

**Регламент обеспечения безопасности
персональных данных при их обработке
в информационных системах персональных данных в ГУСМ ТО**

1. Общие положения.

Требования настоящего Регламента являются обязательными для исполнения сотрудниками Главного управления специальных мероприятий Тюменской области (далее – ГУСМ ТО) и третьими лицами, допущенными к работе с персональными данными (далее - ПДн).

При приеме на работу сотрудники ГУСМ ТО, допущенные к работе с ПДн, должны под расписку быть ознакомлены с требованиями настоящего Регламента.

2. Обеспечение безопасности персональных данных в информационных системах персональных данных

Обеспечение безопасности ПДн в ГУСМ ТО достигается за счет выполнения требований нормативных актов Российской Федерации в сфере защиты ПДн и выполнения требований, установленных документами ГУСМ ТО, пользователями информационных систем персональных данных ГУСМ ТО.

Безопасность ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн) обеспечивается с помощью системы защиты ИСПДн, включающей организационные меры и средства защиты информации. Технические и программные средства обработки и защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации, содержащей ПДн.

Реализация требований по обеспечению безопасности ПДн в ИСПДн возлагается на администратора безопасности информации и ответственных за эксплуатацию ИСПДн.

При обработке ПДн в ИСПДн должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействий на технические средства автоматизированной обработки ПДн, в результате которых может быть нарушено их функционирование;
- возможность восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- контроль обеспечения уровня защищенности ПДн.

Меры по защите ПДн, обрабатываемых в ИСПДн, принимаются в соответствии с моделью угроз безопасности ПДн для каждой ИСПДн.

Порядок осуществления контроля состояния защищенности ИСПДн ГУСМ ТО в целях поддержания требуемого уровня безопасности ПДн, а также предотвращения инцидентов информационной безопасности, определен регламентом

осуществления внутреннего контроля за обеспечением уровня защищенности ПДн и соблюдения условий использования средств защиты информации, а также соблюдения требований законодательства РФ по обработке ПДн в ИСПДн.

3. Основные направления и методы защиты информации в ИСПДн.

Лицо, ответственное за организацию работ по обеспечению безопасности персональных данных при их обработке в информационных ИСПДн ГУСМ ТО обязано организовать работу по защите ПДн в ИСПДн, осуществлять методическое руководство по проведению мероприятий по защите информации, а также осуществлять контроль за эффективностью предусмотренных мер защиты информации.

Ответственные за эксплуатацию ИСПДн в ГУСМ ТО обязаны контролировать в подчиненных подразделениях выполнение установленных общих требований по организации работы с ПДн и предусмотренных организационных и технических мер по защите ПДн в пределах своих полномочий.

Пользователи ИСПДн обязаны соблюдать правила обработки ПДн в ИСПДн. В своей работе с ПДн пользователи руководствуются нормами настоящего Регламента и Инструкцией пользователя при работе с ИСПДн.

Защита ПДн в ИСПДн ГУСМ ТО осуществляется по следующим основным направлениям:

- от вредоносного кода;
- от несанкционированного доступа;
- от несанкционированного воздействия;
- от непреднамеренного воздействия;
- от разглашения.

В качестве основных мер защиты ПДн в ИСПДн должны выполняться:

- документальное оформление и обновление перечня ПДн, обрабатываемых в ИСПДн;
- разграничение доступа Пользователей¹ и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) ПДн и защиты информации;
- ограничение доступа персонала и посторонних лиц в помещения, где размещены средства информатизации и коммуникационное оборудование ИСПДн, а также хранятся носители ПДн;
- регистрация действий пользователей, обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- учет и надежное хранение машинных носителей ПДн и их обращение, исключающее хищение, подмену и уничтожение;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ;
- использование защищенных каналов связи при передаче ПДн;

¹ Пользователями ИСПДн являются лица, использующий при обработке персональных данных средства автоматизированной обработки информации, в том числе средства вычислительной техники, программное обеспечение, электронные носители персональных данных и средства защиты информации

- размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;
- организация физической защиты помещений, где осуществляется обработка ПДн и технических средств обработки ПДн;
- предотвращение внедрения в ИСПДн программ-вирусов, программных закладок;

Объем принимаемых мер защиты информации определяют должностные лица, отвечающие за организацию и руководство работой по защите персональных данных в ГУСМ ТО.

