Ед.экз.

СОГЛАСОВАНО

Генеральный директор
ООО «Единый оператор»

Н.В. Сапогов
_____
(подпись)
«5» августа 2017 г.

УТВЕРЖДАЮ

Главный врач
ООО «МаргоДент»

М.Ш. Джавадова
_____
(подпись)
«7» августа 2017 г.

ПОЛИТИКА
безопасности персональных данных
ООО «МаргоДент»

г. Тюмень – 2017

Оглавление

Список терминов и определений

Организация – ООО «МаргоДент»

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

АРМ – автоматизированное рабочее место.

СЗПДн – система защиты персональных данных.

1. Общие положения

Настоящий документ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Политика разработана в соответствии с 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 Организации.

1.1. Цель политики.

Определить требования безопасности к персональным данным, обрабатываемым в информационных системах персональных данных Организации, с целью предотвращения любого несанкционированного доступа.

Критичным фактором безопасности ПДн является организация эффективного контроля доступа к ПДн, обрабатываемых в информационных системах персональных данных. Отсутствие адекватного контроля доступа может вести к несанкционированному доступу к ИСПДн Организации.

1.2. Область применения.

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

2. Состав и содержание мер по обеспечению безопасности ПДн и план работ по защите ПДн, обрабатываемых в ИСПДн Организации

2.1. 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, входят:

- 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.

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, представленной 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.

2.2. Принципы и способы определения актуальных угроз безопасности ПДн

Для выбора и реализации мер по обеспечению безопасности ПДн в информационной системе Организации назначается ответственный по защите информации в информационных системах персональных данных.

Выбор и реализация мер по обеспечению безопасности ПДн в ИСПДн осуществляются на основе, определяемых в Организации, угроз безопасности персональных данных (модель угроз) и в зависимости уровня защищенности ПДн, определенного в соответствии с Постановлением Правительства от 1.11.2012 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.

Модель угроз персональным данным составляется ответственным по защите ПДн и утверждается руководителем Организации.

Периодичность пересмотра модели угроз для каждой ИСПДн определена в пункте 2.4. данного документа.

2.3. Определение уровня защищенности ПДн

При обработке персональных данных в информационных системах устанавливаются уровни защищенности ПДн в соответствии с Постановлением

Правительства от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При определении уровня защищенности ПДн, при их обработке в ИСПДн учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- тип угроз безопасности ПДн, актуальных для информационной системы;
- проверяется условие принадлежности ПДн сотрудникам оператора ПДн или иным субъектам, не являющимся сотрудниками оператора.

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

Уровень защищенности персональных данных может быть пересмотрен:

- по решению ответственного по защите ПДн в Организации на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

2.4. План мероприятий по обеспечению безопасности ПДн

Для обеспечения безопасности процессов обработки персональных данных в Организации, должны быть выполнены работы, в соответствии с планом, указанном ниже:

Мероприятие	Периодичность
Организационные мероприятия	
Обследование информационных систем персональных данных	Разовое
Определение перечня ИСПДн	Разовое
Определение обрабатываемых ПДн и объектов защиты	Разовое
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 и организацию ИСПДн	Разовое
Определение уровня защищенности ПДн для всех выявленных ИСПДн	Разовое

Мероприятие	Периодичность
Установление контролируемой зоны вокруг ИСПДн	Разовое
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД 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 и восстановления защищаемой информации на твердые носители	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, обрабатываемых в ИСПДн	Разовое
Утверждение политики безопасности персональных данных	Разовое
Организация журнала учета обращений субъектов ПДн	Разовое
Организация перечня по учету технических средств и средств защиты, а также документации к ним	Разовое
Организация постов охраны для пропуска в контролируемую зону	Разовое
Инженерно-технические мероприятия	
Внедрение технической системы контроля доступа в контролируемую зону и помещения	Разовое
Внедрение технической системы контроля доступа к элементам ИСПДн	Разовое
Установка жалюзи на окнах	Разовое
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое
Мероприятия по внедрению СЗИ от НСД	
Внедрение системы защиты от НСД на рабочих станциях и серверах	Разовое
Внедрение системы антивирусной защиты	Разовое
Внедрение средств межсетевого экранирования	Разовое
Внедрение средств анализа защищенности	Разовое
Внедрение средств обнаружения вторжений	Разовое

Мероприятие	Периодичность
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно
Контроль над соблюдением режима обработки ПДн	Еженедельно
Контроль над соблюдением режима защиты	Ежедневно
Контроль над выполнением антивирусной защиты	Еженедельно
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно
Контроль за обеспечением резервного копирования	Ежемесячно
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно
Тестирование реализации правил фильтрации на МЭ, настроек системы защиты от НСД, системы защиты от вирусов, системы обнаружения вторжений и анализа защищенности	Ежемесячно

3. Требования по обеспечению безопасности персональных данных

Выбранные и реализованные меры по обеспечению безопасности ПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных, при их обработке в информационных системах в составе системы защиты персональных данных Организации.

