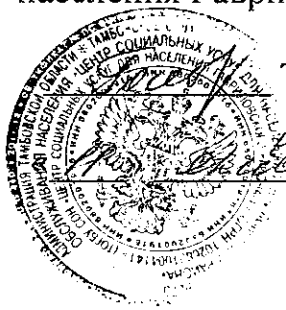
УТВЕРЖДАЮ

Директор

ТОГБУ СОН
«Центр социальных услуг для
населения Гавриловского района»



Т.В. Голованова

_____ 2016 г.

ИНСТРУКЦИЯ

администратора безопасности информационной системы персональных данных

2016 г.

Оглавление

1. Основные понятия

Применяемые в настоящей Инструкции термины и понятия означают:

Администратор безопасности - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Защита информации от разглашения - защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа (ЗИ от НСД) - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Основные технические средства и системы (ОТСС) - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации.

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

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Средство защиты информации (СрЗИ) - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Трансграничная передача персональных данных - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2. Общие положения

2.1. Настоящая инструкция разработана на основании следующих нормативных документов:

- Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.06 г.;
- Приказ ФСТЭК от 18 февраля 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»;
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Государственная техническая комиссия при президенте Российской Федерации, 2002 г.;
- Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Информационное сообщение об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных от 20 ноября 2012г. № 240/24/4669.

2.2. Инструкция определяет основные задачи, функции, обязанности, права и ответственность Администратора безопасности информационной системы персональных данных ТОГБУ СОН «Центр социальных услуг для населения Гавриловского района» (далее Организация).

2.3. Администратор безопасности выполняет функции по обеспечению бесперебойного функционирования системы защиты ИСПДн.

2.4. Закрепление функциональных обязанностей и разделение зон ответственности производится приказом руководителя Организации.

2.5. В своей деятельности Администратор безопасности руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных нормативных документов по вопросам защиты персональных данных (указанных в п. 2.1.) и обеспечивает их выполнение.

2.6. Настоящая Инструкция является дополнением к действующим регламентирующим документам по вопросам защиты информации в Организации и не исключает обязательного выполнения их требований.

3. Задачи и функции Администратора безопасности

3.1. Основными задачами Администратора безопасности являются:

- сопровождение средств защиты информации и основных технических средств и систем (далее ОТСС) в соответствии с эксплуатационной документацией;
- обеспечение работоспособности элементов ИСПДн и локальной вычислительной сети;
- организация разграничения доступа пользователей к информационным ресурсам.

3.2. Для выполнения поставленных задач на Администратора безопасности возлагаются следующие функции:

3.2.1. Настройка и сопровождение средств защиты от несанкционированного доступа (далее НСД), в том числе средств криптографической защиты информации в ИСПДн.

3.2.2. Ведение списка пользователей ИСПДн в информационной базе системы защиты от НСД, их полномочий доступа (чтение, запись) к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем Организации списка сотрудников, допущенных к работе в ИСПДн.

3.2.3. Назначение и смена паролей к информационным ресурсам ИСПДн.

3.2.4. Настройка и сопровождение подсистемы регистрации и учета:

- ввод в базу данных системы защиты от НСД описания событий, подлежащих регистрации в системном журнале;
- проведение регулярного анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
- своевременное информирование руководства о несанкционированных действиях персонала и организация расследования попыток НСД.

3.2.5. Восстановление системы защиты при сбоях.

3.2.6. Поддержание установленного порядка и соблюдение требований антивирусной защиты.

4. Обязанности Администратора безопасности

4.1. Для реализации поставленных задач и возложенных функций Администратор безопасности обязан:

4.1.1. Обеспечивать бесперебойное функционирование системы защиты информации (далее СЗИ) и ОТСС.

4.1.2. Вести учет и знать перечень всех установленных СЗИ (СЗИ от НСД, межсетевые экраны, средства криптографической защиты) и перечень задач, решаемых с их использованием.

