НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ФОНД КАПИТАЛЬНОГО РЕМОНТА МНОГОКВАРТИРНЫХ ДОМОВ ТЮМЕНСКОЙ ОБЛАСТИ»
(НО «ФКР ТО»)

УТВЕРЖДАЮ
Директор
НО «ФКР ТО»

_____С.С. Цынская
«__» _____ 2016 г.

м.п.

П О Л И Т И К А
безопасности конфиденциальной информации, содержащей в том числе персональные данные НО «ФКР ТО»

г. Тюмень – 2016

Оглавление

Список терминов и определений

Оператор – НО «ФКР ТО».

КИ – конфиденциальная информация, содержащая в том числе персональные данные.

ПДн – персональные данные.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

АРМ – автоматизированное рабочее место.

СЗИ – система защиты информации.

СЗПДн – система защиты персональных данных.

1. Общие положения

Настоящий документ устанавливает требования к обеспечению безопасности конфиденциальной информации, содержащей в том числе персональные данные (далее -КИ), при обработке в информационных системах (Далее - ИС), а также информационных технологий и технических средств, позволяющих осуществлять обработку такой КИ 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 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и определяет порядок защиты КИ, обрабатываемой Оператором.

1.1. Цель политики.

Определить требования безопасности КИ, обрабатываемой в ИС Оператора, с целью предотвращения любого несанкционированного доступа.

Критичным фактором безопасности КИ является организация эффективного контроля доступа к КИ, обрабатываемых в ИС. Отсутствие адекватного контроля доступа может вести к несанкционированному доступу к ИС Оператора.

1.2. Область применения.

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.).

2. Состав и содержание мер по обеспечению безопасности КИ и план работ по защите КИ, обрабатываемой в ИС Оператора

2.1. Состав и содержание мер по обеспечению безопасности КИ

В состав мер по обеспечению безопасности КИ, реализуемых в рамках системы защиты информации с учетом актуальных угроз безопасности 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 КИ (средств обработки (хранения) КИ, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них КИ, а также несанкционированное использование съемных машинных носителей КИ.
- 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 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 КИ, 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 КИ, представленных в виде акустической (речевой) информации, заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена ИС, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе КИ в ИС или воспроизведении информации акустическими средствами.

2.2. Принципы и способы определения актуальных угроз безопасности КИ

Для выбора и реализации мер по обеспечению безопасности КИ в ИС Оператора назначается ответственный по защите информации в ИС.

Выбор и реализация мер по обеспечению безопасности КИ в ИС осуществляются на основе, определяемых у Оператора, угроз безопасности

КИ (модель угроз), в зависимости от класса ИС, определенного в соответствии с Приказом ФСТЭК России № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», обрабатывающей информацию, являющуюся государственным информационным ресурсом, и уровня защищенности персональных данных (Далее - 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 КИ составляется ответственным по защите информации в ИС и утверждается заместителем директора НО «ФКР ТО».

Периодичность пересмотра модели угроз для каждой ИС определена в пункте 2.5. данного документа.

2.3. Определение класса защищенности информационной системы

При обработке в ИС информации, являющейся государственным информационным ресурсом и взаимодействии с государственными информационными системами необходимо установить класс защищенности информационной системы в соответствии с Приказом ФСТЭК России № 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

При определении класса защищенности ИС учитываются следующие исходные данные:

- Степень возможного ущерба для обладателя информации, в случае нарушения конфиденциальности, целостности или доступности обрабатываемой информации;
- Уровень значимости обрабатываемой информации;
- Масштаб ИС.

По результатам анализа исходных данных ИС, в которых осуществляется обработка государственных информационных ресурсов, устанавливается класс защищенности информационной системы и

составляется «Акт классификации информационной системы», утверждаемый заместителем директора НО «ФКР ТО».

Класс защищенности ИС может быть пересмотрен в случаях:

- изменения масштаба информационной системы;
- пересмотра значимости обрабатываемой информации.

