Для служебного пользования
Ед.экз.

Согласовано
Генеральный директор
ООО "Единый оператор"
_____ Н.В. Сапогов
«26» мая 2014 г.
м.п.

Утверждаю
Директор
МАДОУ «Детский сад комбинированного вида № 29»
г.Тобольска
_____ С.В. Шевелёва
«26» мая 2014 г.
м.п.

ПОЛИТИКА

безопасности персональных данных, обрабатываемых в
МАДОУ «Детский сад комбинированного вида № 29» г.Тобольска

Тобольск,2014

Оглавление

1. Термины и сокращения

АРМ – автоматизированное рабочее место
ПДн – персональные данные
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
МЭ – межсетевой экран
НСД – несанкционированный доступ к информации
ВП – вредоносная программа
СВТ – средства вычислительной техники
НДВ – недекларированные возможности
СЗПДн - система защиты персональных данных

2. Общие положения

Настоящая политика безопасности персональных данных, обрабатываемых в МАДОУ «Детский сад комбинированного вида № 29» г.Тобольска (далее - Политика) устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации, а также при их неавтоматизированной обработке.

Политика разработана в соответствии со следующими законами и нормативными документами:

- Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет порядок защиты персональных данных, обрабатываемых в МАДОУ «Детский сад комбинированного вида № 29» г.Тобольска (далее - Оператор).

Целью Политики является определение требований безопасности к персональным данным, обрабатываемым в информационных системах персональных данных Оператора и предотвращение любого несанкционированного доступа к ним.

Основным фактором безопасности ПДн является организация эффективного контроля доступа к ПДн, обрабатываемых в информационных системах персональных данных. Отсутствие адекватного контроля доступа может привести к несанкционированному доступу к ИСПДн Оператора.

Требования настоящей Политики распространяются на всех сотрудников Оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.), связанных с обработкой ПДн.

3. Меры по обеспечению безопасности ПДн, обрабатываемых Оператором

3.1. Состав и содержание мер по обеспечению безопасности ПДн

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, могут быть включены:

- Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);
- Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил;
- Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения;
- Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;
- Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;
- Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;
- Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия;
- Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных;
- Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных;
- Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы;
- Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам

управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям;

- Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей;
- Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных;
- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов;
- Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

3.2. Реализация мер по обеспечению безопасности ПДн

Для реализации указанных мер по обеспечению безопасности могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

Для защиты ПДн, представленных в виде информативных электрических сигналов и физических полей могут применяться следующие методы и способы защиты информации:

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

Возможные методы и способы защиты ПДн, представленных в виде акустической (речевой) информации, заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

3.3. Основные принципы определения актуальных угроз безопасности ПДн

Выбор и реализация мер по обеспечению безопасности ПДн в ИСПДн осуществляются на основе угроз безопасности персональных данных, обрабатываемых Оператором, выявленных в Модели угроз безопасности ПДн(далее - Модель угроз), а также в зависимости от уровня защищенности ПДн, определенного в соответствии с Постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модель угроз разрабатывается на основе следующих методических документов:

- Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;
- Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России.

Для выбора и реализации мер по обеспечению безопасности ПДн в ИСПДн Оператора назначается Ответственный за защиту информации в информационных системах персональных данных(далее - Ответственный за защиту). Ответственный за защиту также составляет и Модель угроз.

Периодичность пересмотра Модели угроз для каждой ИСПДн Оператора определена в пункте 3.5. данной Политики.

3.4. Определение уровня защищенности ПДн

При обработке персональных данных в информационных системах устанавливаются уровни защищенности ПДн, обрабатываемых в ИСПДн Оператора, в соответствии с Постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При этом учитываются следующие исходные характеристики ИСПДн:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором параметры безопасности персональных данных, обрабатываемых в информационной системе;
- тип угроз безопасности ПДн, актуальных для информационной системы;
- категория субъектов ПДн, чьи данные обрабатываются Оператором. Это могут быть сотрудники Оператора или иные субъекты ПДн, не являющиеся сотрудниками.

По результатам анализа исходных данных каждой ИСПДн Оператора присваивается соответствующий уровень защищенности ПДн и составляется «Акт определения уровня защищенности ПДн, при их обработке в ИСПДн», утверждаемый руководителем Оператора.