4.1.3. Осуществлять непосредственное управление режимами работы и поддержку функционирования (настройку и сопровождение) применяемых на рабочих станциях специальных программных и программно-аппаратных СЗИ.

4.1.4. Присутствовать при внесении изменений в конфигурацию аппаратно-программных средств защищенных рабочих станций и серверов.

4.1.5. Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

4.1.6. Контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) средств вычислительной техники и вести учет изменений аппаратно-программной конфигурации.

4.1.7. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных рабочих станций.

4.1.8. Проводить периодический инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты персональных данных.

4.1.9. Разрабатывать решения по:

- осуществлению контроля за наличием активных компьютеров в локальной сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;
- разработке порядка выхода пользователей в сети общего пользования и использованию встроенных СЗИ от НСД в сервисных программах.

4.1.10. Осуществлять оперативный контроль за работой пользователей, обрабатывающих персональные данные, анализировать содержимое журналов событий операционных систем, систем управления базами данных, пакетов прикладных программ, СЗИ от НСД всех ПЭВМ и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий и надлежащий режим хранения данных архивов.

4.1.11. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания рабочих станций и отправке их в ремонт (контролировать стирание информации на магнитных носителях).

4.1.12. Контролировать обеспечение защиты персональных данных при взаимодействии пользователей с информационными сетями общего пользования.

4.1.13. Контролировать эффективность защиты персональных данных:

- проводить работу по выявлению возможности вмешательства в процесс функционирования ПЭВМ и осуществления НСД к информации и техническим средствам;
- докладывать ответственному за организацию обработки персональных данных о выявленных угрозах безопасности информации, обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам рабочих станций;
- участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в ИСПДн.

4.2. Администратору безопасности запрещается:

4.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и предоставлять его другим с целью ее модификации, копирования, уничтожения.

4.2.2. Использовать ставшие доступные в ходе исполнения обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий.

4.2.3. Самостоятельно (без согласования с ответственным за организацию обработки персональных данных) вносить изменения в настройки серверной части ИСПДн.

4.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим.

4.2.5. Выключать СЗИ без санкции руководства.

4.2.6. Передавать третьим лицам сетевые адреса, имена, пароли, информацию о привилегиях пользователей, конфигурационные настройки.

4.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокировке, потери информации и предупреждения пользователей.

4.2.8. Нарушать правила эксплуатации оборудования ИСПДн.

4.2.9. Корректировать, удалять, подменять журналы аудита.

5. Права и ответственность Администратора безопасности

5.1. Администратор безопасности имеет право:

5.1.1. Получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и рабочих станций пользователей.

5.1.2. Требовать от пользователей ИСПДн выполнения инструкций по обеспечению безопасности персональных данных в ИСПДн.

5.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

5.1.4. Осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим докладом ответственному за организацию обработки персональных данных.

5.1.5. Производить анализ защищенности ИСПДн и попыток взлома системы защиты ИСПДн путем применения специальных средств.

5.1.6. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

5.2. Администратор несет ответственность за:

5.2.1. Реализацию утвержденных в Организации документов, регламентирующих порядок обеспечения безопасности персональных данных.

5.2.2. Программно - технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и автоматизированные системы обработки информации, закрепленные за ним приказом

руководителя Организации и за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

5.2.3. Разглашение персональных данных и сведений ограниченного распространения, ставших известными ему при выполнении функциональных обязанностей.

5.2.4. Качество и последствия проводимых им работ по контролю действий пользователей при работе в ИСПДн.

6. Организация учета лиц, допущенных к работе с персональными данными

6.1. Администратор безопасности предоставляет пользователям доступ к персональным данным по списку пользователей, допущенных к работе с персональными данными в ИСПДн. Список пользователей ведется в специальном журнале учета (Приложение 1).

6.2. На основании списка Администратор безопасности разрабатывает таблицу разграничения доступа к персональным данным в ИСПДн (далее матрицу доступа).