3.1. Защита от вредоносного программного обеспечения

Организация антивирусной защиты информации в ГУСМ ТО достигается путем:

- внедрения и применения средств антивирусной защиты информации;
- обновления сигнатурных баз данных средств антивирусной защиты информации;

Система антивирусной защиты ИСПДн включает в себя:

- антивирусную защиту рабочих станций ИСПДн;
- антивирусную защиту серверов и баз ПДн;
- возможность автоматического обновления сигнатурных антивирусных баз и версий.

Организация работ по антивирусной защите информации возлагается на администратора безопасности информации и должностных лиц, ответственных за эксплуатацию ИСПДн в ГУСМ ТО, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на лицо, ответственное за организацию работ по обеспечению безопасности ПДн при их обработке в ИСПДн ГУСМ ТО.

Порядок применения средств антивирусной защиты устанавливается с учетом необходимости выполнения следующих требований:

а) пользователями ИСПДн:

- периодическая проверка носителей информации (не реже одного раза в неделю) и обязательная проверка используемых в работе съемных носителей информации перед началом работы с ними на отсутствие программных вирусов;
- внеплановая проверка носителей информации на отсутствие программных вирусов в случае подозрения на наличие программного вируса.

При обнаружении программных вирусов пользователь ИСПДн обязан прекратить все работы на рабочем месте, поставить в известность администратора безопасности информации и совместно с ним принять меры к локализации и удалению вирусов с помощью имеющихся антивирусных средств защиты.

При функционировании автоматизированного рабочего места в качестве локальной рабочей станции производится ее отключение от локальной сети, локализация и удаление программных вирусов в вычислительной сети.

3.2. Защита от несанкционированного доступа

Защита ИСПДн ГУСМ ТО обеспечивается комплексом программно-технических средств и организационных мер.

При обработке или хранении ПДн в ИСПДн проводятся следующие организационные мероприятия:

- документальное оформление состава ПДн в виде перечня;
- ознакомление субъекта доступа с перечнем персональных данных и установленным для него уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- обеспечение охраны объекта, на котором расположена защищаемая ИСПДн;
- назначение должностных лиц, осуществляющих учет, хранение и выдачу съемных и резервных носителей информации, паролей, ключей, ведение служебной информации системы защиты информации от несанкционированного доступа, приемку включаемых в ИСПДн программных средств, а также контроль за ходом технологического процесса обработки ПДн и т. д.;

3.4. Основные мероприятия по предотвращению несанкционированного доступа к ПДн ГУСМ ТО:

- разграничение доступа к ПДн;
- определение единого порядка парольной защиты;
- идентификация пользователей и подтверждение их права на работу с запрашиваемой информацией;
- регистрация действий пользователей в ИСПДн;
- реакция на попытки несанкционированного доступа, например, блокировка доступа и т. д.;
- тестирование информационных ресурсов ИСПДн с помощью специальных программных средств выявления уязвимостей;
- учет выходных конфиденциальных печатных, графических форм и твердых копий.

3.5. Защита от несанкционированного и непреднамеренного воздействия.

