ПРИНЯТО:
Общим собранием работников
МДОАУ № 222
от «09» января 2023г.
Протокол № 1

УТВЕРЖДАЮ:
Приказом МДОАУ № 222
от «09» января 2023 г. № 4
Заведующий МДОАУ № 222
_____Н.Н. Бычкова

Бычкова Наталия Николаевна
Подписано цифровой подписью: Бычкова Наталия Николаевна
DN: cn=Бычкова Наталия Николаевна, o=МДОАУ № 222, ou, email=orensad222@gmail.com, c=RU
Дата: 2023.12.05 10:46:19 +05'00'

СОГЛАСОВАНО:
Первичной профсоюзной
организацией МДОАУ № 222
от «09» января 2023г.
Протокол № 1

ПОЛОЖЕНИЕ
по обеспечению информационной безопасности персональных данных при их обработке в информационных системах персональных данных Муниципального дошкольного образовательного автономного учреждения «Детский сад № 222»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аттестация объекта информатизации - комплекс организационно-технических мероприятий, в результате которых специальным документом – Аттестатом соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации.

Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Защита информации от несанкционированного доступа и воздействия - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, базах данных, других информационных системах), а также машинные носители информации (жёсткие магнитные диски, гибкие магнитные диски, оптические диски и т.п.);

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах или обсуждаемая в ЗП.

Информационные сети общего пользования - вычислительные (информационно-телекоммуникационные) сети, открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

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.

Инцидент информационной безопасности - появление одного или нескольких нежелательных, или неожиданных событий информационной безопасности, с которыми связана значительная вероятность реализации угрозы информационной безопасности.

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

Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Машинные носители информации - встроенные (съёмные) накопители на жёстких магнитных дисках, гибкие магнитные диски, Flash-накопители, DVD(CD)-диски, карты памяти и др. устройства, используемые для записи, накопления и хранения информации в электронном виде.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств ИСПДн.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и уничтожение.

Основные технические средства и системы – система, включающая автоматизированные рабочие места и сервера ИСПДн, соединительные линии, распределительные и коммутационные устройства.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Событие информационной безопасности - Идентифицированное появление определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место
ИБ – информационная безопасность
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МНИ – машинный носитель информации
НДВ – недекларированные возможности
НСД – несанкционированный доступ
ОС – операционная система
ОТСС – основные технические средства и системы
ПДн – персональные данные
ПО – программное обеспечение
ПЭВМ – персональная электронно-вычислительная машина
СЗИ – средства защиты информации
СЗПДн – система защиты персональных данных
ТЗ – техническое задание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее «Положение по обеспечению информационной безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – Положение) разработано в целях установления единых требований по защите персональных данных при их автоматизированной обработке в муниципальном дошкольном образовательном автономном учреждении «Детский сад № 222» (далее — Положение) (далее – Учреждение).

1.2. Настоящее Положение разработано с учетом требований следующих нормативных документов:

- Федеральный закон от 27.06.2006 г. №152-ФЗ «О персональных данных»;
- Федеральный закон РФ 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008 г.;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008 г.;
- Приказ ФСТЭК России №21 от 18 февраля 2013 года «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСБ России от 10 июля 2014 года №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности»;
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (Утв. руководством 8 Центра ФСБ России 31 марта 2015 г. №149/7/2/6-432);
- ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

1.3. Настоящее Положение является методологической основой для:

- формирования единой политики в области обеспечения информационной безопасности ПДн при их обработке в ИСПДн;
- принятия практических мер технического и организационно-технического характера, направленных на обеспечение информационной безопасности ПДн при их обработке в ИСПДн;
- организации работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению информационной безопасности ПДн;
- разработки нормативных документов Общества, регламентирующих порядок и правила обработки и обеспечения информационной безопасности ПДн при их обработке в ИСПДн.

1.4. Настоящее Положение определяет:

- порядок моделирования угроз безопасности ПДн при их обработке в ИСПДн;
- порядок определения необходимых уровней защищенности ПДн при их обработке в ИСПДн;
- порядок определения требований к организационным и техническим мерам по обеспечению безопасности ПДн при их обработке в ИСПДн;

– порядок предоставления доступа работникам Общества к ресурсам ИСПДн;

– требования к составу и содержанию документов, регламентирующих порядок и правила обеспечения информационной безопасности ПДн;

– требования к организации повышения осведомленности персонала по вопросам обеспечения ИБ ПДн;

– требования к учету и обращению электронных (машинных) носителей информации, содержащей ПДн;

– полномочия и ответственность работников за обеспечение безопасности ПДн при их обработке в ИСПДн.

1.5. Настоящее Положение предназначено для работников подразделений Общества, непосредственно связанных с организацией защиты ПДн в ИСПДн Общества.

2. ХАРАКТЕРИСТИКА ИСПДн КАК ОБЪЕКТА ЗАЩИТЫ

2.1. ИСПДн Общества - сегмент информационно-вычислительной сети Обществе, включающий АРМ пользователей, участвующих в обработке ПДн, линии передачи данных, периферийное и сетевое оборудование, технологические сервера и сервера баз данных, рабочие места администраторов ИСПДн.

2.2. Объектом защиты являются информационные ресурсы, содержащие ПДн различных категорий субъектов ПДн.

2.3. Состав, цели и сроки обработки ПДн определены в «Положении по обработке персональных данных…».

2.4. Защите должны подвергаться средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации и другие технические средства обработки графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), средства защиты информации, используемые для обработки и защиты ПДн.

2.5. На каждую ИСПДн должен быть разработан Технический паспорт, структурно содержащий следующие разделы:

– Общие сведения об ИСПДн:
  а. наименование ИСПДн;
  б. расположение ИСПДн;
  в. необходимый уровень защищенности ПДн (с указанием номера и даты утверждения акта определения необходимого уровня защищенности ПДн).

– Состав оборудования ИСПДн (состав ОТСС с указанием типа и заводского номера);

– Сведения о структуре, топологии и размещении ОТСС относительно границ контролируемой зоны Общества:
  а. структурная (топологическая) схема с указанием информационных связей между устройствами;
  б. схема размещения и расположения ОТСС с привязкой к границам контролируемой зоны.

– Состав средств защиты информации (с указанием наименования и типа технического средства, заводского (серийного) номера, сведений о наличии сертификатов соответствия требованиям по безопасности информации, сведений о месте и дате установки).

– Сведения об используемых программных средствах.

– Сведения об аттестации ИСПДн на соответствие требованиям по безопасности информации:
  а. инвентарные номера аттестата соответствия;
  б. инвентарные номера заключения по результатам аттестационных испытаний;

в. инвентарные номера протоколов испытаний и даты их регистрации.

– Сведения о результатах периодического контроля (с указанием: даты проведения периодического контроля; наименования организации, проводившей контроль; результатов проверки, номера отчетного документа).

3. ЖИЗНЕННЫЙ ЦИКЛ ИСПДн

3.1. Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ, выполняемых в рамках жизненного цикла ИСПДн.

3.2. Рекомендуемый состав этапов жизненного цикла ИСПДн приведен в Таблице 1.