6.3. Матрица доступа (Приложение 2) составляется как на электронном, так и на бумажном носителях. На бумажном носителе матрица доступа составляется в двух экземплярах: подлинник (контрольный экземпляр) и рабочий экземпляр.

6.4. Администратор безопасности на основании матрицы доступа предоставляет пользователям доступ к информационным ресурсам ИСПДн. Проверяет на ПЭВМ пользователя заданные возможности доступа и выдает пользователю под расписку в соответствующем журнале учета его персональный идентификатор.

6.5. Администратор безопасности, обеспечивающий эксплуатацию комплекса средств автоматизации, иные пользователи, допущенные к персональным данным, имеют право предоставлять такие сведения только руководителю Организации, а также лицам, имеющим право получать указанные сведения в соответствии с настоящей Инструкцией, соответствующими федеральными законами и другими нормативно-правовыми актами. Передавать проверяющим организациям сами персональные данные запрещается. Проверяться должны только документы, описывающие защиту.

7. Порядок учета средств защиты персональных данных и эксплуатационной и технической документации к ним

7.1. Используемые средства защиты персональных данных, в т.ч. криптографические (далее средства защиты), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету Администратором безопасности в журналах установленной формы. Средства защиты, эксплуатационная и техническая документация к ним, ключевые документы доставляются Администратором безопасности при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

7.2. Передача средств защиты, эксплуатационной и технической документации к ним между пользователями производится под расписку в соответствующем журнале.

7.3. Носители программного обеспечения, эксплуатационную и техническую документацию к ним, ключевые документы хранятся в шкафах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.4. Системные блоки рабочих станций, на которые установлены программные средства защиты, оборудуются средствами контроля за их вскрытием (опечатываются). Место опечатывания должно быть таким, чтобы его можно было визуально контролировать.

7.5. Уничтожение программных средств защиты производится Администратором безопасности по указанию органа криптографической защиты с составлением акта. Акт об уничтожении средств криптографической защиты информации (далее СКЗИ) представляется в орган криптографической защиты.

7.6. Ключевые документы уничтожаются Администратором безопасности не позднее 10 суток после вывода их из действия (окончания срока действия) с отметкой об уничтожении в соответствующем журнале.

7.7. Учет средств защиты информации производится в соответствующих журналах:

«Журнал поэкземплярного учета средств защиты информации, эксплуатационной и

технической документации к ним»;

«Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов».

8. Порядок учета, хранения и выдачи носителей ПДн

8.1. При учете носителей реализуются следующие требования обеспечения защиты персональных данных:

- формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;
- предупреждение возможности нецелевого использования носителя или его неправильного хранения;
- предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, частей фото-, видео- или магнитной пленки), для чего фиксируются технические характеристики носителя (количество листов, длина ленты, наличие склеек и др.);
- включение носителя в сферу регулярного контроля сохранности и местонахождения;
- предотвращение выдачи носителя лицу, исключенному из состава лиц, допускаемых к данному носителю (составляемому документу);
- выявление факта утраты носителя или его частей, организация поиска носителя и проведения служебного расследования;
- предотвращение нарушения принципа персональной ответственности за сохранность носителя и фиксируемых в нем персональных данных;
- обнаружение факта подмены носителя другим, фальсификации части носителя;
- обнаружение фактов случайной или умышленной порчи носителя, изменения формата, нумерации листов, вырывания листов, их загрязнения, склеивания и т.п.;
- предотвращение несанкционированной и неоправданной деловой необходимостью передачи носителя между руководителями и исполнителями;
- предотвращение несанкционированного ознакомления посторонних лиц с содержанием информации, зафиксированной на носителе, в процессе его выдачи исполнителю и прием от исполнителя.

8.2. Обязательному инвентарному учету и маркировке подлежат магнитные носители персональных данных, для которых любые угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений.

