УТВЕРЖДЕНА
Распоряжением Главы
сельского поселения Красный Яр
муниципального района Красноярский
Самарской области
от 18.08.2022 г № 53

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Настоящая инструкция разработана на основании постановления Правительства Российской Федерации от 21 марта 2012г. № 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», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», «Положением об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных и других нормативно-правовых актов регулирующих обработку персональных данных в автоматизированных системах.

1.2. Инструкция определяет функции, права и обязанности ответственного за обеспечение безопасности персональных данных в Администрации сельского поселения Красный Яр (далее — Администрация) по вопросам обеспечения информационной безопасности при обработке персональных данных.

1.3. Ответственный за обеспечение безопасности персональных данных назначается из числа сотрудников и обеспечивает правильность использования и нормальное функционирование установленных средств защиты информации (далее - СЗИ).

1.4. К СЗИ относятся средства защиты от несанкционированного доступа (далее - НСД), средства межсетевого экранирования, а также антивирусные средства.

1.5. К выполнению обязанностей в области организации разграничения доступа, настройке локальной вычислительной сети ответственный за обеспечение безопасности персональных данных может привлекать к работам сторонних сотрудников. Все работы должны согласовываться с Главой поселения и проводиться только в присутствии ответственного за обеспечение безопасности персональных данных при этом не должны затрагиваться средства защиты информации от несанкционированного доступа и обрабатываемые персональные данные.

1.6. К выполнению обязанностей в области сопровождения средств защиты информации от НСД и их настройки ответственный за обеспечение безопасности персональных данных выполняет только по согласованию с органом, проводившим аттестационные мероприятия.

1.7. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения защиты персональных данных, и не исключает обязательного выполнения их требований.

2. Основные задачи и функции ответственного за обеспечение безопасности персональных данных.

2.1. Основными задачами ответственного за обеспечение безопасности персональных данных является:

2.1.1. Сопровождение средств защиты информации от несанкционированного доступа (далее - СЗИ от НСД) и основных технических средств и систем (далее - ОТСС);

2.1.2. Организация разграничения доступа;

2.1.3. Контроль эффективности защиты информации.

2.2. Для выполнения поставленных задач, на ответственного за обеспечение безопасности персональных данных возлагаются следующие функции:

2.2.1. Контроль за выполнением требований действующих нормативных документов по

вопросам обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных.

2.2.2. Настройка и организация сопровождения в процессе эксплуатации подсистемы управления доступом на рабочих станциях (далее - РС):

— опыт реализации полномочий доступа (чтение, запись, модификация, создание, удаление) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтерам);

— опыт ввода описаний пользователей ИСПДн в информационную базу, установленную на РС СЗИ от НСД;

— организация своевременного удаления описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе на РС лиц.

2.2.3. Контроль доступа лиц в помещения, где расположены технические средства ИСПДн, в соответствии со списком сотрудников, допущенных к работе в ИСПДн.

2.2.4. Контроль проведения смены паролей для доступа к ИСПДн пользователями ИСПДн. Периодичность смены паролей – 90 дней.

2.2.5. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

— введение в базу данных, установленную на РС СЗИ от НСД описания событий, подлежащих регистрации в системном журнале;

— регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам.

2.2.6. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

— организация периодического тестирования функций установленной на РС СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

— организация восстановления программной среды, программных средств и настроек СЗИ при сбоях;

— организация поддержания установленного порядка и правил антивирусной защиты информации на ПЭВМ;

— контроль за периодическим обновлением антивирусных средств (баз данных), установленных на РС, контроль соблюдения пользователями порядка и правил антивирусной защиты.

2.2.7. Контроль соблюдения требований по размещению и использованию ИСПДн, указанных в Техническом паспорте.

3. Права и обязанности администратора безопасности

3.1. Для реализации поставленных задач и возложенных функций, ответственный за обеспечение безопасности персональных данных ОБЯЗАН:

3.1.1. Сопровождать СЗИ от НСД и ОТСС:

— вести учет и знать перечень установленных в ИСПДн ОТСС, СЗИ от НСД и перечень задач, решаемых с их использованием.

— осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на РС специальных программных и программно-аппаратных СЗИ от НСД.

— присутствовать при внесении изменений в конфигурацию (модификации) аппаратнопрограммных средств защищенных РС и серверов, осуществлять проверку работоспособности системы зашиты после установки (обновления) программных средств в ИСПДн.

— периодически проверять состояние используемых СЗИ от НСД, осуществлять проверку правильности их настройки (выборочное тестирование).

— контролировать соответствие технического паспорта объекта вычислительной техники (далее - СВТ) фактическому составу (комплектности) СВТ в ИСПДн и вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн).

— вести учет нештатных ситуаций, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн.

— проводить инструктаж (первичный, периодический, внеочередной) сотрудников больницы, допущенных к обработке персональных данных в ИСПДн по правилам работы с используемыми средствами и системами зашиты информации.

3.1.2. Организовывать разграничения доступа:

а) участвовать в разработке и знать перечень защищаемых информационных ресурсов ИСПДн.