Таблица 1. Жизненный цикл ИСПДн

№	Этап ЖЦ ИСПДн	Описание этапа
1.	**Определение состава ИСПДн**	
1.1.	определение необходимости обработки ПДн в ИСПДн	На данном этапе: 1. определяются информационные системы, в которых ведется обработка ПДн; 2. определяется необходимость ведения такой обработки.
1.2.	сбор информации об ИСПДн	На данном этапе для каждой ИСПДн производится: - определение состава ПДн, которые будут обрабатываться в ИСПДн; - определение целей обработки ПДн, действий, выполняемых с ПДн, допустимых сроков хранения ПДн; - определение состава ОТСС; - определение степени участия персонала в обработке ПДн.
1.3.	определение предварительной категории ПДн	В ИСПДн могут обрабатываться следующие категории ПДн: - биометрические; - специальные; - общедоступные; - иные. Кроме того, данные ПДн могут быть: - ПДн работников; - ПДн субъектов, не являющихся работниками. На данном этапе также необходимо определить количество субъектов ПДн, чьи ПДн обрабатываются в ИСПДн (для каждой ИСПДн).
1.4.	определение возможности оптимизации ИСПДн	На данном этапе для каждой ИСПДн определяется возможность: - исключения избыточных ПДн; - обезличивания ПДн, обрабатываемых в ИСПДн.
2.	**Моделирование угроз и определение требований к СЗПДн**	
2.1.	разработка моделей угроз и нарушителя безопасности ПДн	Для каждой ИСПДн разрабатывается «Модель угроз и вероятного нарушителя информационной безопасности».
2.2.	определение необходимого уровня защищенности ПДн и (при необходимости) класса защищенности ПДн	По результатам моделирования угроз и определения актуальности угроз НДВ, для каждой ИСПДн определяется необходимый уровень защищенности ПДн в соответствии с ПП РФ №1119.
2.3.	определение наборов организационных и технических мер по защите ПДн при их обработке в ИСПДн	На данном этапе производится определение требований к системе защиты персональных данных. В соответствии с положениями Приказа №21 ФСТЭК России происходит определение наборов базовых и компенсирующих мер по защите ПДн при их обработке в ИСПДн.
2.4.	разработка технического задания на разработку СЗПДн	На основе наборов базовых и компенсирующих мер по защите ПДн при их обработке в ИСПДн формируются требования для каждой из подсистем СЗПДн. На основе этих требований разрабатывается техническое задание на построение СЗПДн.
3.	**Разработка Технического проекта на построение СЗПДн**	
3.1.	разработка Технического проекта на построение СЗПДн	На данном этапе разрабатывается Технический проект на построение СЗПДн, содержащий: - ведомость технического проекта; - ведомость покупных изделий; - пояснительную записку;

№	Этап ЖЦ ИСПДн	Описание этапа
		- описание комплекса технических средств.
4.	**Техническое обеспечение СЗПДн**	
4.1.	выбор поставщика	Выбор поставщика программных и программно-аппаратных технических СЗИ.
4.2.	приобретение СЗИ	В соответствии с Техническим проектом осуществляется закупка необходимых программных и программно-аппаратных СЗИ.
4.3.	сертификация имеющегося оборудования	В случае, если необходимое оборудование уже приобретено, но не имеет сертификата соответствия ФСТЭК России, может организовываться его сертификация.
4.4.	передача имеющегося оборудования на сертификацию	Передача оборудования в испытательную лабораторию для оценки соответствия по требованиям безопасности информации.
4.5.	получение сертифицированного оборудования	Получение оборудования, прошедшего процедуру оценки соответствия по требованиям безопасности информации ФСТЭК России и сертификата на это оборудование.
5.	**Построение СЗПДн**	
5.1.	внедрение комплекса средств и мер защиты ПДн	Производятся монтажные, пуско-наладочные работы средств защиты информации. Производится реализация комплекса организационно-технических мероприятий по защите ПДн.
5.2.	определение подразделений и лиц, ответственных за эксплуатацию средств защиты информации	На данном этапе работникам назначаются роли по администрированию используемых средств защиты информации.
5.3.	реализация разрешительной системы доступа	На данном этапе формируется Матрица доступа (разрешительная система доступа) к ресурсам ИСПДн
5.4.	разработка эксплуатационной документации на ИСПДн	Производится разработка положений, регламентов, инструкций, определяющих порядок и правила обеспечения информационной безопасности при работе в ИСПДн, порядок эксплуатации СЗИ
6.	**Повышение осведомленности работников**	
6.1.	ознакомление сотрудников с нормативными документами в области защиты ПДн	На данном этапе осуществляется ознакомление работников с эксплуатационной документацией на ИСПДн, используемые средства защиты информации.
6.2.	обучение работников по обеспечению информационной безопасности ПДн	При необходимости организовывается обучение работников по обеспечению информационной безопасности ПДн. Обучение может проводиться как силами подразделений Общества, ответственных за обеспечение информационной безопасности ПДн, так и с привлечением сторонних организаций.
7.	**Проведение оценки соответствия требованиям по безопасности персональных данных**	
7.1.	подготовка к проведению оценке соответствия требованиям по безопасности персональных данных (в т.ч. в форме аттестационных испытаний)	Заключение договора с компанией-лицензиатом ФСТЭК России на проведение аттестационных испытаний.
7.2.	согласование программы	Согласование программы и методики проведения

№	Этап ЖЦ ИСПДн	Описание этапа
	и методики проведения аттестационных испытаний	аттестационных испытаний с компанией-лицензиатом ФСТЭК России.
7.3.	оценка соответствия ИСПДн требованиям по безопасности ПДн	Проведение аттестационных испытаний силами компании-лицензиата ФСТЭК России, согласование протоколов испытаний и заключений по результатам аттестационных испытаний. Получение аттестата соответствия требованиям по безопасности информации.
8.	**Эксплуатация ИСПДн**	
8.1.	допуск персонала к обработке ПДн в ИСПДн	Ведение учета лиц, допущенных к обработке ПДн в ИСПДн.
8.2.	проведение контрольных мероприятий	На данном этапе проверяются: - соответствие принятых мер по обеспечению безопасности ПДн; - своевременность и полнота выполнения требований настоящего Положения и других документов по обеспечению безопасности ПДн, в т.ч. ведение журналов учета, актуальность разрешительной системы доступа к ресурсам ИСПДн; - эффективность применения организационных и технических мер по защите ПДн.
8.3.	контроль изменений в составе и структуре ИСПДн	Проверка соответствия состава и структуры ИСПДн Техническим паспортам на них.
8.4.	резервное копирование ПДн	Осуществление резервного копирования ПДн.
8.5.	эксплуатация ИСПДн	Работа в ИСПДн в соответствии с эксплуатационной документацией
9.	**Изменение состава и структуры ИСПДн**	
9.1.	оценка предполагаемой модернизации ИСПДн	Проводится анализ: - возможности изменения уровня защищенности ПДн, актуальных угроз, требований к СЗПДн; - необходимости корректировки эксплуатационной документации на ИСПДн; - необходимости проведения дополнительных организационных и технических мероприятий по защите ПДн.
9.2.	реализация мероприятий в соответствии с этапами 1-7 настоящей Таблицы	Пересмотр моделей угроз и нарушителя, требований к СЗПДн. Доработка эксплуатационной документации на ИСПДн.
9.3.	проведение переаттестации ИСПДн	В случае внесения существенных изменений в состав ИСПДн, используемых средств защиты, необходимо организовать проведение аттестации ИСПДн.
10.	**Вывод из эксплуатации ИСПДн**	
10.1.	уничтожение ПДн	Уничтожение ПДн в процессе вывода ИСПДн из эксплуатации.
10.2.	вывод из эксплуатации ПО ИСПДн	Вывод из эксплуатации ИСПДн.

3.3. Отдельные этапы жизненного цикла ИСПДн по решению руководства Общества могут быть исключены.

4. ОПТИМИЗАЦИЯ ИСПДн

4.1. Оценка возможности оптимизации ИСПДн имеет своей целью реструктуризацию ИСПДн таким образом, чтобы выполнение требований по защите ПДн могло быть обеспечено с минимальным уровнем затрат на создание и эксплуатацию СЗПДн.

4.2. При проведении оптимизации ИСПДн должна оцениваться возможность:

- изменения категории ПДн, обрабатываемых в ИСПДн;
- обезличивания ПДн, обрабатываемых в ИСПДн;
- придания ПДн, обрабатываемых в ИСПДн, статуса общедоступных;
- изменения структуры и состава технических и программных средств ИСПДн;
- реструктуризации технологических процессов, связанных с обработкой ПДн.

4.3. Изменение категории обрабатываемых ПДн может быть осуществлено путем исключения из состава, обрабатываемых ПДн биометрических и специальных категорий ПДн. Данная мера позволяет снизить необходимый уровень защищенности ПДн и, как следствие, состав организационных и технических мер по защите, предъявляемых к соответствующему уровню защищенности ПДн.

4.4. Обезличивание ПДн осуществляется в соответствии положениями Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) от 05.09.2013 г. №996 «Об утверждении требований и методов по обезличиванию персональных данных», а также методическими рекомендациями по его применению, утвержденными Руководителем Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций 13.12.2013 г.

4.5. Обезличивание персональных данных и отнесение ПДн к общедоступным позволяет избежать необходимости обеспечения конфиденциальности обрабатываемых ПДн. Отсутствие необходимости защиты конфиденциальности ПДн не снимает необходимости защиты других характеристик безопасности (целостности, доступности и т.п.).