8.3. Этапы оформления и учета носителей персональных данных, выдачи их исполнителям и приема от исполнителей выполняются как в традиционном, так и автоматизированном режимах и включают в себя следующие процедуры:

- первичное оформление носителя, в процессе которого выполняются специализированные операции, позволяющие в дальнейшем контролировать подлинность носителя и сохранность всех его элементов;
- традиционный или автоматизированный учет носителя, при котором документируется факт включения носителя в категорию носителей ограниченного доступа с присвоением ему инвентарного номера;
- окончательное оформление носителя, в процессе которого учетные данные переносятся на носитель и его составные части для их идентификации;
- выдача учтенного, укомплектованного носителя персональных данных исполнителю, закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование;
- выдача исполнителю при необходимости дополнительных учтенных листов, форм и бланков;

- прием от исполнителя носителя информации, в процессе которого проверяются комплектность носителя, наличие оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя;
- ежедневная проверка правильности учета носителей и их наличия.

9. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения и персональных данных

9.1. Администратор безопасности организует архивирование и восстановление прикладного программного обеспечения и персональных данных на рабочих станциях пользователей.

9.2. Администратор безопасности осуществляет:

- ведение графика резервных копий;
- восстановление утерянных данных;
- контроль за созданием резервных копий персональных данных;
- создание подробного отчета о каждой архивации, содержащий информацию о всех заархивированных и пропущенных файлах и папках;
- ведение учета заданий архивации в виде календаря, в котором указаны дни и время, когда они выполнялись. Для каждого задания должны указываться: тип архива и местоположение носителя;
- оказание помощи в решении проблем, возникающих при эксплуатации программ архивирования.

9.3. Средства организации архивирования и восстановления прикладного программного обеспечения должны устанавливаться на всех средствах вычислительной техники.

9.4. Порядок применения средств организации архивирования и восстановления прикладного программного обеспечения устанавливается с учетом соблюдения следующих требований:

- обязательное хранение всех архивов в защищенном месте;
- частота архивации данных зависит от их важности и частоты их изменения;
- системные папки операционной системы необходимо архивировать после серьезных изменений конфигурации;
- данные, которые изменяются очень редко, не имеет смысла архивировать.
- восстановление работоспособности программных средств и информационных массивов, в случае утери и повреждения.

9.5. Организации архивирования и восстановления прикладного программного обеспечения подлежат следующие файлы и документы:

- все файлы операционной системы и установленных приложений. Архивирование системных файлов должно производиться только после установки новых приложений или обновления самой операционной системы;
- личные профили пользователей;
- папки, содержащие важные документы;
- базы данных;
- другие файлы и папки, представляющие ценность.

9.6. Организация архивирования и восстановления прикладного программного обеспечения и персональных данных является необходимым элементом защиты информационных ресурсов от их модификации и уничтожения. Организация архивирования и восстановления прикладного программного обеспечения и персональных данных на серверах и рабочих станциях должна, как правило, проводиться по согласованию с Администратором безопасности в нерабочее время, за исключением внештатных ситуаций.

10. Требования к организации парольной защиты

10.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями осуществляет Администратор безопасности.

10.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

10.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности ИСПДн. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самого Администратора безопасности с паролями пользователей.

10.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

10.5. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы персональных данных в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа) должна производиться Администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

10.6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа) Администратора безопасности и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

10.7. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.9.6 или п.9.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

11. Порядок подключения рабочих станций к сетям общего пользования

11.1. Сеть общего пользования является открытой системой передачи данных, при работе в которой могут возникнуть следующие основные угрозы безопасности информации:

– заражение информационно-вычислительных ресурсов программными вирусами;
– несанкционированный доступ внешних пользователей к ресурсам информационной системы персональных данных;
– внедрение в автоматизированные системы программных закладок;
– загрузка трафика нежелательной корреспонденцией (спамом);
– несанкционированная передача персональных данных пользователями ИСПДн в сети общего пользования.

11.2. Для предотвращения указанных угроз необходимо:

– разграничить доступ пользователей к ресурсам сетей общего пользования путём использования средств межсетевого экранирования защищённого сегмента локальной вычислительной сети, в котором происходит обработка персональных данных;
– осуществлять контроль за персональными данными, выходящими из информационной системы Организации и загружаемых из сети общего пользования;

– передача информации с персональными данными при использовании каналов связи сети общего пользования должна осуществляться только с применением средств криптографии.

