Научно-исследовательский радиофизический институт
федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» **(НИРФИ ННГУ им. Н.И. Лобачевского)**

СОГЛАСОВАНО

Начальник 117 военного представительства Министерства обороны Российской Федерации

А.В. Нефёдов

«09» 12 2019 г.

УТВЕРЖДАЮ

Директор НИРФИ ННГУ им. Н.И. Лобачевского

С.В. Оболенский

«09» 2019 г.

СТАНДАРТ ОРГАНИЗАЦИИ

Система менеджмента качества

Информационная безопасность

СТО НИРФИ 07–2019

Экземпляр №____________

Нижний Новгород

Предисловие

1 РАЗРАБОТАН ответственным представителем руководства

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Приказом Директора от 21.12.2019 № 10-ОД

3 СТАНДАРТ РАЗРАБОТАН с учетом требований ГОСТ Р ИСО 9001-2015, ГОСТ РВ 0015-002-2012, а также стандартов ННГУ им. Н.И. Лобачевского

4 ВВЕДЁН *ВПЕРВЫЕ*

5 СТАНДАРТ РАЗРАБОТАН в обеспечение выполнения Решения КС № 1 от 07.10.2019 года *«О доработке системы менеджмента качества до уровня требований определенных стандартами ГОСТ Р ИСО 9001-2015 и ГОСТ РВ 0015-002-2012»*

Содержание

1 Назначение и область применения

1.1 Данный СТО устанавливает требования к менеджменту информационной безопасности.

1.2 Требования данного СТО распространяются и обязательны для исполнения сотрудниками предприятия, оказывающих услуги по организации системы защиты информации и вводу данных (системный администратор) и пользователями информационных систем предприятия.

2 Нормативные ссылки

2.1. В настоящем стандарте использованы ссылки на следующие нормативные документы:

ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования

ГОСТ РВ 0015-002-2012 Система разработки и постановки продукции на производство военной техники. Системы менеджмента качества. Общие требования

Федеральный закон от 27.07.2006 N 149 "Об информации, информационных технологиях и о защите информации»;

ГОСТ Р ИСО/МЭК 27001-2006 Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования.

Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Федеральный закон "Об электронной подписи" № 63 от 06.04.2011;

Федеральный закон от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне».

Постановление от 17 ноября 2007 г. N 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

СТО НИРФИ 01-2019 Требования к составу, содержанию и оформления стандартов предприятия

СТО НИРФИ 06-2019 Управление записями по качеству

3 Термины, определения, обозначения и сокращения

В настоящем стандарте используются определения, соответствующие ГОСТ Р ИСО 9000, а также следующие определения:

3.1 Термины и определения:

3.1.1 **информационная система**: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.1.2 **пользователь**: Лицо или организация, которое использует действующую информационную систему для выполнения конкретной функции.

3.1.3 **программное обеспечение**: всё или часть программ, процедур, правил и соответствующей документации системы обработки информации.

3.1.4 **резервное копирование**: Процесс создания копии данных, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

3.1.5 **информационная безопасность**: Сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность и надежность.

3.1.6 **ответственный за СМИБ**: Сотрудник предприятия назначенный ответственным за разработку, внедрение, поддержание в рабочем состоянии и совершенствование СМИБ

3.2 Сокращения

ГОСТ – государственный стандарт;

ГОСТ Р – национальный стандарт;

ДОУ – документационное обеспечение и управление;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
СЗПДн – системы защиты персональных данных;
НСД - несанкционированный доступ;
ПЭМИН – побочные электромагнитные излучения и наводки;
ПК – персональный компьютер;
ПО – программное обеспечение;
СМИБ – система менеджмента информационной безопасности;

4 Обеспечение информационной безопасности

4.1 Основные положения

4.1.1 Ответственный за СМИБ назначается приказом директора.

4.1.2 Целью данного СТО является эффективное осуществление менеджмента защиты информации. Требования СТО описывают порядок создания, внедрения, эксплуатации, постоянного контроля, анализа и улучшения системы защиты информации.

4.1.3 Организация системы защиты информации включает следующие действия:

– планирование и создание системы защиты информации;

– внедрение и эксплуатация системы защиты информации;

– контроль и анализ системы защиты информации;

4.1.4 При наличии соответствующих требований в контрактах (договорах) ответственный за СМИБ организует выполнение работ по обеспечению информационной безопасности в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001.

4.2 Планирование и создание системы защиты информации

В целях эффективного планирования и создания системы защиты информации устанавливается следующая Политика информационной безопасности.

