих средства защиты информации в АИС;

– наличие и содержание должностных инструкций персонала, участвующего в обработке информации.

4.5. Требования к разработке Модели угроз безопасности при их обработке в информационных системах.

Модель угроз должна быть разработана в соответствии со следующими документами:

– «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена 14 февраля 2008 года Федеральной службой по техническому и экспортному контролю Российской Федерации (далее ФСТЭК России);

– «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утверждена 15 февраля 2008 года ФСТЭК России).

4.5.1. Требования к разработке пакета документов для обеспечения организационных мероприятия по защите персональных данных.

Пакет документов должен содержать:

– проект положения о защите персональных данных;

– проект приказа о назначении ответственных лиц за обработку информации;

– проект концепции информационной безопасности;

– проект политики информационной безопасности;

– проект технического паспорта объекта информатизации;

– проект описания информационных технологий, применяемых для обработки конфиденциальной информации и персональных данных (раздел Технического паспорта);

– проект перечня программного обеспечения, установленного в автоматизированной системе (раздел Технического паспорта);

– проект перечня защищаемых информационных ресурсов в автоматизированной системе (раздел Технического паспорта);

– проект разрешительной системы доступа (матрицы доступа) к информационным (программным) ресурсам в автоматизированной системе (раздел Технического паспорта);

– проект описания технологического процесса обработки информации (раздел Технического паспорта);

– проект инструкции по резервированию;

– проект приказа о создании комиссии по классификации и обследованию помещений, предназначенных для обработки персональных данных;

– проект приказа о назначении администратора безопасности информации в автоматизированных системах объектов информатизации и возложении на него функциональных обязанностей;

– ежегодный План мероприятий по защите информации (с графой об отметке, о выполнении);

– журнал по учету мероприятий по контролю обеспечению защиты ПДн;

– журнал учета обращений субъектов ПДн о выполнении их законных прав;

– проект функциональных обязанностей администратора безопасности информации в автоматизированных системах объектов информатизации;

– проект данных по уровню подготовки кадров, обеспечивающих защиту информации, в автоматизированной системе;

– проект журнала регистрации машинных носителей информации;

– проект инструкции по работе пользователей в автоматизированной системе;

– проект инструкции по парольной защите;

– проект инструкции по антивирусной защите;

– проект описи разработанных документов.

4.5.1.1. Требования к содержанию проекта технического паспорта АИС:

– полное и сокращенное наименование автоматизированной системы;

– расположение автоматизированной с указанием почтовых адресов, этажей и номеров или наименований помещений;

– состав технических средств, используемых при обработке защищаемой информации с указанием их типа, фирмы-производителя, модели, номера (учетного, заводского, инвентарного) и места размещения;

– состав технических средств, не используемых при обработке защищаемой информации, но размещенных в одних помещениях с техническими средствами, используемыми при обработке конфиденциальной информации с указанием их типа, фирмы-производителя, модели, номера (учетного, заводского, инвентарного) и места размещения;

– перечень применяемых средств защиты информации с указанием их типа, фирмы-производителя, модели, номера сертификата соответствия по требованиям безопасности информации и сроках его действия, места размещения;

– схемы расположения зданий и прилегающей к ним территории;

– схемы расположения помещений на этаже (на этажах);

– схемы помещений, в которых расположены технические средства, обрабатывающие конфиденциальную информацию и персональные данные с указанием расположения всех технических средств, систем, линий и коммуникаций, в том числе транзитных;

– схемы прокладки линий и расположения оконечных и распределительных устройств электропитания в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных и распределительных устройств освещения в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных устройств электрического заземления;

– схемы размещения систем и коммуникаций центрального отопления в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных и распределительных устройств телефонной связи в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных и распределительных устройств локальной вычислительной сети в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных и распределительных устройств пожарной сигнализации в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы прокладки линий и расположения оконечных и распределительных устройств охранной сигнализации в целом в организации (здании) и в помещениях, в которых расположены технические средства;