4.6. Придание ПДн статуса общедоступных возможно в следующих случаях:

- при наличии федерального закона, определяющего, что данный состав ПДн является общедоступным;
- при наличии возможности сбора согласий у субъектов на внесение их ПДн в общедоступные источники.

4.7. Изменение структуры и состава технических и программных средств ИСПДн, технологических процессов обработки ПДн может проводиться с целью:

- уменьшения количества компонентов ИСПДн (серверов, АРМ, необходимых средств защиты и пр.);
- изменения состава угроз информационной безопасности ПДн при их обработке в ИСПДн.

5. ОСНОВНЫЕ УГРОЗЫ ПДн ПРИ ИХ ОБРАБОТКЕ В ИСПДн

5.1. При обработке ПДн в ИСПДн в Обществе рассматриваются следующие угрозы:

5.1.1. Угрозы от утечки по техническим каналам:

а. угрозы утечки акустической информации;
б. угрозы утечки видовой информации;
в. угрозы утечки информации по каналам ПЭМИН.

5.1.2. Угрозы несанкционированного доступа к информации:

а. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн:

– кража ПЭВМ;
– кража носителей информации;
– кража ключей и атрибутов доступа
– кражи, модификации, уничтожения информации;
– вывод из строя узлов ПЭВМ, каналов связи;
– несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ;
– несанкционированное отключение средств защиты.

б. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий):

– действия вредоносных программ (вирусов);
– недекларированные возможности системного ПО и прикладного ПО, предназначенного для обработки персональных данных;
– установка ПО, не связанного с исполнением служебных обязанностей.

в. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера:

– утрата ключей и атрибутов доступа;
– непреднамеренная модификация (уничтожение) информации сотрудниками;
– непреднамеренное отключение средств защиты;
– выход из строя аппаратно-программных средств;
– сбой системы электроснабжения;
– стихийное бедствие.

г. Угрозы преднамеренных действий внутренних нарушителей:

– доступ к информации, ее модификация или уничтожение лицами, не допущенными к ее обработке;
– разглашение информации, ее модификация или уничтожение лицами, допущенными к ее обработке.

д. Угрозы несанкционированного доступа по каналам связи:

– Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:
– перехват за пределами контролируемой зоны;
– перехват в пределах контролируемой зоны внешними нарушителями;
– перехват в пределах контролируемой зоны внутренними нарушителями.
– Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
– Угрозы выявления паролей по сети;
– Угрозы навязывания ложного маршрута сети;
– Угрозы подмены доверенного объекта в сети;
– Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
– Угрозы типа «Отказ в обслуживании»;
– Угрозы удаленного запуска приложений;
– Угрозы внедрения по сети вредоносных программ.

5.2. Перехват информации или воздействие на нее с использованием технических средств может вестись:

– из-за границы КЗ, из ближайших строений и транспортных средств;

– из смежных помещений, принадлежащих другим организациям и расположенных в том же здании, что и объект защиты;

– при посещении Общества посторонними лицами;

– за счет НСД к информации, циркулирующей в ИСПДн, как с помощью технических средств ИСПДн, так и через информационно-телекоммуникационные сети.

5.3. Кроме перехвата информации техническими средствами, возможно непреднамеренное попадание ПДн к лицам, не допущенным к их обработке, за счет некомпетентных, ошибочных или умышленных действий пользователей или администраторов ИСПДн.

5.4. При разработке моделей угроз безопасности информации рекомендуется наряду с угрозами, приведенными в п. 5.1 использовать актуальный на момент разработки модели перечень угроз безопасности информации, приведенных в банке данных угроз безопасности информации, сформированном ФСТЭК России (bdu.fstec.ru), применимых в отношении рассматриваемой ИСПДн с учетом ее структурно-функциональных характеристик и существующего технологического процесса обработки информации.

6. РАЗРАБОТКА МОДЕЛЕЙ УГРОЗ

6.1. Разработка моделей угроз ИБ ИСПДн осуществляется в соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. Зам. директора ФСТЭК России 15.02.2008 г.

6.2. В ходе работы по определению актуальных угроз информационной безопасности ПДн и формированию модели угроз проводится комплексное обследование ИСПДн, основными направлениями которого являются:

– анализ актуальности угроз НДВ в системном и прикладном программном обеспечении;

– анализ возможности физического доступа посторонних лиц к критичным с точки зрения защиты информации элементам ИСПДн и к объекту в целом;

– анализ возможности утечки информации по побочным электромагнитным излучениям и наводкам (ПЭМИН);

– анализ возможности перехвата информации при передаче по проводным (кабельным) линиям связи;

– анализ возможности перехвата информации при передаче по каналам радио и радиорелейной, тропосферной, космической связи;

– анализ возможности несанкционированного доступа с применением программно-аппаратных и программных средств;

– оценка актуальности угроз программно-математического воздействия;

– оценка актуальности угроз безопасности ПДн от непреднамеренных несанкционированных действий пользователей;

– анализ возможности преднамеренного или непреднамеренного воздействия вероятного нарушителя информационной безопасности ПДн;

– оценка актуальности угроз неантропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания).

6.3. Формирование перечня актуальных угроз безопасности ПДн осуществляется с учетом модели вероятного нарушителя. Производится классификация вероятных нарушителей по отношению к среде ее функционирования:

– Для внутренних нарушителей определяется роль нарушителя по отношению к ИСПДн (пользователь, администратор, обслуживающий персонал и пр.), выполняемые функции, возможности, в соответствии с выполняемыми функциями и степень опасности.

– Для внешних нарушителей приводится описание вероятных категорий субъектов, делается их предположение по квалификации и технической оснащенности и как следствие – степень их опасности.

– Определяются субъекты, рассматриваемые в качестве потенциальных нарушителей и субъекты, не рассматриваемые в качестве таковых.

– Делаются предположения о возможностях вероятного нарушителя и имеющихся средствах реализации угроз информационной безопасности, указываются основные каналы и способы реализации угроз информационной безопасности.

6.4. Обследование с целью формирования модели угроз и модели нарушителя проводится комиссией из числа работников Общества, ответственных за процессы обеспечения информационной безопасности. Для проведения обследования также могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

7. ОПРЕДЕЛЕНИЕ НЕОБХОДИМЫХ УРОВНЕЙ ЗАЩИЩЕННОСТИ ПДн

7.1. В целях определения необходимых уровней защищенности ПДн приказом Директора Общества назначается комиссия, в состав которой входят работники Общества, ответственные за процессы обеспечения информационной безопасности, а также представители структурных подразделений, являющиеся пользователями рассматриваемых ИСПДн.

7.2. Базисом для определения необходимых уровней защищенности ИСПДн и требований к подсистемам защиты СЗПДн являются разрабатываемые в соответствии требованиями Раздела 7 настоящего Положения «Модели угроз и вероятного нарушителя информационной безопасности ИСПДн».

7.3. Определение необходимых уровней защищенности осуществляется в соответствии с Постановлением Правительства РФ №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г.

7.4. При определении необходимых уровней защищенности необходимо учитывать:

– результаты моделирования угроз информационной безопасности ИСПДн;
– количество субъектов, чьи ПДн обрабатываются в ИСПДн;
– категорию обрабатываемых ПДн (общедоступные, биометрические, специальные, иные);
– категорию субъектов, чьи ПДн обрабатываются (сотрудники Общества, субъекты ПДн, не являющиеся сотрудниками Общества).

7.5. По результатам определения необходимых уровней защищенности членами комиссии оформляется акт определения необходимого уровня защищенности ПДн для каждой ИСПДн.

8. ОПРЕДЕЛЕНИЕ НЕОБХОДИМОСТИ ИСПОЛЬЗОВАНИЯ СКЗИ

8.1. Определение необходимости использования СКЗИ в целях защиты персональных данных в рассматриваемых ИСПДн осуществляется на основе анализа разработанной модели нарушителя информационной безопасности и формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн применительно к СКЗИ и среде их функционирования.

8.2. Формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн применительно к СКЗИ и среде их функционирования осуществляется в соответствии с «Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (Утв. руководством 8 Центра ФСБ России 31 марта 2015 г. №149/7/2/6-432).

8.3. В общем случае использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

– если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

– если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

8.4. К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

– передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (в т. ч., при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);

– хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

8.5. По результатам формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак на ИСПДн применительно к СКЗИ и среде их функционирования, а также с учетом класса актуальных угроз НДВ определяются требования к классу СКЗИ, необходимых к использованию в составе СЗПДн.

9. ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К СЗПДн

9.1. Формирование требований к СЗПДн осуществляется на основе Приказа ФСТЭК России №21 от 21.01.2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9.2. Для каждой ИСПДн в зависимости от архитектуры и необходимого уровня защищенности определяются наборы базовых и компенсирующих организационно-технических мер по защите ПДн при их обработке в ИСПДн.

9.3. Основными организационно-техническими мерами по защите ПДн, при их обработке в ИСПДн являются:

– реализация разрешительной системы доступа пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– учет работников, допущенных к обработке ПДн в ИСПДн;

– регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

– учет и хранение машинных носителей информации, реализация комплекса мер, исключающих их хищение, подмену и уничтожение;

– осуществление резервного копирования ПДн;

– использование средств защиты информации, сертифицированных ФСТЭК России по требованиям безопасности информации;

– использование защищенных каналов связи, в том числе с использованием сертифицированных ФСБ России средств криптографической защиты информации;

– размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории (контролируемой зоны);

– организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку ПДн;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;

– наличие работников, ответственных за обеспечение безопасности ПДн при их обработке в ИСПДн;

– отделение функциональных обязанностей по администрированию информационной инфраструктуры (системных/сетевых администраторов, ИТ-специалистов) от обязанностей администратора информационной безопасности ИСПДн Общества;

– определение персональной ответственности за обеспечение ИБ ПДн при их обработке в ИСПДн для работников Общества.

9.4. В случае, когда для обеспечения безопасности ПДн определяется необходимость применения СКЗИ, в процессе построения системы СЗПДн необходимо учитывать требования Приказа ФСБ России от 10 июля 2014 года №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством РФ требований к защите персональных данных для каждого из уровней защищенности».

10. ОБЩИЕ ТРЕБОВАНИЯ К СЗПДн

10.1. Обеспечение безопасности ПДн при их обработке в ИСПДн осуществляется путем выполнения комплекса организационных и технических мероприятий (применения технических средств) в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

10.2. СЗПДн в общем виде должна включать в себя следующие подсистемы:

– защиты информации от НСД (включает в себя управление доступом и регистрацией событий);
– антивирусной защиты;
– резервного копирования информации и восстановления после сбоев;
– межсетевого экранирования;
– обнаружения вторжений;
– анализа защищенности;
– криптографической защиты информации.

10.3. Требования, предъявляемые к функционалу каждой из подсистем СЗПДн, зависят от уровня защищенности ИСПДн и сформированных наборов базовых и компенсирующих мер по защите ПДн при их обработке в ИСПДн.

10.4. Назначение подсистем СЗПДн и общее описание их возможной реализации приведено в Таблице 2.

Таблица 2. Общие требования к подсистемам СЗПДн

Наименование подсистемы	Назначение подсистемы	Описание возможной реализации
защиты информации от несанкционированного доступа	Подсистема защиты информации от НСД предназначена для реализации следующих функций: –идентификация и проверка подлинности субъектов доступа	Подсистема защиты от НСД может быть реализована с помощью сертифицированных ФСТЭК России средств и систем защиты информации от НСД, а также применения встроенных сертифицированных механизмов защиты

Наименование подсистемы	Назначение подсистемы	Описание возможной реализации
	при входе в ИСПДн; −идентификация терминалов, узлов сети, каналов связи, внешних устройств по логическим именам; −идентификация программ, томов, каталогов, файлов, записей, полей записей по именам; −регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова. −регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам; −регистрация попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.	информации операционных систем, сертифицированных ФСТЭК по требованиям безопасности информации. При этом сертификат ФСТЭК на средство защиты информации должен соответствовать необходимому уровню обеспечения защиты персональных данных, определённому для рассматриваемой ИСПДн. В процессе реализации подсистемы защиты от НСД необходимо документально определить: −разрешительную систему доступа (матрицу доступа) к ресурсам ИСПДн; −порядок предоставления доступа к ресурсам ИСПДн; −парольную политику Общества; −состав регистрируемых событий, сроки хранения журналов регистрации.
антивирусной защиты	Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты, серверов и АРМ пользователей ИСПДн Общества.	Подсистема реализуется путем использования средств антивирусной защиты на всех элементах ИСПДн. В процессе реализации подсистемы антивирусной защиты от НСД необходимо документально определить периодичность обновления антивирусных баз, проведения антивирусных проверок на серверах и АРМ ИСПДн.
резервного копирования и восстановления информации после сбоев	Подсистема резервного копирования информации и восстановления после сбоев предназначена для обеспечения доступности ПДн, обрабатываемых в ИСПДн Общества.	Подсистема реализуется посредством организации периодического резервного копирования ПДн, резервирования технических и программных средств обработки ПДн. Состав резервируемой информации, периодичность проведения резервного копирования, правила ротации, сроки хранения резервных копий, порядок восстановления информации после сбоев должны и порядок доступа к резервным копиям быть документально определены.
межсетевого экранирования	Подсистема межсетевого экранирования предназначена для защиты сетевого периметра и сегментирования ресурсов ИСПДн от остальных объектов ИТ-инфраструктуры.	Подсистема межсетевого экранирования реализуется путем использования программно-аппаратных комплексов межсетевого экранирования, сертифицированных по требованиям безопасности информации ФСТЭК

Наименование подсистемы	Назначение подсистемы	Описание возможной реализации
		России. В процессе реализации подсистемы межсетевого экранирования необходимо документально определить политику межсетевого экранирования, включающую требования к сегментированию ЛВС Общества, правила фильтрации сетевого трафика, порядок проведения контроля целостности конфигурации средств МЭ.
обнаружения вторжений	Подсистема обнаружения вторжений предназначена для выявления сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.	Функционал подсистемы может быть реализован программными и программно-аппаратными средствами обнаружения/предотвращения вторжений (IDS/IPS). Данная подсистема реализовывается совместно с подсистемой межсетевого экранирования.
анализа защищенности	Подсистема анализа защищённости предназначена для выявления уязвимостей в программно-аппаратном обеспечении ИСПДн.	Подсистема анализа защищенности может быть реализована путем применения программного комплекса анализа защищённости, который должен обеспечивать реализацию следующих базовых функций: −проверка на уязвимости серверов со сложной конфигурацией, когда сервисы имеют произвольно выбранные порты; −определение типов и имен серверов (HTTP, FTP, SMTP, POP3, DNS, SSH) вне зависимости от их ответа на стандартные запросы; −определение RPC-сервисов и поиска уязвимостей в них, а также определения детальной конфигурации компьютера в целом; −анализ всех скриптов HTTP-серверов и поиск в них уязвимостей: SQL инъекций, инъекций кода, запуск произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting и т.п.; −проверка на нестандартные DoS-атаки; −использование механизмов, уменьшающих вероятность ложных срабатываний; −выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атак на систему. Должны быть документально

Наименование подсистемы	Назначение подсистемы	Описание возможной реализации
		определены периодичность проведения проверок, обновления баз сигнатур. Для реализации мероприятий по анализу защищенности должны быть назначены ответственные лица.
криптографической защиты информации	Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Общества, в том числе при ее передаче по каналам связи сетей общего пользования и (или) международного обмена. Подсистема реализуется внедрением средств криптографической защиты информации, сертифицированных ФСБ России по требованиям безопасности информации.	Необходимость реализации подсистемы криптографической защиты информации определяется на этапе моделирования угроз информационной безопасности ИСПДн. В случае использования средств криптографической защиты информации в целях обеспечения безопасности персональных данных при их обработке в ИСПДн Общества, эксплуатация данных технических средств должна осуществляться с учетом требований Приказа №378 ФСБ России.

11. ОБЯЗАНОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ, ОСУЩЕСТВЛЯЮЩИХ МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ПДн ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ

11.1. Общее руководство работами по защите ПДн осуществляет Директор Общества.

11.1.1. Директор Общества:

– утверждает локальные нормативные акты, регламентирующие порядок защиты ПДн при их обработке в ИСПДн Общества;

– утверждает перечень допущенных к обработке ПДн работников;

– назначает должностных лиц, ответственных за защиту ПДн в Обществе и его структурных подразделениях;

– обеспечивает условия эффективной реализации требований по защите ПДн;

– принимает решение по финансированию мероприятий, связанных с организацией обработки и защиты ПДн;

– рассматривает информацию и отчеты о состоянии защиты ПДн в Обществе.