4.2.1 Политика информационной безопасности

4.2.1.1 Целями настоящей Политики являются:

– сохранение конфиденциальности критичных информационных ресурсов;

– обеспечение непрерывности доступа пользователей к информационным ресурсам для поддержки бизнес-деятельности;

– защита целостности деловой информации с целью поддержания возможности организации и ее клиентов по оказанию услуг высокого качества и принятию эффективных управленческих решений;

- защита персональных данных работников (в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»);

– повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами;

– определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности.

4.2.1.2 Руководители подразделений Организации, а также пользователи информационных систем должны обеспечить регулярный контроль за соблюдением положений настоящей Политики.

4.2.2 Область применения политики информационной безопасности

4.2.2.1 Требования Политики распространяются на всю информацию и ресурсы обработки информации предприятия и пользователей информационных систем. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

4.2.2.2 Организации принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация (в том числе на вычислительных ресурсах, приобретенных (полученных) и введенных в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством).

4.2.2.3 Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Организации, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Организации.

4.2.3 Внедрение и эксплуатация системы защиты информации

4.2.3.1 Ответственность за информационные активы

Перечень документации и информации, имеющей ограничения на распространение, определяется согласно приложению А СТО НИРФИ 06. По инициативе руководителей любого уровня Ответственным за СМИБ должен быть оперативно рассмотрен вопрос об уточнении перечня с учетом необходимости изменения прав доступа к записям. Ответственный за СМИБ должен обеспечить ознакомление с процедурой информационной безопасности сотрудников, которые являются или могут стать обладателями информации, к которой есть ограничение прав доступа.

4.2.3.2 Контроль доступа к информационным системам. Общие положения

4.2.3.2.1 Все работы в пределах офисов организации выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

4.2.3.2.2 В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход пользователя в систему должен осуществляться с использованием уникального имени пользователя и пароля.

4.2.3.2.3 Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется удаленно на дому.

4.2.3.2.4 В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 (пятнадцати) минут.

4.2.4 Доступ третьих лиц к информационной системе

4.2.4.1 Доступ третьих лиц к информационным системам Предприятия должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Предприятия должен быть четко определен, контролируем и защищен.

Удаленный доступ

4.2.4.2 Удаленный доступ к информационным ресурсам Организации не представляется.

4.2.5 Доступ к сети Интернет

4.2.5.1 Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила работы в сети Интернет при выполнении сотрудниками Организации своих трудовых функций:

– сотрудникам Организации и пользователям информационных систем разрешается использовать сеть Интернет только в служебных целях;

– запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

– сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Организации;

– запрещен доступ в Интернет через сеть Организации для всех лиц, не являющихся сотрудниками.

4.2.6 **Защита оборудования**

4.2.6.1 Сотрудники Организации и пользователи информационных систем должны обеспечивать безопасность оборудования, на котором хранится информация Организации.

4.2.6.2 Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Изменения организуются ответственным за СМИБ.

4.2.7 **Аппаратное обеспечение**

4.2.7.1 Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Организации, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

4.2.7.2 Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

4.2.7.3 Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться в отдел технической поддержки. Данные не должны быть скомпрометированы в случае халатности или небрежности, приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

4.2.7.4 При записи какой-либо информации на носитель для передачи его контрагентам необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных.

4.2.7.5 Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства, не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

4.2.8 **Программное обеспечение**

4.2.8.1 Все программное обеспечение, установленное на обслуживаемом предприятии компьютерном оборудовании, должно использоваться исключительно в производственных целях.

4.2.8.2 Пользователям информационных систем запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника.

4.2.8.3 На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

– персональный межсетевой экран;

– антивирусное программное обеспечение;

4.2.8.4 Все компьютеры, подключенные к информационным системам, должны быть оснащены системой антивирусной защиты. Пользователям информационных систем запрещается:

– блокировать антивирусное программное обеспечение;

– устанавливать другое антивирусное программное обеспечение;

– изменять настройки и конфигурацию антивирусного программного обеспечения.

4.2.9 **Правила пользования электронной почтой**.

4.2.9.1 Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес деятельности.

4.2.9.2 Строго конфиденциальная информация, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

4.2.9.3 Сотрудники Организации и пользователи информационных систем для обмена документами с бизнес-партнерами должны использовать только свой официальный адрес электронной почты.

4.2.9.4 Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма, и факсимильные сообщения.

4.2.9.5 В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать ответственного за СМИБ.

4.2.9.6 Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

4.2.9.7 Недопустимы следующие действия при использовании электронной почты:

– рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

– рассылка рекламных материалов, не связанных с деятельностью Организации;

– подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

– поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

– пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности или беспорядков.