Система защиты персональных данных, строится на основании:

- Модели угроз безопасности персональным данным при их обработке в информационной системе персональных данных «Сотрудники» ООО «МаргоДент»;
- Модели угроз безопасности персональным данным при их обработке в информационной системе персональных данных «Пациенты» ООО «МаргоДент»;
- Технического проекта «системы защиты персональных данных информационных систем персональных данных ООО «МаргоДент»;
- Руководящих документов ФСТЭК и ФСБ России.

Выбранные необходимые мероприятия по защите ПДн отражаются в «Описании системы защиты персональных данных ООО «МаргоДент».

3.1. Требования по обеспечению защиты в ИСПДн «Сотрудники» и ИСПДн «Пациенты»

Для защиты от НСД в ИСПДн на рабочих станциях и серверах устанавливается средства защиты информации, обеспечивающие:

- 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) и 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;

3.2. Требования по организации обеспечения безопасности в ИСПДн

Регистрируемые системой защиты от НСД события безопасности на компьютерах и серверах ИСПДн должны просматриваться и анализироваться на наличие не санкционированных действий администратором безопасности *по расписанию, указанному в пункте 2.4*.

Для эффективной защиты от вредоносных программ и вирусов на компьютерах и серверах ИСПДн периодически (*по расписанию, указанному в пункте 2.4*) должны проверятся журналы системы антивирусной защиты.

Для обеспечения защиты ИСПДн от угроз безопасности ПДн в Организации необходимо обеспечить:

- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);

- физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.
- процесса контроля за целостностью программной и информационной части, процедуры восстановления (*по расписанию, указанному в пункте 2.4*).

3.3. Порядок организации доступа к ИСПДн

Все пользователи ИСПДн должны иметь доступ к ресурсам ИСПДн только в соответствии с разрешениями, установленными в «Матрице доступа пользователей к ресурсам ИСПДн».

Организация доступа нового пользователей к ресурсам ИСПДн осуществляется следующим образом:

1. Согласование доступа пользователя к ресурсам ИСПДн и добавление пользователя в «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей»;
2. Ознакомление пользователя с «Положением об обработке и защиты ПДн в Организации» и истребование с пользователя подписания «Соглашения о неразглашении ПДн»;
3. Создание учетной записи пользователя и организация доступа в соответствии с разрешениями, зафиксированными в «Матрице доступа пользователей к ресурсам ИСПДн».

При необходимости удаления доступа пользователя к ресурсам ИСПДн (в случаях увольнения сотрудника и т.д.) необходимо заблокировать (или удалить) учетную запись пользователя и откорректировать «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей».

3.4. Порядок обработки инцидентов безопасности

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

3.5. Порядок выполнения процедур резервного копирования

Порядок процедур резервного копирования ПДн описан в «Инструкции по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ИСПДн».

4. Пользователи ИСПДн

В Организации можно выделить следующие группы пользователей ИСПДн, участвующих в обработке и хранении ПДн:

- Администратора безопасности;
- Оператора АРМ;

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в матрице доступа пользователей к ресурсам ИСПДн.

4.1 Администратор безопасности

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

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- 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 СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Организации.

4.2 Оператор АРМ

Оператор АРМ, сотрудник Организации, 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 конфиденциальными данными, 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. Требования к персоналу по обеспечению безопасности персональных данных

Все сотрудники Организации, 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.

Сотрудник должен быть ознакомлен со сведениями положения по обработке и обеспечению безопасности персональных данных, обрабатываемых в Организации.

Сотрудники Организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Организации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Организации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам, а также бывшим сотрудникам, запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Организации, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Организации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Организации 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.

Сотрудники 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 лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Контроль за соблюдением, выше описанных требований по защите персональных данных сотрудниками Организации, возлагается на ответственного по защите информации в ИСПДн и ответственного за организацию обработки персональных данных в Организации.

6. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора безопасности;
- Инструкция пользователя по эксплуатации СЗИ в ИСПДн;
- Инструкция по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ПДн;
- Инструкция пользователей ИСПДн.

7. Ответственность сотрудников ИСПДн Организации

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 ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Организации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.