11.2. Ответственность за реализацию необходимого комплекса мероприятий по защите ПДн в Обществе возлагается на специалиста по защите информации, функции которого включают:

– согласование с Директором Общества планов работ по ПДн, локальных нормативных актов Общества по вопросам обеспечения защиты ПДн;

– организация и проведение совещаний по вопросам защиты ПДн, в том числе:

а) по доведению результатов проверок и мониторинга состояния защиты ПДн в Обществе, его территориальных подразделениях;

б) по доведению результатов проверок уполномоченными органами;

в) по результатам служебных расследований и разбирательств по вопросам нарушения режима защиты ПДн;

г) по доведению планов работ по защите ПДн и подведению результатов их выполнения;

– согласование с Директором Общества и его заместителями бюджета необходимого для развития системы обеспечения информационной безопасности Общества, систем защиты ИСПДн,

реализации периодических мероприятий по контролю эффективности реализованных мер и средств защиты информации на объектах информатизации, мероприятий по контролю реализации требований по защите информации в подразделениях Общества;

- контроль реализации планов работ по защите ПДн;
- координация действий, связанных с обеспечением защиты ПДн в Обществе.
- согласование необходимости допуска сотрудников к работам с ПДн;
- принятие решения о прекращении работ на участках, где выявлены нарушения в обеспечении безопасности ПДн, а также о возобновлении выполнения работ после их устранения.

11.3. Оперативная деятельность и реализация мероприятий по защите ПДн в Обществе осуществляются и координируются Администратором информационной безопасности.

11.3.1. Задачами специалиста по защите информации, являются:

- определение потребностей Общества в применении мер по обеспечению защиты ПДн и внедрению средств защиты информации (в т.ч. прошедших в установленном порядке оценку соответствия требованиям по защите информации в форме сертификации) для обеспечения необходимого уровня защищенности ПДн при их обработке в ИСПДн;
- планирование мероприятий по защите ПДн;
- организация работ, связанных с выполнением требований по обеспечению информационной безопасности ПДн;
- разработка и пересмотр внутренних нормативных документов Общества по обеспечению ИБ ПДн;
- разработка и типизация решений по применению мер и средств защиты информации в Обществе и распространение типовых решений на корпоративную информационную инфраструктуру Общества;
- осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (инструкций, планов и т.д.), затрагивающих вопросы защиты ПДн;
- организация контроля выполнения требований по защите ПДн;
- организация повышения и контроля осведомленности работников Общества по вопросам организации защиты ПДн;
- непосредственное участие в реализации проектов по развитию ИТ-сервисов, внедрению новых ИСПДн в Обществе, в части формирования требований по защите ПДн, контроля выполнения требований по защите ПДн в ходе внедрения, итоговой оценки соответствия внедренных систем и сервисов установленным требованиям по защите ПДн;
- организация проведения оценки эффективности принимаемых мер и средств защиты ПДн и работ по устранению выявленных недостатков;
- осуществление надзора за ходом выполнения работ по технической защите ПДн сторонними организациями;
- руководство работами по расследованию инцидентов информационной безопасности и устранению их последствий;
- информирование в установленном порядке ответственных должностных лиц Общества об угрозах и рисковых событиях ИБ;
- пресечение несанкционированных действий нарушителей ИБ;
- организация разрешительной системы доступа работников к обработке ПДн в ИСПДн;
- организация проведения аттестационных испытаний ИСПДн по требованиям безопасности ПДн.

11.4. Руководители структурных подразделений Общества, реализующих процессы обработки ПДн:

- определяют перечень информационных систем и технических средств (основных и вспомогательных), необходимых для осуществления основной деятельности в подразделении, связанных с обработкой ПДн;
- участвуют в подготовке и проведении работ по созданию ИСПДн;

– обеспечивают выполнение установленных в Обществе требований по организации обработки и защиты ПДн во вверенных им подразделениях;

– организуют допуск сотрудников к обработке ПДн;

– периодически пересматривают права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам ИСПДн.

11.5. Основными задачами работников Общества при выполнении возложенных на них обязанностей и в рамках их участия в деятельности по защите ПДн, являются:

– соблюдение требований по защите ПДн, устанавливаемых нормативными документами Общества;

– выявление и предотвращение реализации угроз информационной безопасности ПДн в пределах своей компетенции;

– выявление и реагирование на инциденты информационной безопасности;

– информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях ИБ;

– прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;

– мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции.

12. ФУНКЦИОНАЛЬНЫЕ РОЛИ ПО АДМИНИСТРИРОВАНИЮ

12.1. Для обеспечения функционирования СЗПДн, реализации организационно-технических мероприятий по защите ПДн при их обработке в ИСПДн с учетом структурно-функциональных характеристик корпоративной информационной инфраструктуры и критичности отдельных ИСПДн в Обществе формируются функциональные роли по администрированию отдельных объектов (категорий объектов) на различных уровнях корпоративной информационной инфраструктуры.

12.2. Администраторы информационной безопасности в рамках обеспечения функционирования ИСПДн:

– обеспечивают функционирования подсистем СЗПДн;

– осуществляют контроль разрешительной системы доступа в ИСПДн;

– осуществляют контроль технологического процесса обработки ПДн в ИСПДн;

– участвуют в планировании работ по реализации требований законодательства в сфере защиты ПДн;

– осуществляют повышение осведомленности работников по вопросам обеспечения безопасности ПДн и эксплуатации используемых средств защиты информации;

– руководят работами по конфигурированию оборудования и изменению состава ИСПДн;

– участвуют в работах по расследованию инцидентов информационной безопасности и устранению их последствий;

– осуществляют контроль за деятельностью Администраторов ИСПДн.

12.3. Администраторы ИСПДн:

– выполняют функции по администрированию ИСПДн Общества;

– консультируют работников по вопросам, связанным с эксплуатацией используемых средств защиты информации;

– участвуют в работах по модернизации СЗПДн Общества;

– участвуют в расследовании инцидентов информационной безопасности.

12.4. В целях распределения обязанностей и закрепления персональной ответственности администраторов ИСПДн за обеспечение информационной безопасности функциональные роли по

администрированию средств и систем защиты информации закрепляются приказом Директора Общества.

12.5. Перечень типовых функциональных ролей по администрированию приведен в Таблице 1. В зависимости от структурно-функциональных характеристик и критичности конкретной ИСПДн перечень ролей по администрированию может быть изменён. Присвоение нескольких различных ролей по администрированию одному сотруднику допускается.

Таблица 3. Типовые роли по администрированию

Наименование подсистемы	Наименование роли администрирования	Основные обязанности администратора
Подсистема защиты от НСД	Администратор средств защиты АРМ и серверов	− Установка, конфигурирование и обеспечение функционирования ОС АРМ и серверов. − Заведение учетных записей пользователей в ОС. − Блокирование и удаление учетных записей пользователей. − Обеспечение регистрации событий ИБ в ОС АРМ и серверов. − Мониторинг событий ИБ, зарегистрированных с использованием механизмов ОС АРМ и серверов. − Доведение до пользователей требований по обеспечению ИБ, в т.ч. требований эксплуатационной документации на используемые средства и системы зашиты информации (при необходимости). − Установка и обеспечение функционирования программного обеспечения АРМ и серверов, в том числе средств защиты информации. − Управление учетными записями пользователей в программном обеспечении, предоставление им прав и полномочий. − Блокирование и удаление учетных записей пользователей. − Конфигурирование ПО с учетом требований по обеспечению ИБ, в т.ч. требований парольной политики, требований к регистрации событий ИБ. − Мониторинг событий ИБ в процессе функционирования программного обеспечения. − Доведение до пользователей ПО требований по обеспечению ИБ, в т.ч. требований эксплуатационной документации на ПО. − Проведение анализа защищенности АРМ и серверов ИСПДн. − Своевременная установка обновлений системного и прикладного программного обеспечения АРМ и серверов.
	Администратор домена	− Администрирование контроллеров доменов. − Обеспечение бесперебойного функционирования контроллеров доменов. − Управление доступом с использованием средств службы каталогов Active Directory (заведение пользователей, групп пользователей,