Защита ПДн от несанкционированного и непреднамеренного воздействия осуществляется по следующим направлениям:

- соблюдение порядка разработки, ввода в действие и эксплуатации объектов информатизации;
- определение условий размещения информационных ресурсов ИСПДн относительно границ контролируемой зоны;
- определение технических средств и систем, предполагаемых к использованию в ИСПДн;
- определение режимов обработки ПДн в ИСПДн;
- установление правил разграничения доступа для пользователей с целью минимизации их воздействия на программные и аппаратные средства автоматизации обработки ПДн;
- повышение уровня квалификации пользователей в области информационной безопасности;
- контроль, техническое обслуживание и обеспечение установленных режимов работы ТСПИ в целях предупреждения их сбоев, аварий, неисправностей;

- обновление антивирусного программного обеспечения;
- защита от природных и техногенных явлений и стихийных бедствий (пожары, наводнения и т.п.);
- предупреждение передачи конфиденциальных ПДн по открытым линиям связи и их обработки незащищенными техническими средствами;
- выполнение сотрудниками установленных в Управлении требований по защите ПДн;
- использование ИСПДн в защищенном исполнении.

3.6. Защита от распространения неограниченному кругу лиц.

Правовой основой работы сотрудников ГУСМ ТО с ПДн являются:

- наличие в должностном регламенте или должностной инструкции сотрудника пунктов о мерах безопасности при обработке ПДн и ответственности за ее несанкционированное разглашение;
- наличие инструкций и регламентов по защите ПДн, ознакомление с которыми должно производиться сотрудником в первый день поступления на должность и под обязательную роспись в ознакомлении;
- создание сотрудникам достаточных условий для обеспечения эффективной защиты ПДн.

В целях предупреждения разглашения ПДн лицо, ответственное за организацию обработки ПДн, организует мероприятия по аудиту защищенности ПДн, тестированию уровня осведомленности сотрудников о мерах защиты ПДн.

4.Порядок резервирования и восстановления работоспособности ИСПДн

Ответственным за реагирование на инциденты, связанные с нарушением безопасности защищаемой информации, является администратор безопасности информации.

Ответственным за контроль обеспечения мероприятий по предотвращению данных инцидентов является лицо, ответственное за организацию работ по обеспечению безопасности ПДн в ИСПДн.

Происшествие, вызывающее инцидент², может произойти в результате:

- непреднамеренных действий Пользователей;
- преднамеренных действий Пользователей и третьих лиц;
- нарушения правил эксплуатации технических средств;
- возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

4.1. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

4.1.1.Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

² Под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн Управления, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

- системы жизнеобеспечения (пожарные сигнализации и системы пожаротушения, системы резервного питания);
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;

Все критичные помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции, подключаются к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленты, жесткий диск и т.п.).

4.2. Организационные меры

Резервное копирование и хранение данных должно осуществлять на периодической основе:

для обрабатываемых ПДн – не реже раза месяц;

для технологической информации – не реже раза в квартал;

Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

Носители, на которые записаны резервные копии, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

Носители должны храниться в несгораемом шкафу или помещении, оборудованном системой пожаротушения, обеспечивающими защиту от несанкционированного доступа.

Носители должны храниться не менее года.

5. Порядок обращения со средствами криптографической защиты информации

Использование средств криптографической защиты информации (далее - СКЗИ) необходимо для достижения следующих целей:

- обеспечение целостности ПДн, обрабатываемых в ИСПДн;
- обеспечение конфиденциальности ПДн, обрабатываемых в ИСПДн;
- обеспечение невозможности отказа от авторства внесенных изменений в обрабатываемые ПДн.

5.1. Состав СКЗИ

Могут использоваться программные и программно-аппаратные СКЗИ, состав которых утверждается лицом, ответственным за организацию безопасности ПДн в ИСПДн.

5.2. Учет используемых СКЗИ

СКЗИ, используемые в ИСПДн, а также эксплуатационная и техническая документация к ним, подлежат поэкземпляльному учету в Журнале учета СКЗИ.

Поэкземплярный учет СКЗИ осуществляет администратор безопасности информации. При ведении учета, программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация.

Единицей поэкземплярного учета СКЗИ является отчуждаемый ключевой носитель многократного использования. При осуществлении перезаписи криптографических ключей на носитель администратор информационной безопасности обязан осуществить его повторную регистрацию в Журнале поэкземплярного учета СКЗИ с указанием сведений о вновь записанных криптографических ключах.