– схемы коммутации сетевого оборудования вычислительных сетей с указанием портов подключения технических средств, назначения и номеров таких средств;

– схемы информационных потоков между логическими узлами автоматизированной системы с указанием способов или средств передачи таких потоков;

– функциональная схема сети связи к которой подключены технические средства, с указанием функциональных узлов, средств коммутации, характеристиками каналов и линий передачи информации, применяемых информационных технологий в части касающейся обрабатываемых в такой сети конфиденциальной информации и персональных данных;

– описание технологического процесса обработки конфиденциальной информации и персональных данных на технических средствах с указанием вида, издавшего органа, номера, даты принятия и наименования нормативно-правового акта, в том числе локального, или иного документа определяющего, регламент такой обработки (в том числе, с применением специального программного обеспечения и средств защиты информации);

– перечень и характеристика используемых в технических средствах, обрабатывающих конфиденциальную информацию и персональные данные, программных средств (средств доступа к информации) с указанием назначения программного продукта, наименованием фирмы-производителя, наименованием программного продукта, его версии, места установки и серийного номера;

– требования по доступу к аппаратным ресурсам технических средств, обрабатывающих конфиденциальную информацию и персональные данные с указанием таких аппаратных средств и устанавливаемых требований по доступу к ним;

– перечень субъектов доступа к техническим средствам обработки конфиденциальной информации и персональных данных с указанием должности, фамилии, имени, отчества, имени пользователя в операционной системе (login) и уровня полномочий (в операционной системе);

– перечень объектов доступа в технических средствах обработки конфиденциальной информации и персональных данных с указанием типа информации и путей (локальных, сетевых) доступа к ресурсам;

– описание реализованных правил разграничения доступа (матрицы доступа) к используемым в технических средствах обработки конфиденциальной информации и персональных данных аппаратным ресурсам с указанием имени пользователя в

операционной системе (login), перечнем действий с аппаратными ресурсами и полномочиями по их использованию для каждого заявленного пользователя;

– описание реализованных правил разграничения доступа (матрицы доступа) к используемым в технических средствах обработки конфиденциальной информации и персональных данных программным средствам с указанием имени пользователя в операционной системе (login), установленного программного обеспечения и полномочий по его использованию для каждого заявленного пользователя;

– описание реализованных правил разграничения доступа (матрицы доступа) к ресурсам, содержащим персональные данные в технических средствах обработки персональных данных и ресурсам, содержащим информацию, назначением которых, является обеспечение безопасности обрабатываемой информации, с указанием имени пользователя в операционной системе (login), местом размещения такого ресурса и полномочий по его использованию для каждого заявленного пользователя.

5. ОСНОВНЫЕ ЗАДАЧИ ПО ПРОЕКТИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ АИС ЯВЛЯЮТСЯ:

Создание системы защиты информации, обеспечивающей конфиденциальность, целостность и достоверность информации, обрабатываемых в АИС, исключающую несанкционированный, в том числе случайный доступ к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий.

5.1. Требования к проектированию системы защиты информации АИС

5.1.1. Требования к структуре и функционированию системы

– система защиты информации должна обеспечивать защищенность информации от неправомерных действий при их хранении, обработке и передаче по каналам связи;

– при построении СЗИ должны быть выполнены требования по обеспечению безопасности КИ и ПДн при их обработке в информационных системах;

– при создании СЗИ должны использоваться сертифицированные по требованиям ФСТЭК России «Защита от НСД к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню не ниже 2-го;

– при создании СЗИ должны использоваться сертифицированные по требованиям ФСТЭК России «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации» не ниже 3-го класса;

– при создании СЗИ должны использоваться сертифицированные по требованиям ФСТЭК России для применения в информационных системах персональных данных (ИСПДн) **до класса защищенности ИС – К1,** в соответствии с Приказом ФСТЭК от 11 февраля 2013 г. № 17, **и уровня защищенности УЗ 1** в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 включительно;

– при создании СЗИ должны использоваться сертифицированные по требованиям ФСТЭК России для защиты информации в автоматизированных системах по классу защищенности **не ниже 1Б**;

СЗИ должно осуществлять:

- защиту серверов и рабочих станций от НСД;
- контроль входа пользователей в систему, в том числе и с использованием аппаратных средств защиты;
- разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;
- разграничение доступа пользователей к информации;
- контроль утечек информации;
- регистрацию событий безопасности и аудит.