12. Организация обмена персональными данными со сторонними организациями

При приеме и передаче персональных данных Администратор безопасности должен учитывать следующие требования:

- коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны;
- при конфигурировании коммуникационного оборудования (маршрутизаторов, концентраторов, мостов и мультиплексоров) и прокладке кабельной системы ЛВС необходимо учитывать разделение трафика по отдельным сетевым фрагментам на производственной основе и видам деятельности предприятия;
- подключение ЛВС к другой автоматизированной системе (локальной или неоднородной вычислительной сети) иного класса защищенности должно осуществляться с использованием межсетевого экрана, требования к которому определяются РД Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи.

13. Порядок применения средств антивирусной защиты информации

13.1. Средства антивирусной защиты информации должны устанавливаться на всех средствах вычислительной техники, обрабатывающих персональные данные.

13.2. Порядок применения средств антивирусной защиты информации устанавливается с учетом соблюдения следующих требований:

- обязательный входной контроль за отсутствием программных вирусов во всех поступающих в Организацию электронных носителях информации, информационных массивах, программных средствах общего и специального назначения;
- обязательная проверка всех электронных писем на предмет отсутствия программных вирусов;
- периодическая проверка на предмет отсутствия программных вирусов жестких магнитных дисков (не реже одного раза в неделю) и обязательная проверка съемных носителей информации перед началом работы с ними;
- внеплановая проверка жестких магнитных дисков и съемных носителей информации в случае подозрения на наличие программных вирусов;
- восстановление работоспособности программных средств и информационных массивов, поврежденных программными вирусами.

13.3. Инсталляция и настройка средств антивирусной защиты информации осуществляются в соответствии с программной и эксплуатационной документацией, поставляемой в комплекте с ними.

13.4. Копирование любой информации, переносимой с помощью любых съемных носителей информации, должно производиться только после проведения процедуры полного антивирусного контроля съемного носителя.

13.5. Антивирусная профилактика является необходимым элементом защиты информационных ресурсов от их модификации и уничтожения. Антивирусная профилактика состояния средств антивирусной защиты информации на серверах и рабочих станциях должна проводиться по согласованию с Администратором безопасности.

13.6. Своевременное обновление баз данных средств антивирусной защиты информации в структурных подразделениях является неотъемлемой частью обеспечения эффективной политики антивирусной защиты информации.

13.7. Обновление баз данных средств антивирусной защиты информации на рабочих станциях и серверах осуществляется в автоматическом режиме.

13.8. На рабочем месте Администратора безопасности могут быть установлены средства,

позволяющие через ЛВС управлять компонентами системы антивирусной защиты, установленными на рабочих станциях и серверах в структурных подразделениях, а также проводить обновления баз средств антивирусной защиты информации. В случае если рабочая станция пользователя не подключена к ЛВС, обновление средств антивирусной защиты информации производится пользователем через съемные носители информации. Периодичность обновления определяется программными требованиями средств антивирусной защиты информации или устанавливается Администратором безопасности.

13.9. При невозможности ликвидации последствий заражения программными вирусами Администратору безопасности необходимо:

• сообщить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

• заархивировать зараженные файлы с внедренными программными вирусами и направить в организацию, осуществляющую техническую поддержку эксплуатации средств антивирусной защиты информации;

• осуществить полную переустановку программного обеспечения на зараженном компьютере.

13.10. Все факты модификации и разрушения данных на серверах или рабочих станциях, заражение их вирусами, а также обнаружение других вредоносных программ классифицируются как значимые нарушения информационной безопасности и должны анализироваться посредством проведения служебного расследования.