4.2.9.8 Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

4.2.10 **Сообщение об инцидентах информационной безопасности, реагирование и отчетность**

4.2.10.1 Все пользователи должны быть осведомлены о своей обязанности сообщать ответственному за СМИБ, собственности и режиму об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

4.2.10.2 В случае кражи или утери переносного компьютера следует незамедлительно сообщить об инциденте ответственному за СМИБ.

4.2.10.3 Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

4.2.10.4 Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

– проинформировать ответственного за СМИБ;

– не пользоваться и не выключать зараженный компьютер;

– не подсоединять этот компьютер к компьютерной сети Организации до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование системным администратором.

4.2.11 **Помещения с техническими средствами информационной безопасности**

4.2.11.1 Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

4.2.11.2 Участникам таких заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с ответственным за СМИБ.

4.2.11.3 Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник Организации, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

4.2.12 Управление сетью

4.2.12.1Сотрудникам предприятия и пользователям информационных систем запрещается:

– нарушать информационную безопасность и работу сети Организации;

– сканировать порты или систему безопасности;

– контролировать работу сети с перехватом данных;

– получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

– использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

– передавать информацию о сотрудниках или списки сотрудников Организации посторонним лицам;

– создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

4.2.13 **Защита и сохранность данных.**

4.2.13.1 Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Ответственный за СМИБ обязан оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

4.2.13.2 Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

4.2.13.3 Ответственный за СМИБ на основании заявок руководителей подразделений может создавать и удалять(организовывать данную работу) совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

4.2.13.4 Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

4.2.13.5 Все заявки на проведение технического обслуживания компьютеров должны направляться ответственному за СМИБ.

4.3 Контроль и анализ системы защиты информации

4.3.1 В целях постоянного контроля и анализа системы защиты информации, а также обеспечения ее постоянной пригодности, адекватности и результативности, ответственный за СМИБ ежегодно организует анализ организованной в соответствии с данным СТО системы защиты информации.

4.3.2 Результаты анализа, в части любых проблем информационной безопасности должны быть документированы и сообщены Генеральному директору для принятия решения.

4.4 Мониторинг (поддержка в рабочем состоянии и улучшение системы защиты информации)

4.4.1 Организация постоянно повышает результативность системы защиты информации посредством уточнения политики информационной безопасности (п. 4.2.1), использования результатов аудитов, осуществления корректирующих и предупреждающих действий, основанных на результатах анализа системы защиты информации в соответствии с п. 4.3.

4.4.2 В качестве предупреждающего действия разработана Модель угроз информационной безопасности (Приложение А), в соответствии с которой определены виды и вероятности угроз, и установлены технические и организационные меры по их противодействию.

5 Информация

Содержание информации	Ответственный за регистрацию	Форма записи	Кто информируется	Место и срок хранения	Право доступа	Способ восстановления
Модель угроз информационной безопасности	Ответственный за СМИБ	Приложение А	Ответственный за СМИБ	Ответственный за СМИБ, 5 лет	Без ограничения	По электронной копии Раздел 5 стандартов организации

СОГЛАСОВАНО

Инженер 117 военного представительства Минобороны России

_________ В.А. Васюнин

«9» 12 2019 г.

СОГЛАСОВАНО

Ответственный представитель по системе менеджмента качества НИРФИ ННГУ

_________ И.В. Ракуть

«9» 12 2019 г.

Приложение А (обязательное)
МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наименование угрозы	**Вероятность реализации угрозы**	**Опасность угрозы**	**Меры по противодействию угрозе**	
			Технические	**Организационные**
Угрозы от утечки по техническим каналам				
Угрозы утечки видовой информации				
Просмотр информации на дисплее сотрудниками, не допущенными к обработке персональных данных	Средняя вероятность	Низкая вероятность	Мониторы с малыми углами обзора, расположение ЭВМ	Инструкция пользователя
Просмотр информации на дисплее посторонними лица, находящимися в помещении, в котором ведется обработка персональных данных	Средняя вероятность	Низкая вероятность	Не требуются	Пропускной режим
Просмотр информации на дисплее посторонними лицами, находящимися за пределами помещения в котором ведется обработка персональных данных	Низкая вероятность	Низкая вероятность	Не требуются	Пропускной режим
Просмотр информации с помощью специальных электронных устройств, внедренных в помещении, в котором ведется обработка персональных данных	Низкая вероятность	Низкая вероятность	Не требуются	Пропускной режим
Угрозы утечки информации по каналам ПЭМИН	К информационным системам персональных данных 1-класса требования по защите от утечки информации по каналам ПЭМИН не предъявляются			
Утечка информации по сетям электропитания	-	-	-	-
Утечка за счет наводок на линии связи, технические средства, расположенные в помещении и системы	-	-	-	-