Наименование подсистемы	Наименование роли администрирования	Основные обязанности администратора
		предоставление им прав и полномочий и т.п.). − Блокирование и удаление учетных записей пользователей. − Конфигурирование политик безопасности службы каталогов Active Directory. − Реализация разрешительной системы доступа на уровне файлов и каталогов с использованием механизмов службы каталогов Active Directory. − Мониторинг событий ИБ, зарегистрированных с использованием службы каталогов Active Directory.
	Администратор баз данных	− Установка и обеспечение бесперебойного функционирования СУБД. − Заведение новых учетных записей в СУБД, предоставление им необходимых прав, присвоение ролей. − Блокировка и удаление учетных записей пользователей АБС. − Заведение необходимых БД. − Конфигурирование СУБД с учетом требований по обеспечению ИБ, в т. ч. требований парольной политики, требований к регистрации событий ИБ. − Мониторинг событий ИБ в процессе функционирования СУБД. − Организация резервного копирования БД, содержащих защищаемые информационные активы.
Подсистема виртуализации	Администратор среды виртуализации	− Администрирование среды виртуализации. − Обеспечение бесперебойного функционирования среды виртуализации. − Развертывание виртуальных машин в среде виртуализации. − Конфигурирование средств обеспечения ИБ гипервизора. − Мониторинг событий ИБ, связанных с функционированием среды виртуализации.
Подсистема межсетевого экранирования и обнаружения вторжений	Администратор средств межсетевого экранирования и обнаружения вторжений	− Конфигурирование средств межсетевого экранирования и обнаружения вторжений в соответствии с установленными в Банке требованиями. − Обеспечение бесперебойного функционирования средств межсетевого экранирования и обнаружения вторжений. − Поддержание бесперебойного функционирования ЛВС и восстановления ее функционирования после отказов и аварий. − Принятие мер по восстановлению функционирования ЛВС в случаях отказов и аварий в работе средств межсетевого экранирования и обнаружения вторжений. − Конфигурирование средств регистрации событий ИБ средств межсетевого экранирования

Наименование подсистемы	Наименование роли администрирования	Основные обязанности администратора
		и обнаружения вторжений. − Контроль журналов регистрации событий ИБ межсетевых экранов и средств обнаружения вторжений.
	Администратор сетевого оборудования	− Мониторинг корректности функционирования сетевого оборудования. − Проведение профилактических работ, направленных на выявление потенциально возможных сбоев или отклонений в работе сетевого оборудования и сетевых устройств. − Техническое обслуживание сетевого оборудования и сетевых устройств, в соответствии с эксплуатационной документацией. − Контроль конфигурации сетевого оборудования в целях предотвращения нарушения правил размещения сетевых устройств, АРМ и серверов в предопределенных сетевых сегментах. − Контроль отсутствия несанкционированных и неучтенных подключений к сетевому оборудованию. − Выполнение профилактических работ и технического обслуживания сетевого оборудования и устройств в соответствии с установленным в Банке порядком и требованиями эксплуатационной документации.
Подсистема антивирусной защиты	Администратор средств антивирусной защиты	− Настройка параметров функционирования средств антивирусной защиты в соответствии с эксплуатационной документацией на них, а также требованиями, установленными в Обществе. − Контроль функционирования средств антивирусной защиты на всех АРМ, серверах, межсетевых экранах и своевременное обновление баз вирусных сигнатур. − Мониторинг систем оповещения средств антивирусной защиты. − Контроль автоматического обновления баз вирусных сигнатур средств антивирусной защиты, используемых на всех АРМ и серверах, и контроль их работоспособности. − Организация проведения периодического антивирусного контроля на объектах информационной инфраструктуры Общества.
Подсистема криптографической защиты информации	Администратор средств криптографической защиты информации	− Учет лиц, допущенных к работе с СКЗИ; − Установка, настройка и сопровождение СКЗИ в соответствии с требованиями эксплуатационной и технической документации на используемые средства. − Реализация необходимых мероприятий в случае компрометации ключей; − Реализация необходимых мероприятий по

Наименование подсистемы	Наименование роли администрирования	Основные обязанности администратора
		восстановлению работоспособности СКЗИ в случае их сбоев и отказов. − Управление криптографическими ключами: изготовление, блокирование, уничтожение криптографических ключей. − Проведение регламентных работ, предусмотренных эксплуатационной документацией на используемые в Банке СКЗИ.
Подсистема резервного копирования и восстановления защищаемой информации	Администратор резервного копирования	− Формирование заданий на проведение процедур резервного копирования. − Мониторинг журналов регистрации средств резервного копирования.

12.6. Реализация мероприятий по администрированию с учетом ролевой модели, приведенной в Таблице 3, осуществляется с учетом требований эксплуатационной документации на используемые программные и аппаратные средства, а также средства защиты информации. При необходимости указанные требования уточняются применительно к конкретным подсистемам СЗПДн с учетом структурно-функциональных характеристик ИСПДн и отражаются в разрабатываемых администраторами информационной безопасности инструкциях, содержащих требования к порядку администрирования соответствующих компонентов ИСПДн и их системы защиты.

12.7. Контроль за действиями администраторов осуществляется администраторами информационной безопасности.

13. РЕГИСТРАЦИЯ СОБЫТИЙ ИНФОРМАЦИОНОЙ БЕЗОПАСНОСТИ

13.1. В целях предупреждения инцидентов ИБ, обеспечения мониторинга функционирования подсистем СЗПДн (в том числе оценки их эффективности) и своевременного реагирования на инциденты ИБ, обеспечения возможности их расследования, события информационной безопасности в ИСПДн Общества подлежат регистрации.

13.2. Перечень базовых событий ИБ, подлежащих регистрации в ИСПДн, приведен в Таблице 4.

Таблица 4. Состав событий информационной безопасности, подлежащих регистрации

Наименование подсистемы	Типы регистрируемых событий
защиты информации от несанкционированного доступа	а. создание и удаление учетных записей пользователей; б. назначение и распределение прав субъектов доступа; в. предоставление доступа к защищаемым ресурсам ИСПДн; г. использование субъектами доступа своих привилегий (в т.ч. изменение полномочий пользователей и создание защищаемых объектов); д. доступ к защищаемым объектам; е. результаты идентификации / аутентификации / авторизации субъекта доступа; ж. события, связанные с истечением сроков действия средств идентификации и аутентификационной информации; з. блокировка/разблокировка консоли; и. события, связанные с попытками изменения/удаления журналов регистрации событий.

Наименование подсистемы	Типы регистрируемых событий
антивирусной защиты	а. обновление антивирусных баз; б. проведение антивирусных проверок; в. обнаружение вредоносного кода или подозрительных объектов; г. события, связанные с попытками изменения/удаления журналов регистрации событий; д. ошибки функционирования антивирусного средства.
резервного копирования и восстановления информации после сбоев	а. события, связанные с администрированием средств резервного копирования; б. создание резервной копии; в. ошибки функционирования системы резервного копирования информации; г. переполнение дискового пространства, отведенного под хранение резервных копий; д. события, связанные с попытками изменения/удаления журналов регистрации событий. е. события, связанные с выполнением автоматических сценариев резервирования и ротацией резервных копий;
межсетевого экранирования и обнаружения вторжений	а. события, связанные с администрированием МЭ и СОВ, попытками доступа к средствам администрирования МЭ, созданием/изменением/удалением учетных записей пользователей, вынесением изменений в конфигурацию МЭ, изменение параметров фильтрации сетевого трафика и режимов функционирования СОВ; б. обновление программной и информационной части ПО МЭ; в. проведение периодических мероприятий по контролю целостности, в т.ч. реализуемые автоматически; г. события, связанные с ошибками и сбоями в процессе функционирования средства МЭ; д. события, связанные с анализом сетевого трафика СОВ; е. события, связанные с попытками изменения/удаления журналов регистрации событий.
криптографической защиты информации	Типы регистрируемых событий, определяются в соответствии с эксплуатационной документацией на СКЗИ и условиями их применения. Как минимум, требуется регистрация следующих событий: а. события, связанные с администрированием СКЗИ; б. события, связанные с работой с ключевой информацией и ключевыми документами (генерация криптоключей, введение криптоключей в аппаратную платформу и т.п.); в. все действия по администрированию аппаратной платформы, в составе которой функционирует СКЗИ, оказывающие влияние на среду его функционирования (обновление ПО аппаратной платформы, изменение состава ПО и конфигураций и т.п.) г. проведение периодических мероприятий по контролю целостности, в т.ч. реализуемые автоматически.