14. Контроль эффективности защиты персональных данных

14.1. С целью своевременного выявления и предотвращения утечки персональных данных по техническим каналам, исключения или существенного затруднения несанкционированного доступа к ним и предотвращения специальных программно-технических воздействий, вызывающих нарушение конфиденциальности, целостности или доступности персональных данных, в Организации электронных носителях информации проводится периодический (не реже одного раза в год) контроль состояния защиты информации.

14.2. Контроль заключается в проверке выполнения требований нормативных документов по защите персональных данных, а также в оценке их обоснованности и эффективности принятых мер.

14.3. Средства и системы защиты, применяемые в Организации электронных носителях информации, для обеспечения безопасности персональных данных нуждаются в контроле эффективности выполняемых задач, заключающемся в следующем:

- периодическая проверка состояния используемых СЗИ;
- проверка правильности настройки СЗИ;
- проверка правильности функционирования СЗИ:
  - для СКЗИ – проверка журнала пакетов входящих/ исходящих;
  - для СЗИ от НСД – невозможность входа в ОС без введения пароля пользователя или использования электронного идентификатора iButton.

Итоги контроля Администратор безопасности фиксирует в «Журнал по учету мероприятий по контролю обеспечения защиты персональных данных в ИСПДн».

15. Организация обучения

15.1. Уровень знаний Администратора безопасности должен быть достаточным для выполнения работ по настройке, поддержания в работоспособном состоянии и контроля эффективности системы защиты персональных данных.

15.2. Обучение Администратора безопасности включает подготовку по следующим направлениям:

— методы и способы противодействия несанкционированному доступу к защищаемой конфиденциальной информации;

— методы и способы противодействия утечки информации по каналам побочных электромагнитных излучений и наводок;

— методы и способы противодействия вирусным угрозам (использование антивирусного программного обеспечения);

— методы и способы обнаружение сетевых вторжений в сегмент локальной вычислительной сети, в котором производится обработка персональных данных;

— криптографические методы защиты конфиденциальной информации при ее передаче по открытым каналам связи;

— основы законодательства Российской Федерации в области обеспечения безопасности персональных данных в ИСПДн.

15.3. В ходе выполнения своих должностных обязанностей Администратору безопасности необходимо проводить периодический инструктаж сотрудников подразделения (пользователей средств вычислительной техники) по правилам работы с используемыми средствами и системами зашиты персональных данных.

15.4. Инструктажи проводятся в помещениях Организации электронных носителях информации, непосредственно на рабочих местах пользователей ПЭВМ, обрабатывающих персональные данные.

15.5. В ходе инструктажей освещаются следующие вопросы:

— правила работы со средствами защиты информации от несанкционированного доступа;

— правила работы с персональными идентификаторами;

— правила парольной защитой ПЭВМ;

— правила работы с антивирусными средствами, в том числе при использовании отчуждаемых (сменных) носителей;

— правила работы с криптографическими средствами защиты конфиденциальной информации при ее передачи по открытым каналам связи.

15.6. Помимо периодических инструктажей Администратор безопасности проводит первичный инструктаж вновь допущенных к персональным данным сотрудников Организации электронных носителях информации, по правилам работы с используемыми средствами и системами зашиты персональных данных. Освещаемые вопросы в ходе первичного инструктажа аналогичны вопросам при периодических инструктажах.

_____	_____	_____
(должность)	(подпись)	(ФИО)

«___» _____ 201_ г.

С инструкцией ознакомлен:

Инженер-электроник	_____	Гилязова Е.А.
(должность)	(подпись)	(ФИО)

«01» 01 2016 г.

Приложение 1

ЖУРНАЛ

учёта списка пользователей ИСПДн

№ п/п	Фамилия И.О.	Номер ПЭВМ	Дата начала допуска к ПДн	Подпись	Дата окончания допуска к ПДн
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					

Приложение 2

МАТРИЦА

доступа пользователей к ИСПДн

№ п/п	Группа	ФИО сотрудника	Уровень доступа к ПДн
1.	Пользователи		
2.	Пользователи		
3.	Пользователи		
4.	Пользователи		
5.	Администратор		
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			