Требования к операционной платформе и аппаратной части:

- 32-битные операционные системы: MS Windows Server 2003 SP2, MS Windows Server 2003 R2 SP2, MS Windows Server 2008 SP2, MS Windows XP Professional SP3, MS Windows Vista SP2, MS Windows 7 SP1; MS Windows 8/8.1;
- 64-битные операционные системы: MS Windows Server 2003 x64 Edition SP2, MS Windows Server 2003 R2 x64 Edition SP2, MS Windows Server 2008 x64 Edition SP2, MS Windows Server 2008 R2 x64 Edition SP1, MS Windows XP Professional x64 Edition SP2, MS Windows Vista x64 Edition SP2, MS Windows 7 x64 Edition SP1; MS Windows 8/8.1;Windows Server 2012/Server 2012 R2;
- Active Directory/ADAM/LDS (для применения СЗИ с централизованным управлением);
- наличие привода CD-ROM;
- в случае совместного применения средств доверенной загрузки - наличие свободного разъёма системной шины стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В, или свободный разъем PCI-Express.

Требования к функциональности:

- может функционировать совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей;
- может функционировать совместно с персональными идентификаторами (для обеспечения усиленной аутентификации пользователей);
- поддерживать персональные идентификаторы iButton (при совместном использовании со средствами доверенной загрузки), eToken PRO, eToken PRO Java (в форм-факторах USB и смарт карт), Rutoken;
- должно обеспечивать автоматическую блокировку автоматизированной системы при изъятии персонального идентификатора пользователя;
- поддержка терминального режима работы пользователей для платформ Microsoft и Citrix, а так же при использовании бездисковых рабочих станций (“тонких клиентов”);
- контроль устройств:
  - последовательные и параллельные порты;
  - локальные устройства
  - сменные, логические и оптические диски;
  - USB – устройства,
  - устройства PCMCI,
  - устройства IEEE1394,
  - устройства Secure Digital;

- контроль устройств подключаемых/отключаемых в процессе работы автоматизированной системы;
- контроль неизменности аппаратной конфигурации компьютера;
- управление подключениями (IrDA, WiFi, FireWire, Ethernet, Bluetooth);
- контроль вывода информации на отчуждаемые носители;
- теневое копирование отчуждаемой информации;
- разграничение доступа к принтерам;
- контроль буфера обмена Windows;
- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера;
- должно обеспечивать автоматическую настройку механизмов защиты при добавлении в систему приложения, обрабатывающего конфиденциальную информацию;
- возможность выбора уровня конфиденциальности сессии для пользователя;
- разграничение доступа пользователей к конфиденциальным данным и приложениям;
- мандатное управление доступом, включая – к устройствам;
- контроль вывода конфиденциальных данных на печать, управление грифами конфиденциальности при печати конфиденциальных и секретных документов;
- контроль целостности файлов, каталогов, элементов системного реестра;
- возможность контроля целостности до загрузки операционной системы (при совместном применении со средствами доверенной загрузки);
- функциональный контроль ключевых компонентов системы;
- - автоматическое затирание данных на диске при удалении конфиденциальных файлов пользователем;
- регистрация событий безопасности в журнале безопасности;
- возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа;
- возможность формирования отчетов по результатам аудита;
- реакции СЗИ при нарушении целостности:
  - регистрацию события в журнале;
  - блокировку компьютера;
  - восстановление повреждённой/модифицированной информации;
  - отклонение или принятие изменений;
- функциональный самоконтроль подсистем защиты.