Нумерация носителей СКЗИ ведется в соответствии с индивидуальными номерами, присваиваемыми изготовителями СКЗИ.

5.3. Допуск сотрудников к СКЗИ

Допуск Пользователей ИСПДн к работе с СКЗИ осуществляется на основании заявки, подаваемой ответственным за эксплуатацию ИСПДн.

В заявке указываются следующие сведения:

- перечень задач, для которых необходимо использование СКЗИ;
- период времени, в течение которого необходимо использование СКЗИ.

Ответственный за организацию работ по защите ПДн в ИСПДн, обязан организовать обучение пользователя ИСПДн по правилам работы с СКЗИ, к которым он будет допущен.

5.4. Порядок выдачи СКЗИ

Экземпляры СКЗИ, эксплуатационная и техническая документация к ним выдаются под подпись пользователю ИСПДн. Пользователи ИСПДн несут персональную ответственность за сохранность выданного им экземпляра СКЗИ.

Администратор безопасности информации выдает основной экземпляр СКЗИ лично пользователю ИСПДн.

5.5. Порядок прекращения прав допуска и изъятия СКЗИ из обращения

Прекращение прав доступа Пользователя ИСПДн к СКЗИ осуществляется администратором безопасности информации в следующих случаях:

- достигнуты цели использования СКЗИ;
- истек период времени, указанный в заявке ответственного за эксплуатацию ИСПДн;
- увольнение Пользователя ИСПДн или его перевод на должность, не связанную с необходимостью использования СКЗИ.

При наступлении вышеуказанных случаев администратор информационной безопасности осуществляет исключение Пользователя ПДн из перечня лиц, до-

пущенных к работе с СКЗИ и изымает СКЗИ из обращения. Перед повторным использованием с основного и резервного ключевых носителей СКЗИ при помощи средств гарантированного уничтожения должна быть удалена вся информация

6. Порядок обращения с материальными носителями персональных данных

Учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, Blu-ray и прочее);
- неотчуждаемые носители информации (жесткие магнитные диски).

6.1. Порядок организации учёта машинных носителей, содержащих ПДн

Все машинные носители данных, используемые при работе со средствами вычислительной техники (далее СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в «Журнале учета машинных носителей ПДн, обрабатываемых в ИСПДн (далее – Журнал учета носителей) с присвоением индивидуального учетного номера.

Ответственность за хранение машинных носителей ПДн и ведение Журнала учета носителей несёт ответственный за эксплуатацию ИСПДн.

Учетный номер и гриф «Конфиденциально» наносятся на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель.

6.2. Порядок использования машинных носителей ПДн.

Машинные носители ПДн выдаются Пользователям, участвующим в обработке ПДн, для работы под расписку в Журнале учета машинных носителей ПДн.

Запрещается использовать указанные носители ПДн в иных целях и хранение информации на них не содержащих ПДн.

В случае повреждения машинных носителей, содержащих ПДн, сотрудник, за которым закреплён носитель, сообщает о случившемся ответственному за эксплуатацию ИСПДн.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны запрещается без соответствующего разрешения лица, ответственного за эксплуатацию ИСПДн.

6.3. Порядок хранения машинных носителей, содержащих ПДн

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, изменения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или шкафы, запираемые на ключ.

Не допускается оставлять на рабочем столе или в СВТ машинные носители, содержащие ПДн.

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа, к записанным на них ПДн, несет сотрудник, за которым закреплен носитель.

6.4. Порядок уничтожения машинных носителей, содержащих ПДн.

Основанием для уничтожения машинных носителей, содержащих ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает лицо, ответственное за организацию эксплуатации ИСПДн.

Уничтожение производится раз в год путем их физического разрушения с предварительным затиранiem (уничтожением) содержащейся на них информации, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее трех человек, в состав Комиссии должны обязательно входить администратор информационной безопасности и лицо, ответственное за организацию безопасности ПДн в ИСПДн. После уничтожения всех машинных носителей составляется Акт об уничтожении.

При уничтожении машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале учета носителей.