13.3. Уточнение перечня базовых событий ИБ, приведенных в Таблице 3, подлежащих обязательной регистрации для каждой ИСПДн, осуществляется на стадии технического проектирования ее системы защиты с учетом особенностей архитектуры ИСПДн, среды ее функционирования и перечня актуальных угроз информационной безопасности.

13.4. Регистрация событий информационной безопасности в ИСПДн должна обеспечиваться функциями средств защиты информации, используемыми для обеспечения безопасности ПДн при их обработке в ИСПДн. Дополнительно могут быть использованы функции операционных систем и средств регистрации сетевого оборудования.

13.5. СЗПДн в отношении регистрации событий информационной безопасности должна обеспечивать:

13.5.1. возможность централизованной обработки событий ИБ на уровне подсистем защиты информации и автоматической сигнализации об обнаружении инцидентов ИБ в ходе обработки событий ИБ;

13.5.2. централизованное, безопасное хранение информации о событиях и инцидентах ИБ.

13.5.3. регистрацию по каждому событию ИБ, как минимум, следующих параметров:

- дату и время возникновения события;
- тип события, либо его идентификатор в соответствии с возможностями, предоставляемыми средствами регистрации;
- идентификатор инициатора события (субъект доступа, сервис/служба, сетевой адрес);
- результат обработки события: успешное (событие ИБ должно быть определено как относящиеся или не относящиеся к инцидентам ИБ) / неуспешное (событие ИБ только зарегистрировано, но не обработано);
- иные характерные данные с учетом специфики реализации.

13.6. Безопасность регистрируемых событий должна обеспечиваться функциями защиты информации средств, обеспечивающих регистрацию.

13.7. Доступ к журналам (логам) устройств, содержащих зарегистрированные события информационной безопасности, должен предоставляться только Администратору ИБ и Администратору ИСПДн, реализующему функции администрирования, для обеспечения которых такой доступ необходим.

13.8. Хранение и накопление результатов регистрации событий ИБ по каждой из подсистем защиты СЗПДн должны осуществляться в аппаратных журналах средства регистрации на максимально возможный срок до проведения очередных мероприятий по контролю эффективности мер и средств защиты информации, обеспечивающих безопасность ПДн при их обработке в ИСПДн, предусмотренных нормативно-методическими документами по защите ПДн.

13.9. Срок хранения и накопления результатов регистрации событий ИБ в аппаратных журналах средств регистрации должен быть определен с учетом того, что в результате накопления регистрируемых событий ИБ не должны ухудшаться параметры функционирования самих средств (АРМ, серверов, средства межсетевого экранирования) регистрации, в результате исчерпания их ресурсов.

13.10. В ходе опытной эксплуатации устанавливаются сроки удалении результатов регистрации из аппаратных журналов технических средств, осуществляющих регистрацию.

13.11. Очистка аппаратных журналов от событий регистрации должна осуществляться Администратором ИБ. При этом непосредственно перед удалением результатов регистрации событий ИБ из аппаратного журнала, должна осуществляться их выгрузка. Выгруженные результаты регистрации событий ИБ должны храниться у Администратора ИБ с соблюдением условий их конфиденциальности. Срок хранения должен соответствовать времени проведения очередных мероприятий по контролю эффективности мер и средств защиты информации, обеспечивающих безопасность ПДн при их обработке в ИСПДн, предусмотренных нормативно-методическими документами по защите ПДн.

13.12. Нарушение условий обращения с результатами регистрации событий ИБ, в т.ч. их несанкционированное удаление из аппаратных журналов средства регистрации, должно рассматриваться как инцидент ИБ, в случае наступления которого необходимо установленным порядком инициировать служебное расследование.

13.13. Результаты регистрации событий ИБ должны периодически изучаться и систематизироваться, в целях выявления недостатков в конфигурациях технических средств и систем, а также для разработки и реализации превентивных защитных мер, модернизации и совершенствованию СЗПДн.

14. КОНТРОЛЬ ИЗМЕНЕНИЙ В СОСТАВЕ (СТРУКТУРЕ) ИСПДн

14.1. Все изменения в составе и структуре ИСПДн должны контролироваться работниками администраторами ИБ ИСПДн.

14.2. Контролю подлежат следующие изменения:

– внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);

– удаление устройств из состава ИСПДн;

– изменения состава используемых средств защиты информации;

– изменение расположения устройств из состава ИСПДн;

– существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;

– создание новых и изменение существующих технологических процессов, связанных с обработкой ПДн.

14.3. Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите информации.

14.4. При необходимости должна осуществляться актуализация существующих технических паспортов, моделей угроз и пр.

14.5. В случае, если ИСПДн была аттестована по требованиям безопасности информации, изменения в ее составе или структуре должны согласовываться с организацией, осуществившей аттестацию.

15. ПОРЯДОК ДОПУСКА СОТРУДНИКОВ К РАБОТЕ В ИСПДн

15.1. К работе в ИСПДн Общества допускаются работники Общества, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (должностных) обязанностей.

15.2. Допуск работников к соответствующим ПДн осуществляется на основании перечня, утвержденного Директором Общества.

15.3. К работе в ИСПДн Общества могут быть допущены лица, не являющиеся работниками Общества, на основании распоряжения Директора Общества.

16. ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ

16.1. В Обществе проводится регулярное повышение осведомленности работников по вопросам, связанным с обеспечением безопасности ПДн при их обработке в ИСПДн.

16.2. Основными задачами повышения осведомленности персонала по вопросам обеспечения ИБ ПДн являются:

– доведение до работников требований нормативных документов РФ и внутренних документов Общества вопросам обеспечения ИБ ПДн;

– доведение до работников сведений об используемых защитных мерах;

– мотивация работников на сознательное выполнение требований и правил по вопросам обеспечения ИБ ПДн;

– доведение до работников степени их ответственности за обеспечение ИБ ПДн;

– выработка у работников Общества умений по оперативному реагированию в случае возникновения нештатной ситуации (инцидента ИБ).

16.3. По формам проведения повышение осведомленности персонала по вопросам обеспечения ИБ ПДн может быть:

– внутреннее (проводится за счет внутренних ресурсов Общества);

– внешнее (проводится с привлечением внешних обучающих организаций, институтов, учебных центров по разработанным ими программам).

16.4. Определены следующие форматы внутреннего повышения осведомленности персонала по вопросам обеспечения ИБ ПДн:

– Вводный инструктаж проводится при приеме на работу нового сотрудника, допущенного в рамках своих должностных обязанностей к ИСПДн. Вводный инструктаж должен включать общую информацию о структуре ИБ Общества и проводиться на основании разработанных инструкций по эксплуатации ИСПДн и имеющихся средств защиты информации.

По факту проведения вводного инструктажа работниками ставятся подписи в листах ознакомления с инструкциями.

– Повторный инструктаж проводится для сотрудников, выполняющих работы, к которым предъявляются дополнительные (повышенные) требования по информационной безопасности, например, администраторов ИСПДн.

– Внеочередной инструктаж проводится при изменении требований по информационной безопасности нормативных правовых актов РФ или внутренних документов Общества, при выявлении нарушений сотрудником требований по обеспечению ИБ, при назначении или переводе сотрудника на другую должность, если новые обязанности требуют от работников дополнительных знаний по информационной безопасности.

– Целевой инструктаж проводится при выполнении разовых работ, не связанных с прямыми должностными обязанностями работника. При этом основанием для проведения такого инструктажа и допуска работника к ИСПДн является приказ Директора Общества.

16.5. Контроль за осведомленностью персонала по вопросам обеспечения ИБ ПДн при их обработке в ИСПДн осуществляется работниками Общества, назначенными администраторами ИБ ИСПДн.

17. РЕАГИРОВАНИЕ НА НЕШТАТНЫЕ СИТУАЦИИ

17.1. Для эффективного реагирования на нештатные ситуации (инциденты информационной безопасности), возникающие в процессе обработки и защиты ПДн в ИСПДн, в Обществе должны быть документированы:

– порядок определения ИИБ;

– порядок оповещения администраторов ИБ и администраторов ИСПДн при возникновении различных ИИБ;

– порядок действий по реагированию на ИИБ;

– порядок действий по нейтрализации последствий ИИБ;

– порядок расследования ИИБ;

– порядок принятия мер по недопущению возникновения ИИБ в дальнейшем.