Требования к централизованному управлению в доменной сети:

- централизованный мониторинг и оперативное управление рабочими станциями;
- централизованный сбор и хранение журналов безопасности, регистрация событий безопасности;
- аудит безопасности, формирования отчетов по результатам аудита;
- возможность создания централизованной политики безопасности по использованию отчуждаемых USB носителей информации;
- возможность создания централизованной политики замкнутой программной среды;
- возможность интеграции с политиками безопасности Active Directory;

- централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу;
- должно обеспечивать создание доменов безопасности в территориально-распределенной сети, при этом предоставляется возможность делегирования административных полномочий по информационной безопасности;
- возможность создания отчетов по перечню установленного ПО, сведениям о ресурсах, объектах и параметрах защищаемого компьютера;

Требования по сертификации:

- должно быть сертифицировано на соответствие требованиям ФСТЭК России для применения в информационных системах персональных данных (ИСПДн) до класса К1 включительно;
- показатель защищенности от НСД (Гостехкомиссия России, 1999) не ниже 3-го класса защищенности. Классификация по уровню отсутствия НДВ (Гостехкомиссия России, 1999) – не ниже 2-го уровня контроля;
- может использоваться при создании автоматизированных систем до класса защищенности 1Б включительно.
- должны использоваться сертифицированные на соответствие требованиям руководящих документов не ниже 4-го класса защиты для системы обнаружения вторжений и не ниже 4-го класса защищенности для межсетевого экрана, средства защиты информации.

– средства защиты КИ и ПДн должны быть совместимы с программными и аппаратными средствами автоматизированной обработки информации, используемыми в АИС в настоящее время;

– предлагаемые решения должны максимально учитывать инвестиции в эксплуатируемые сертифицированные средства защиты информации;

– с каждым комплектом продукции должна поставляться эксплуатационная и техническая документация на русском языке, а также копия действующего сертификата средств защиты информации по требованиям безопасности информации и входить в государственный реестр сертифицированных средств защиты информации.

При разработке технического решения по построению системы защиты информации состав подсистем и требования к ним, **уточняются** Исполнителем и Заказчиком в зависимости от особенностей и (или) изменений и в соответствии с руководящими документами ФСТЭК и ФСБ России.

В случае необходимости, за свой счёт и своими силами закупить всё недостающее оборудование, программное обеспечение (Операционные системы, офисное ПО, серверное ПО, ПО для работы с Базами Данных и т.д.), устройства защиты от утечки информации по техническим каналам предназначенное для защиты объектов ВТ (вычислительной техники) от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств и другие необходимые для проведения работ устройства и материалы, в том числе автоматизированные рабочие места, предварительно согласовав характеристики поставляемого оборудования и материалов с Заказчиком.

6. ОСНОВНЫЕ ЗАДАЧИ ПО ПРОВЕДЕНИЮ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ АИС

В соответствии с нормативно-методическими документами РФ Исполнитель обязуется оказать услуги и провести работы по созданию системы защиты информации на автоматизированных рабочих местах, включая аттестационные испытания автоматизированной информационной системы. Указанные услуги должны включать в себя следующие виды работ:

– Поставка, настройка и установка средств защиты информации, в том числе технических для защиты информации ограниченного доступа (конфиденциальная информация и персональные данные);

– Поставка в случае необходимости программного обеспечения (Операционные системы, офисное ПО, серверное ПО, ПО для работы с Базами Данных и т.д.) и устройств защиты от утечки информации по техническим каналам предназначено для защиты объектов ВТ (вычислительной техники) от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств, для функционирования средств защиты информации, средств вычислительной техники-Локальной вычислительной сети (ЛВС);

– Проведение аттестационных испытаний АИС по обработке персональных данных и конфиденциальной информации.