Уровень защищенности персональных данных может быть пересмотрен:

- по решению Ответственного за защиту на основе проведенного им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной ИСПДн;
- по результатам мероприятий по контролю за выполнением Требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

3.5. План мероприятий по обеспечению безопасности ПДн

Для обеспечения безопасности персональных данных, обрабатываемых Оператором, должны быть выполнены работы, в соответствии с указанным ниже планом:

Мероприятие	Периодичность мероприятия
Организационные мероприятия	
Обследование информационных систем персональных данных	Разовое
Определение перечня ИСПДн	Разовое
Определение обрабатываемых ПДн и объектов защиты	Разовое

Мероприятие	Периодичность мероприятия
Определение круга лиц участвующих в обработке ПДн	Разовое
Определение ответственности лиц участвующих в обработке	Разовое
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое
Назначение ответственных за безопасность ИСПДн и организацию обработки ПДн	Разовое
Определение уровня защищенности ПДн для всех выявленных ИСПДн	Разовое
Установление контролируемой зоны Оператора	Разовое
Выделение специальных помещений Оператора для установки аппаратных средств ИСПДн с целью исключения НСД к ИСПДн лиц, не допущенных к обработке ПДн	Разовое
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое
Организация порядка резервного копирования твердые носители и восстановления защищаемой информации	Разовое
Введение в действие инструкции по защите ИСПДн	Разовое
Организация информирования и обучения сотрудников о порядке обработки и защиты ПДн	Разовое
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое
Разработка положения об обработке и защите ПДн в ИСПДн Оператора	Разовое
Утверждение Политики безопасности персональных данных	Разовое
Организация журнала учета обращений субъектов ПДн	Разовое
Организация перечня по учету технических средств и средств защиты, а так же документации к ним	Разовое
Организация охраны для пропуска субъектов в контролируемую зону Оператора	Разовое
Технические мероприятия	
Внедрение технической системы контроля доступа в контролируемую зону и помещения	Разовое
Внедрение технической системы контроля доступа к объектам ИСПДн	Разовое
Установка жалюзи на окна	Разовое
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое
Мероприятия по внедрению и контролю СЗПДн	
Внедрение системы защиты от НСД на рабочих станциях и серверах Оператора	Разовое
Внедрение системы антивирусной защиты	Разовое
Внедрение средств межсетевого экранирования	Разовое
Внедрение средств анализа защищенности	Разовое
Внедрение средств обнаружения вторжений	Разовое
Создание журнала внутренних проверок обеспечения безопасности ПДн и поддержание его в актуальном состоянии	Ежемесячно
Контроль над соблюдением режима обработки ПДн	Еженедельно
Контроль над соблюдением режима защиты ПДн	Ежедневно
Контроль над выполнением антивирусной защиты на рабочих станциях и серверах Оператора	Еженедельно
Контроль над соблюдением режима защиты при подключении к сетям общего	Еженедельно

Мероприятие	Периодичность мероприятия
пользования и (или) международного обмена	
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно
Контроль за обновлениями программного обеспечения, применяемого на объектах ИСПДн	Еженедельно
Контроль за обеспечением резервного копирования	Ежемесячно
Организация анализа и пересмотра актуальных угроз безопасности ПДн, а так же прогноз появления новых угроз безопасности ПДн	Ежегодно
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно
Контроль за разработкой и внесением изменений в программное обеспечение Оператора или штатное ПО, дорабатываемое собственными разработчиками или сторонними организациями	Ежемесячно
Контроль за реализацией правил фильтрации на МЭ, настроек системы защиты от НСД, системы защиты от вирусов, системы обнаружения вторжений и анализа защищенности	Ежемесячно

4. Обеспечение безопасности персональных данных

4.1. Состав мер по обеспечению безопасности ПДн в ИСПДн

Выбранные меры по обеспечению безопасности ПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных, при их обработке в ИСПДн Оператора и лежать в основе реализации системы защиты персональных данных Оператора, которая строится на основании Модели угроз, проекта Системы защиты персональных данных, обрабатываемых в ИСПДн Оператора, а также руководящих документов ФСТЭК и ФСБ России.

Выбранные мероприятия по защите ПДн отражаются в Описании системы защиты персональных данных, обрабатываемых в ИСПДн Оператора.

Для защиты от НСД к ПДн на рабочих станциях и серверах Оператора, исходя из требуемого уровня защищенности ИСПДн, необходимо принятие следующих мер по обеспечению безопасности ПДн:

- Идентификация и аутентификация пользователей являющихся работниками Оператора;
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- Защита обратной связи при вводе аутентификационной информации;
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип), правил разграничения доступа;
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- Защита информации о событиях безопасности;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- Контроль установки обновлений программного обеспечения. включая обновление программного обеспечения средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- Контроль состава технических средств, программного обеспечения и средств защиты информации;
- Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

4.2. Состав дополнительных мер по обеспечению безопасности ПДн в ИСПДн

Кроме мер по обеспечению безопасности ПДн в ИСПДн также необходимо:

- Ответственному за защиту анализировать и просматривать регистрируемые системой защиты от НСД события безопасности на компьютерах и серверах ИСПДн Оператора на наличие несанкционированных действий по расписанию, указанному в пункте 3.5;
- Ответственному за защиту для эффективной защиты от вредоносных программ и вирусов на компьютерах и серверах ИСПДн Оператора проверять журналы систем антивирусной защиты по расписанию, указанному в пункте 3.5;
- обеспечить контроль доступа пользователей ИСПДн к защищаемым ресурсам ИСПДн в соответствии с Матрицей доступа Пользователей к объектам ИСПДн;
- обеспечить учет всех защищаемых носителей информации с помощью их маркировки и занесение их в Журнал учета носителей ПДн;
- обеспечить физическую охрану технических средств ИСПДн, предусматривающую контроль доступа в помещения с объектами ИСПДн посторонних лиц, а также наличие надежных препятствий для несанкционированного проникновения в хранилища ПДн;
- обеспечить наличие средств восстановления СЗПДн, предусматривающих ведение двух копий программных компонентов средств защиты информации, а также их периодическое обновление и контроль работоспособности;
- утвердить инструкцию по восстановлению свойств межсетевого экрана после сбоев и отказов оборудования;
- обеспечить контроль за реализацией правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации, аутентификации и регистрации администратора межсетевого экрана;
- обеспечить контроль за целостностью процедуры восстановления объектов ИСПДн по расписанию, указанному в пункте 3.5.

4.3. Организация доступа Пользователей ИСПДн

Все Пользователи ИСПДн должны иметь доступ к ресурсам ИСПДн только в соответствии с разрешениями, установленными в Матрице доступа Пользователей к объектам ИСПДн.

Доступ нового Пользователя к ресурсам ИСПДн осуществляется следующим образом:

- Происходит согласование доступа Пользователя к ресурсам ИСПДн и его добавление в Список лиц, доступ которых к ПДн, обрабатываемых в ИСПДн Оператора, необходим для выполнения служебных (трудовых) обязанностей Ответственным за защиту;
- Происходит ознакомление Пользователя ИСПДн с Положением об обработке и защите ПДн, обрабатываемых Оператором и подписание Пользователем Соглашения о неразглашении ПДн;
- Происходит создание в ИСПДн учетной записи Пользователя и организация его доступа к объектам ИСПДн в соответствии с разрешениями, зафиксированными в Матрице доступа Пользователей к ресурсам ИСПДн.

При необходимости блокирования доступа Пользователя ИСПДн к ресурсам ИСПДн (например, в случае увольнения сотрудника Оператора) необходимо удалить учетную запись

Пользователя и откорректировать Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей.

4.4. Порядок обработки инцидентов безопасности

Порядок обработки инцидентов безопасности ПДн описан в Инструкции по организации резервирования, восстановления ИСПДн и обработке инцидентов безопасности ИСПДн.

4.5. Порядок выполнения процедур резервного копирования

Порядок резервного копирования ПДн в ИСПДн описан в Инструкции по организации резервирования, восстановления ИСПДн и обработке инцидентов безопасности ИСПДн.

5. Пользователи ИСПДн

Можно выделить следующие категории пользователей ИСПДн Оператора, участвующих в обработке ПДн или связанных с обслуживанием объектов ИСПДн:

- Ответственный за защиту (Администратор безопасности);
- Оператор ИСПДн;
- Специалист по поддержке технических средств ИСПДн и корпоративной сети (Администратор);

Сведения о категориях пользователей ИСПДн, а также об уровне их доступа к объектам ИСПДн должны быть отражены в Матрице доступа Пользователей к ресурсам ИСПДн.

5.1. Администратор безопасности

Администратор безопасности, сотрудник Оператора, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент ИСПДн.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми Оператор ИСПДн получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

5.2. Оператор ИСПДн

Оператор ИСПДн, сотрудник Оператора, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает сведениями о ПДн, к которым имеет доступ.
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

5.3. Специалист по поддержке технических средств ИСПДн и корпоративной сети (Администратор)

Администратор, сотрудник Оператора, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Администратор не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

6. Требования к работникам Оператора по обеспечению безопасности персональных данных

Все сотрудники Оператора, являющиеся Пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудники Оператора

- должны быть ознакомлены с положением по обработке и обеспечению безопасности персональных данных, обрабатываемых в Оператора.
- использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним и возможность их утери или использования третьими лицами. Сотрудник Оператора несут персональную ответственность за сохранность идентификаторов.
- должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
- должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.
- не должны устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.
- не должны разглашать защищаемую информацию третьим лицам, которая стала им известна при работе в ИСПДн Оператора.
- при работе с ПДн в ИСПДн обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
- при завершении работы в ИСПДн обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.
- должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.
- обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и Ответственному за защиту.

Контроль за соблюдением вышеописанных требований сотрудниками Оператора возлагается на Ответственного за защиту и Ответственного за организацию обработки ПДн.

7. Должностные обязанности Пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция Ответственного за защиту информации в информационных системах персональных данных;
- Инструкция пользователя по эксплуатации СЗПДн;
- Инструкции по организации резервирования, восстановления ИСПДн и обработке инцидентов безопасности ИСПДн;
- Инструкция Оператора ИСПДн;

8. Ответственность Пользователей ИСПДн

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор защиты несёт ответственность за все действия, совершенные от имени его учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях Пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.