б) разрабатывать совместно с администраторами ЛВС решения по:

— приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;

— определению списка устройств, логических дисков, каталогов общего пользования на серверах, с указанием состава допущенных к ним пользователей и режимов допуска (матрица доступа);

- осуществлению контроля за наличием активных компьютеров сети, состоянием активных пользователей, использованием разделяемых ресурсов, процессом печати на общих принтерах;

— разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов);

— разработке порядка выхода пользователей в сети общего пользования (Internet) и использованию встроенных СЗИ от НСД в сервисных программах;

— определению режимов использования СЗИ от НСД: защита паролей, защита в протоколах передачи данных, кодирование файлов, в случае необходимости подключение дополнительных алгоритмов криптографической защиты и подтверждение подлинности электронных документов (электронная цифровая подпись);

— разработке политики аудита: определению состава регистрируемых событий и списка лиц, имеющих допуск к журналам аудита.

в) осуществлять учет и периодический контроль состава и полномочий пользователей различных РС в ИСПДн.

г) контролировать и требовать соблюдения установленных правил по организации парольной защиты в больнице.

д) контролировать обеспечение защиты информации, содержащей персональные данные при взаимодействии с информационными сетями общего пользования и требовать соблюдения установленных правил по использованию сетей общего пользования (Интернет) в больнице;

е) контролировать выполнение требований парольной защиты в больнице;

ж) осуществлять оперативный контроль работы пользователей защищенных РС, анализировать содержимое журналов событий операционных систем (далее - ОС), систем управления базами данных (далее - СУБД), пакетов прикладных программ и СЗИ от НСД всех РС и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование журналов событий РС и надлежащий режим хранения данных архивов.

з) принимать участие в работах по внесению изменений в аппаратно-программную конфигурацию серверов и РС в ИСПДн.

и) обеспечивать строгое выполнение требований безопасности информации при организации технического обслуживания РС и отправке их в ремонт (контролировать стирание информации на магнитных носителях).

к) организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль правильности их использования. л) осуществлять периодический контроль порядка учета, создания, хранения и использования резервных и архивных копий массивов данных.

м) по указанию руководства своевременно и точно отражать изменения в организационнораспорядительных и нормативных документах по управлению СЗИ от НСД, установленных на РС в ИСПДн.

н) требовать от пользователей стирания остаточной информации на несъёмных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки РС.

б) докладывать гл. врачу больницы о выявленных угрозах безопасности информации

3.1.3. Контролировать эффективность защиты информации:

а) проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам РС.

обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам РС.

в) проводить занятия с пользователями ИСПДн по правилам работы на РС, оснащенных СЗИ от НСД, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности зашиты информации.

г) участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в АС.

3.2. Ответственному за обеспечение безопасности персональных данных запрещается:

3.2.1. Используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей в ИСПДн, получать доступ к персональным данным и предоставлять доступ другим лицам с целью ознакомления, модификации, копирования, уничтожения, блокирования доступа к информации;

3.2.2. Использовать ставшие доступными в ходе исполнения служебных обязанностей идентификационные данные пользователей (имя, пароль, ключи и т.п.) для маскирования своих действий;

3.2.4. Использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, а также предоставлять такую возможность другим лицам;

3.2.5. Выключать СЗИ от НСД, установленные в ИСПДн, без санкции гл. врача больницы;

3.2.6. Передавать третьим лицам тем или иным способом сетевые адреса, имена, пароли, информацию о привилегиях пользователей ИСПДн, конфигурационные настройки ИСПДн;

3.2.7. Производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы ИСПДн, блокированию доступа, потере информации без санкции гл. врача больницы и предупреждения пользователей ИСПДн;

3.2.8. Нарушать правила эксплуатации оборудования ИСПДн;

3.2.9. Корректировать, удалять, подменять журналы аудита событий в ИСПДн.

4. Права и ответственность ответственного за обеспечение безопасности персональных данных

4.1. Ответственный за обеспечение безопасности персональных данных имеет право:

4.1.1. Получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах ИСПДн и РС пользователей;

4.1.2. Требовать от пользователей ИСПДн выполнения требований нормативно-методических документов в больнице по обеспечению безопасности и защите персональных данных.

4.1.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения безопасности персональных данных, НСД, утраты, порчи защищаемой информации, содержащей персональные данные и технических компонентов ИСПДн;

4.1.4. Осуществлять оперативное вмешательство в работу пользователя ИСПДн при явной угрозе безопасности персональным данным в результате несоблюдения установленной технологии обработки персональных данных и невыполнения требований по безопасности с последующим докладом ответственному за обеспечение безопасности персональных данных.

4.1.5. Производить анализ защищенности ИСПДн путем применения специального программного обеспечения, осуществления попыток взлома системы защиты ИСПДн. Такие работы должны проводиться в часы наименьшей информационной нагрузки с обязательным уведомлением гл. врача больницы.

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

4.2. Ответственный за обеспечение безопасности защиты персональных данных несет ответственность за:

4.2.1. Реализацию принятых в ИСПДн мероприятий по защите персональных данных;

4.2.2. Программно — технические средства защиты информации, технические средства вычислительной техники ИСПДн, закрепленные за ним, а также за качество проводимых им работ по обеспечению защиты персональных данных в соответствии с функциональными обязанностями.

4.2.3.За несоблюдение требований по защите персональных данных ответственный за обеспечение безопасности персональных данных несет ответственность в соответствии с законодательством Российской Федерации