На стадии **Поставки**, настройки и установки средств защиты информации для защиты АС ИСПДн по обработке персональных данных и конфиденциальной информации Исполнителю необходимо:

– осуществить поставку, настройку и установку всех необходимых для проведения аттестационных испытаний средств защиты информации, в том числе **технических средств защиты** от утечек по каналам ПЭМИН;

– осуществить поставку в случае необходимости программного обеспечения (Операционные системы, офисное ПО, серверное ПО, ПО для работы с Базами Данных и т.д.) и устройств защиты от утечки информации по техническим каналам предназначено для защиты объектов ВТ (вычислительной техники) от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств для функционирования средств защиты информации, средств вычислительной техники-Локальной вычислительной сети (ЛВС);

– совместно с Заказчиком выполнить мероприятия по организации охраны и физической защиты помещений, исключающей НСД к техническим средствам, их хищение и нарушение работоспособности, хищение носителей информации;

– осуществить инструктаж лиц, использующих средства защиты информации, применяемые в АИС, правилам работы с ними.

На стадии Проведения **аттестационных** испытаний АИС Исполнителю необходимо провести следующие мероприятия:

– Анализ и оценку исходных данных, полученных в ходе предварительного обследования, анализ организационной структуры Заказчика. Проверку условий размещения, монтажа и эксплуатации технических средств и СЗИ, изучение технологического процесса обработки, передачи и хранения информации, анализ

информационных потоков, определение состава использованных для обработки, передачи и хранения информации технических средств.

– Испытания технических и программных средств АИС (серверов, рабочих станций операторов), средств и систем защиты информации на соответствие требованиям защиты информации по утвержденным и согласованным с Заказчиком Программе и методикам проведения аттестационных испытаний.

– Проведение комплексных Аттестационных испытаний АИС на соответствие требованиям по защите информации с использованием экспертно-документальных и инструментальных методов.

– Проведение **инструментального контроля защищенности информации в линиях связи ЛВС стандарта 100BASE-TX от утечки по каналам побочных электромагнитных излучений** в ходе аттестационных испытаний;

– Подготовку и оформление отчетной документации по результатам проведения Аттестационных испытаний – протоколов испытаний и Заключения по результатам аттестационных испытаний, а так же Аттестата соответствия по требованиям безопасности информации для автоматизированной информационной системы.

Обязательным условием проведения аттестационных испытаний является проведение тестов на проникновение извне (тест на вторжение) — моделирование действий злоумышленника по проникновению в информационную систему АИС в условиях максимально приближённых к реальному взлому с целью обнаружения уязвимостей в защите сети:

- технологический тест на проникновение;
- социотехнический тест на проникновение;
- комплексный тест на проникновение.

Инструментально-контрольное обследование, инструментальный контроль, а также иные виды работ проводятся инструментально-контрольными средствами, инструментальными средствами контроля защищенности информационных систем и иными средствами Исполнителя.

Наличие у Исполнителя сертификатов и (или) лицензий на указанные средства обязательно.

Количество и тип средств вычислительной техники (сервера, рабочие станции и др.) по каждой информационной системе основной деятельности в соответствии с их (СВТ) размещением на объектах, необходимо получить Исполнителю государственного контракта при проведении инвентаризация информационных систем, обрабатывающих персональные данные (определение архитектуры, конфигурации и топологии систем в целом и их отдельных компонент) при экспертно-документальном обследовании процессов автоматизированной обработки персональных данных и инструментально-контрольном обследование процессов автоматизированной обработки персональных данных.

В случае необходимости, за свой счёт и своими силами закупить всё недостающее оборудование, программное обеспечение (Операционные системы, офисное ПО, серверное ПО, ПО для работы с Базами Данных и т.д.), устройств защиты от утечки информации по техническим каналам предназначено для защиты объектов ВТ (вычислительной техники) от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии

вспомогательных технических средств и другие необходимые для проведения работ устройства и материалы, в том числе автоматизированные рабочие места, предварительно согласовав характеристики поставляемого оборудования и материалов с Заказчиком.

7. ОСНОВНЫЕ ЗАДАЧИ ПО ПРОВЕДЕНИЮ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ЗП:

В состав мероприятий по аттестации требованиям по безопасности информации защищаемых помещений входят:

– Разработка проектов организационно-распорядительных документов, определяющих режим безопасности информации в помещении, лиц, ответственных за защиту информации в помещении, правила работы со средствами защиты информации.