2.4. Определение уровня защищенности персональных данных

При обработке ПДн в ИС 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 ИСПДн;
- объем обрабатываемых ПДн (количество субъектов ПДн, ПДн которых обрабатываются в ИС);
- заданные оператором характеристики безопасности ПДн, обрабатываемых в ИС;
- тип угроз безопасности ПДн, актуальных для ИС;
- проверяется условие принадлежности ПДн сотрудникам оператора ПДн или иным субъектам, не являющимся сотрудниками Оператора.

По результатам анализа исходных данных ИСПДн присваивается соответствующий уровень защищенности ПДн, и составляется «Акт определения уровня защищенности ПДн, при их обработке в ИСПДн», либо проводится оценка соответствия установленных уровня защищенности ПДн и класса защищенности информационной системы и результаты отражаются в «Акте классификации информационной системы», утверждаемом заместителем директора НО «ФКР ТО».

Уровень защищенности ПДн может быть пересмотрен:

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

2.5. План мероприятий по обеспечению безопасности конфиденциальной информации, содержащей в том числе персональные данные

Для обеспечения безопасности процессов обработки КИ Оператора, должны быть выполнены работы, в соответствии с планом, указанном ниже:

Мероприятие	Периодичность
Организационные мероприятия	
Обследование ИС	Разовое
Определение перечня ИС	Разовое
Определение обрабатываемой КИ и объектов защиты	Разовое
Определение круга лиц, участвующих в обработке КИ	Разовое
Определение ответственности лиц, участвующих в обработке	Разовое
Определение прав разграничения доступа пользователей ИС, необходимых для выполнения должностных обязанностей	Разовое
Назначение ответственных за безопасность и организацию ИС	Разовое
Определение уровня защищенности ПДн для всех выявленных ИСПДн и по необходимости проведение классификации	Разовое
Определения класса защищенности, для всех выявленных ИС и по необходимости проведение классификации	Разовое
Установление контролируемой зоны вокруг ИС	Разовое
Выбор помещений для установки аппаратных средств ИС в помещениях, с целью исключения НСД лиц, не допущенных к обработке КИ	Разовое
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИС.	Разовое
Организация порядка резервного копирования и восстановления КИ на твердые носители	Разовое
Введение в действие инструкции по защите ИС	Разовое
Организация информирования и обучения сотрудников о порядке обработки и защиты КИ	Разовое
Разработка должностных инструкций о порядке обработки КИ и обеспечении введенного режима защиты	Разовое
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое
Разработка положения об обработке и защите КИ, обрабатываемых в ИС	Разовое
Утверждение политики безопасности КИ	Разовое
Организация журнала учета обращений субъектов КИ	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	

Мероприятие	Периодичность
Внедрение технической системы контроля доступа в контролируемую зону и помещения	Разовое
Внедрение технической системы контроля доступа к элементам ИС	Разовое
Установка жалюзи на окнах	Разовое
Внедрение резервных (дублирующих) технических средств ключевых элементов ИС	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
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно
Контроль над соблюдением режима обработки КИ	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 КИ	Ежегодно
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИС	Еженедельно
Контроль за обеспечением резервного копирования	Ежемесячно
Организация анализа и пересмотра имеющихся угроз безопасности КИ, 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 конфиденциальной информации, содержащей в том числе персональные данные

Выбранные и реализованные меры по обеспечению безопасности КИ должны обеспечивать нейтрализацию предполагаемых угроз безопасности, при их обработке в ИС в составе системы защиты информации Оператора.

Система защиты информации, строится на основании:

- Модели угроз безопасности информационных систем НО «ФКР ТО»;
- Руководящих документов ФСТЭК и ФСБ России.

Выбранные необходимые мероприятия по защите КИ отражаются в «Описании системы защиты информации НО «ФКР ТО».