17.2. Разработанные порядки действий должны регулярно (не менее одного раза в год) проверяться посредством проведения учений с корректировкой порядков по результатам проведенных проверок.

17.3. Разработанные порядки действий в случае обнаружения ИИБ включаются в инструкции пользователей, администраторов ИСПДн и администраторов ИБ ИСПДн.

18. АТТЕСТАЦИЯ ИСПДн

18.1. Аттестация соответствия ИСПДн по требованиям безопасности ПДн является формой подтверждения соответствия реализованных организационно-технических мероприятий по защите ПДн, обрабатываемых в ИСПДн Общества, требованиям законодательства РФ.

18.2. Основными мероприятиями по подготовке ИСПДн к аттестации по требованиям безопасности информации являются:

– определение состава ОТСС. Из состава ИСПДн должны быть исключены элементы, не предназначенные для решения задач, реализуемых в технологическом процессе обработки ПДн;

– определение актуальных угроз информационной безопасности и возможных каналов утечки ПДн при их обработке в ИСПДн и анализ принятых мер по защите информации;

– разработка актуальной модели угроз ИСПДн и моделей нарушителя информационной безопасности ИСПДн;

– определение уровней защищенности ПДн;

– разработка технических паспортов на ИСПДн и разрешительных систем доступа субъектов доступа к защищаемым информационным ресурсам ИСПДн;

– разработка организационно-распорядительной и объектовой документации на ИСПДн;

– установка и настройка средств защиты информации.

18.3. Для проведения аттестации ИСПДн по требованиям безопасности ПДн, а также реализации мероприятий по подготовке к аттестации на договорной основе может привлекаться

организация, имеющая лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

19. КОНТРОЛЬ ВЫПОЛНЕНИЯ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПДн

19.1. Основными целями контроля состояния защиты ПДн в Обществе являются:

– проверка выполнения требований нормативных правовых актов Российской Федерации по защите персональных данных, решений и указаний ФСТЭК России, ФСБ России;

– оценка эффективности принимаемых в Обществе организационно-технических мероприятий по защите ПДн при их обработке в ИСПДн и определение их соответствия действующим требованиям руководящих документов ФСТЭК и ФСБ России;

– проверка выполнения мероприятий по устранению, выявленных ранее недостатков.

19.2. Основными задачами контроля являются:

– проверка выполнения требований по защите ПДн в структурных подразделениях Общества;

– проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите серверного оборудования и автоматизированных рабочих мест пользователей;

– проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

– проверка выполнения требований по работе с электронными (машинными) носителями персональных данных и порядку обращения с ними;

– оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн.

19.3. Постоянный контроль состояния защиты ПДн в подразделениях, обрабатывающих ПДн, осуществляется начальниками данных подразделений.

19.4. Обязанности по контролю эффективности предусмотренных мер по защите ПДн в ИСПДн возлагается на администратора информационной безопасности.

19.5. При необходимости на договорной основе привлекаются эксперты – сотрудники, организаций, имеющих лицензию ФСТЭК на соответствующие виды работ и услуг.

19.6. В ходе контроля проверяются:

– соответствие принятых мер по обеспечению безопасности ПДн;

– своевременность и полнота выполнения требований настоящего Положения и других документов по обеспечению безопасности ПДн, в т.ч. ведение журналов учета, актуальность разрешительной системы доступа к ресурсам ИСПДн;

– эффективность применения организационных и технических мер по защите ПДн.

19.7. Защита ПДн считается эффективной, если принимаемые меры соответствуют установленным требованиям. Несоответствие мер установленным требованиям или нормам по обеспечению информационной безопасности ПДн является нарушением.

19.8. Полученные в ходе проведения контрольных мероприятий результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер по защите информации и выявления нарушений. Результаты проведенных мероприятий оформляются актами в свободной форме.

19.9. Акты по результатам контроля передаются Директору Общества.

19.10. Невыполнение работниками Общества мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее – предпосылка).

19.11. По каждой предпосылке или ИИБ для выяснения обстоятельств, а также причин невыполнения установленных требований по указанию Директора Общества проводится расследование.

19.12. Для проведения расследования назначается комиссия, в состав которой входят работники подразделения, в котором было выявлено нарушение и работник, назначенный Ответственным за организацию обработки персональных данных в Обществе.

19.13. Комиссия обязана установить, имела ли место предпосылка или ИИБ, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить

причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования Директор Общества принимает решение о наказании виновных лиц и реализации необходимых мероприятий по устранению недостатков.

19.14. Контроль СЗПДн осуществляется путем проведения периодических, плановых и внеплановых проверок ИСПДн Общества. Периодические, плановые и внеплановые проверки ИСПДн осуществляются Администратором информационной безопасности.

19.15. Периодичность проведения контрольных мероприятий - не реже одного раза в 6 месяцев.

19.16. Государственный контроль состояния защиты информации, в т.ч. персональных данных, осуществляется Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и Федеральной службой безопасности России (ФСБ России) в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

20. ДОСТУП В СЛУЖЕБНЫЕ ПОМЕЩЕНИЯ, В КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ПДн

20.1. Доступ сотрудников, не участвующих в процессах обработки и защиты ПДн, в служебные помещения, в которых размещаются ОТСС ИСПДн и осуществляется хранение электронных (машинных) носителей ПДн, ограничивается.

20.2. Помещения, в которых размещены технические средства обработки ПДн, должны быть оборудованы охранной и пожарной сигнализацией, после окончания рабочего дня запираться и сдаваться под охрану.

20.3. Нахождение в помещениях лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

20.4. Расположение мониторов АРМ должно препятствовать несанкционированному просмотру со стороны лиц, не допущенных к обработке ПДн в ИСПДн.

20.5. При реализации СЗПДн выделяются функциональные и физические зоны безопасности:

20.5.1. В качестве физической зоны безопасности рассматриваются серверные помещения, запираемые коммутационные шкафы и стойки, как наиболее подходящие для размещения технических средств и оборудования ИСПДн и ее системы защиты. Доступ в данные помещения (к данным шкафам или стойкам) ограничивается дополнительными организационными мероприятиями.

20.5.2. Функциональная зона безопасности размещается внутри физической зоны безопасности, обеспечивающей надежную защиту от бесконтрольного и несанкционированного доступа посторонних, в том числе работников Общества.

20.6. Все оборудование ИСПДн и системы ее защиты, включая коммутационное, размещается в физической зоне безопасности. Коммутация АРМ из состава ИСПДн Общества должна осуществляться исключительно в физической зоне безопасности, вне зависимости от типа используемого коммутационного оборудования.

21. ВЗАИМОДЕЙСТВИЕ СО СТОРОННИМИ ОРГАНИЗАЦИЯМИ В АСПЕКТАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

21.1. Общество осуществляет взаимодействие по вопросам организации защиты ПДн и контроля ее эффективности с ФСТЭК России и организациями, имеющими лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации по следующим видам работ и услуг:

– контроль защищенности ПДн от несанкционированного доступа и модификации в ИСПДн;

– аттестационные испытания и аттестация на соответствие требованиям по обеспечению информационной безопасности персональных данных;

– проектирование СЗПДн;

– 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).

21.2. Обмен информацией со сторонними организациями осуществляются на основании договоров, содержащих раздел, определяющий ответственность, права и обязанности взаимодействующих сторон в области защиты ПДн.

21.3. При возникновении необходимости проведения совместных организационно-технических мероприятий с другими организациями, могут разрабатываться единые документы по защите информации для всех этапов работ, утверждаемые руководителями этих организаций.

22. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

22.1. Требования настоящего Положения обязательны для всех работников Общества, имеющих регламентированный доступ к работе в ИСПДн и участвующих в автоматизированной обработке ПДн.

22.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

22.3. Пересмотр настоящего Положения осуществляется в случае изменения требований нормативных документов по защите ПДн, но не реже, чем раз в два года.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

В таблице приведены сведения о последних изменениях данного документа, включая версию, дату, автора и краткое описание изменений.

Версия	Дата	Автор	Изменения
01			

ЛИСТ ОЗНАКОМЛЕНИЯ

№ п/п	Ф.И.О.	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				