– Рекомендации по исключению неиспользуемых технических средств из помещения, или технических средств, создающих предпосылки к нарушению информационной безопасности.

– Установка и настройка сертифицированных по требованиям безопасности систем защиты от утечки по акустическому и виброакустическому каналам.

– Испытания ограждающих конструкций и инженерных коммуникаций помещения на соответствие требованиям руководящих документов ФСТЭК России по защите информации от утечек по акустическому и виброакустическому каналам с применением контрольно-измерительного оборудования:

- измеряются уровни акустического сигнала и шумов в октавных полосах частот со среднегеометрическими частотами в местах возможной установки микрофонных датчиков средств речевой разведки;
- измеряются уровни вибрационного сигнала и шумов в октавных полосах частот со среднегеометрическими частотами в местах возможной установки датчиков контактного типа средств речевой разведки;
- определяются коэффициенты звукоизоляции ограждающих конструкций (окон, дверей, стен, пола, потолка) выделенного помещения в октавных полосах частот со среднегеометрическими частотами;
- определяются коэффициенты виброизоляции ограждающих конструкций выделенного помещения, а также различных элементов инженерно-технических систем, включая их коммуникации, в октавных полосах частот со среднегеометрическими частотами;
- при использовании в выделенном помещении систем виброакустической маскировки дополнительно проводятся измерения уровней акустический и вибрационных шумов в октавных полосах частот со среднегеометрическими частотами в местах возможной установки датчиков средств акустической разведки;
- измеряются уровни информационных сигналов на выходе ВТСС, возникающих вследствие акустоэлектрического преобразования акустических сигналов элементами ВТСС, в октавных полосах частот со среднегеометрическими частотами;
- измеряются уровни шумов на выходе в октавных полосах частот со среднегеометрическими частотами.

– Испытания технических средств в помещении на соответствие требованиям руководящих документов ФСТЭК России по защите информации от утечек по каналу электроакустических преобразований с применением контрольно-измерительного оборудования.

– Разработка организационных требований к эксплуатации помещения.

– Инструктирование специалистов клиента правилам работы системами защиты информации и их техническому обслуживанию.

8. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ОБУЧАЮЩЕГО ПРОЦЕССА:

Наличие следующих дисциплин в учебном плане:

– общие вопросы технической защиты информации;

– правовые и организационные вопросы технической защиты информации в области обеспечения безопасности персональных данных;

– выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа;

– организация обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, организационные и технические меры защиты информации в информационных системах персональных данных;

– основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в системах персональных данных;

– практические реализации типовых моделей защищенных информационных систем обработки персональных данных.

После изучения курса должен:

Знать:

- основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;
- основные виды угроз безопасности персональных данных в информационных системах персональных данных;
- содержание и порядок организации работ по выявлению угроз безопасности персональных данных;
- процедуры задания и реализации требований по защите информации в информационных системах персональных данных;
- меры обеспечения безопасности персональных данных;
- требования по обеспечению безопасности персональных данных;
- порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

Уметь:

- создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;
- планировать мероприятия по обеспечению безопасности персональных данных;
- обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;
- проводить оценки актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

Владеть:

- навыками работы с правовыми базами данных;
- навыками определения уровней защищённости персональных данных;
- навыками выявления угроз безопасности персональных данных в информационных системах персональных данных;
- навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;
- навыками применения сертифицированных средств защиты информации.

Общие требования к услуге

– осуществлять итоговый контроль знаний слушателей в форме экзамена, состоящего из тестирования;

– организовать учебный процесс и обеспечить слушателей необходимыми учебно-методическими материалами для освоения образовательной программы;

– обновление знаний, совершенствование навыков, а также выработка умений самостоятельно ставить и решать конкретные профессиональные задачи.

Обязательное применение мультимедийных, компьютерных и интернет-технологий.

9. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ

8.1. Требования к используемым технологиям

Создание системы защиты информации должно осуществляться на базе применения современных информационных технологий и обеспечивать:

– расширяемость и гибкость управления конфигурацией системы;
– надежность и отказоустойчивость аппаратных и программных средств системы.

Средства защиты должны быть совместимы с программными и аппаратными средствами автоматизированной обработки и защиты информации, используемыми Заказчиком.
Архитектура системы защиты информации должна быть открытой, масштабируемой и строиться по модульному принципу, каждый модуль должен обеспечивать свою часть функциональности решения задач в целом.

8.2. Требования к гарантийному сопровождению

Разработчиком системы защиты информации должен быть обеспечен не менее чем в 12 месяцев с момента приемки системы в эксплуатацию базовый набор услуг по гарантийному сопровождению, включающий:

– устранение ошибок, выявленных в процессе эксплуатации;
– локализацию инцидентов, связанных с неправильными действиями специалистов Заказчика;
– выезд специалиста Исполнителя к Государственному заказчику для решения проблемы на месте в течении 30 минут для оказания услуг технической и методической поддержки;
– консультирование специалистов Заказчика по вопросам эксплуатации в режиме «вопрос-ответ» (по телефону или посредством электронной почты).

8.3. Требования по стандартизации и унификации

Стандартизация должна охватывать все этапы разработки и внедрения СЗПДн. Выполнение услуг по созданию системы должно осуществляться в соответствии с ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».
Внесение изменений в настоящее техническое задание должно осуществляться по согласованию с Заказчиком в соответствии с положениями ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

10. ТРЕБОВАНИЯ К ПЕРСОНАЛУ

В состав персонала, необходимого для обеспечения безопасности информации на создаваемых объектах, входят следующие категории ответственных лиц:
– администраторы безопасности информации автоматизированных систем.
Данные лица выполняют следующие функциональные обязанности:
– администраторы безопасности информации – администрирование и сопровождение средств защиты информации от НСД, повседневный контроль СЗИ.
В рамках проведения работ Исполнитель должен провести инструктаж указанных должностных лиц по порядку работ с установленными системами защиты информации и выполнения мероприятий по защите информации.

11. ОБЩИЕ ТРЕБОВАНИЯ К ОКАЗАНИЮ УСЛУГ, ИХ КАЧЕСТВУ, В ТОМ ЧИСЛЕ ТЕХНОЛОГИИ ОКАЗАНИЯ УСЛУГ, МЕТОДАМ И МЕТОДИКИ ОКАЗАНИЯ УСЛУГ.

Все мероприятия по созданию системы защиты персональных данных должны осуществляться в соответствии с требованиями:

– Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 № 17;

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено приказом ФСТЭК России от 18.02.2013 № 21;

– Указа Президента Российской Федерации от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера».

– Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008г.;

– Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;

– Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144;

– Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

– Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992 год;

– Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 (часть 1, часть 2, часть 3);

– Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992 год;

– ГОСТ 34.003-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения» от 01.01.1992;

– ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» от 01.01.1990;

– ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» от 01.01.1992;

– ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» от 1990-01-01;

– ГОСТ Р 51624–2000. «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования» от 30.06.2008;

– ГОСТ Р 51583–2000. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» от 01.09.2014;

– ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие положения (ДСП) от 17 апреля 2012 года;

– ГОСТ Р 53112-2008. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний от 30.09.2009;

– ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции от 01.01.2012;

– ГОСТ Р ИСО/МЭК 19791-2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем от 01.10.2009;

– Специальных требований и рекомендаций по технической защите конфиденциальной информации, утвержденных приказом Гостехкомиссии от 30 августа 2002 г. № 282;

– Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссия России от 25.07.1997;

– Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11.02.2014г.;

– Сборник Временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России, 2002 г.;

– Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638;

– Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15 марта 2012 г.

– Методика оценки защищенности высокоскоростных сетей передачи данных от утечки информации по каналам побочных электромагнитных излучений. Утвержден Заместителем председателя Государственной Технической Комиссии при Президенте РФ.