3.1. Требования по обеспечению защиты в информационных системах

Для защиты от НСД в ИС 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;
- 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);
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

- Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);
- Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;
- Учет машинных носителей информации;
- Управление доступом к машинным носителям информации;
- Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);
- 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;
- Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- Генерирование временных меток и (или) синхронизация системного времени в ИС;
- Защита информации о событиях безопасности;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей;
- Контроль установки обновлений ПО, включая обновление ПО средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации;
- Контроль состава технических средств, ПО и средств защиты информации;
- Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС;

- Обеспечение возможности восстановления ПО, включая ПО средств защиты информации, при возникновении нештатных ситуаций;
- 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;
- 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;
- Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств.

3.2. Требования по организации обеспечения безопасности в информационных системах

Регистрируемые системой защиты от НСД события безопасности на компьютерах и серверах ИС должны просматриваться и анализироваться на наличие не санкционированных действий администратором безопасности *по расписанию, указанному в пункте 2.5*.

Для эффективной защиты от вредоносных программ и вирусов на компьютерах и серверах ИС периодически (*по расписанию, указанному в пункте 2.5*) должны проверятся журналы системы антивирусной защиты.

Для обеспечения защиты ИС от угроз безопасности Оператора 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 ИС (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 информации, 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 2.5*).

3.3. Порядок организации доступа к информационным системам

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

Организация доступа нового пользователей к ресурсам ИС осуществляется следующим образом:

1. Согласование доступа пользователя к ресурсам ИС и добавление пользователя в «Список лиц, доступ которых к КИ, обрабатываемой в ИС необходим для выполнения служебных (трудовых) обязанностей»;
2. Ознакомление пользователя с «Политикой оператора в отношении обработки персональных данных» и истребование с пользователя подписания «Соглашения о неразглашении КИ»;
3. Создание учетной записи пользователя и организация доступа в соответствии с разрешениями, зафиксированными в «Матрице доступа пользователей к ресурсам ИС».

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

3.4. Порядок выполнения процедур резервного копирования

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

4. Пользователи информационных систем

Можно выделить следующие группы пользователей ИС, участвующих в обработке и хранении КИ:

- Администратора безопасности;
- Оператора АРМ;

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

4.1 Администратор безопасности

Администратор безопасности, сотрудник Оператора, ответственный за функционирование системы защиты информации, включая обслуживание и настройку административной, серверной и клиентской компонент ИС.

Администратор безопасности обладает следующим уровнем доступа и знаний:

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

Администратор безопасности уполномочен:

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

4.2 Оператор АРМ

Оператор АРМ, сотрудник Оператора, осуществляющий обработку КИ. Обработка КИ включает: возможность просмотра КИ, ручной ввод КИ в ИС, формирование справок и отчетов по информации, полученной из ИС. Оператор не имеет полномочий для управления подсистемами обработки данных и системы защиты информации.

Оператор ИС обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству КИ;
- располагает конфиденциальными данными, к которым имеет доступ.
- обладает частью информации о технических средствах и конфигурации ИС;

- 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 конфиденциальной информации, содержащей в том числе персональные данные

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

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 КИ, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИС.

Сотрудник должен быть ознакомлен со сведениями положения по обработке и обеспечению безопасности КИ, обрабатываемых Оператором.

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

Сотрудники Оператора 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 КИ 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 КИ.

Сотрудникам, а также бывшим сотрудникам, запрещается разглашать КИ, которая стала им известна при работе с ИС Оператора, третьим лицам.

При работе с КИ в ИС сотрудники Оператора обязаны обеспечить отсутствие возможности просмотра КИ третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИС 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 Оператора должны быть проинформированы об угрозах нарушения режима безопасности КИ 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 КИ.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИС, могущих повлечь за собой угрозы безопасности КИ, а также о выявленных ими событиях, затрагивающих безопасность КИ, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности КИ.

Контроль за соблюдением, выше описанных требований по защите КИ сотрудниками Оператора, возлагается на ответственного по защите информации в ИС и ответственного за организацию обработки ПДн Оператора.