Наименование угрозы	**Вероятность реализации угрозы**	**Опасность угрозы**	**Меры по противодействию угрозе**	
			Технические	**Организационные**
коммуникаций				
Побочные излучения технический средств	-	-	-	-
Утечки за счет, электромагнитного воздействия на технические средства	-	-	-	-
Угрозы утечки акустической информации	-	-	-	-
Угрозы несанкционированного доступа к информации				
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
Кража ЭВМ	Низкая вероятность	Низкая вероятность	Пропуск, охранная сигнализация	Пропускной режим, охрана
Кража носителей информации	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим
Кража ключей доступа	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим, учет
Кража, модификация, уничтожение информации.	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим, учет
Вывод из строя узлов ЭВМ, каналов связи	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим, учет
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим, учет
Несанкционированное отключение средств защиты	Низкая вероятность	Низкая вероятность	Пропуск	Пропускной режим, учет
Угрозы хищения, несанкционированной модификации или блокирования информации				

Наименование угрозы	Вероятность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе	
			Технические	Организационные
за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);				
Компьютерные вирусы	Низкая вероятность	Низкая вероятность	Антивирусное ПО	Не требуется
Не декларированные возможности системного ПО и ПО для обработки персональных данных	Средняя вероятность	Низкая вероятность	Настройка средств защиты	Не требуется
Установка ПО, не связанного с исполнением служебных обязанностей	Низкая вероятность	Низкая вероятность	Настройка средств защиты	Не требуется
Наличие аппаратных закладок в приобретаемых ПЭВМ	Низкая вероятность	Низкая вероятность	Не требуется	Не требуется
Внедрение аппаратных закладок посторонними лицами после начала эксплуатации ИСПДн	Низкая вероятность	Низкая вероятность	Не требуется	Не требуется
Внедрение аппаратных закладок сотрудниками организации	Низкая вероятность	Низкая вероятность	Не требуется	Не требуется
Внедрение аппаратных закладок обслуживающим персоналом (ремонтными организациями)	Низкая вероятность	Низкая вероятность	Не требуется	Не требуется
Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.				
Утрата ключей доступа	Средняя вероятность	Низкая вероятность	Хранение в сейфе	Инструкция пользователя, инструкция администратора безопасности, журнал учета паролей
Непреднамеренная	Низкая веро-	Низкая ве-	Настройка	Резервное копиро-

Наименование угрозы	Вероятность реализации угрозы	Опасность угрозы	Меры по противодействию угрозе	
			Технические	Организационные
модификация (уничтожение) информации сотрудниками	ятность	роятность	средств защиты	вание
Непреднамеренное отключение средств защиты	Низкая вероятность	Низкая вероятность	Доступ только у администратора, настройка средств защиты	Не требуется
Выход из строя аппаратно-программных средств	Низкая вероятность	Низкая вероятность	Не требуется	Резервное копирование
Сбой системы электроснабжения	Средняя вероятность	Низкая вероятность	Источники бесперебойного питания	Резервное копирование
Стихийное бедствие	Низкая вероятность	Низкая вероятность	Пожарная сигнализация	Не требуется
Угрозы преднамеренных действий внутренних нарушителей				
Доступ к информации, модификация, уничтожение лицами, не допущенных к ее обработке	Низкая вероятность	Низкая вероятность	Настройка средств защиты	Не требуется
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Низкая вероятность	Низкая вероятность	Не требуется	Не требуется
Угрозы несанкционированного доступа по каналам связи				
Несанкционированный доступ через сети международного обмена	Низкая вероятность	Низкая вероятность	Firewall	Не требуется
Несанкционированный доступ через ЛВС организации	Низкая вероятность	Низкая вероятность	Настройка средств защиты	Не требуется
Утечка атрибутов доступа	Средняя вероятность		Пропуск, антивирусное ПО, firewall	Не требуется
Угрозы перехвата при передаче по проводным (кабельным) линиям связи				
Перехват за переделами с контролируемой зоны	Низкая вероятность	Низкая вероятность	firewall	Не требуется

Наименование угрозы	**Вероятность реализации угрозы**	**Опасность угрозы**	**Меры по противодействию угрозе**	
			Технические	**Организационные**
Перехват в пределах контролируемой зоны внешними нарушителями	Низкая вероятность	Низкая вероятность	Firewall Настройка средств защиты	Не требуется
Перехват в пределах контролируемой зоны внутренними нарушителями	Низкая вероятность	Низкая вероятность	Firewall Настройка средств защиты	Не требуется

Лист регистрации изменений

Изм.	Номера страниц			Номер извещения	Подпись	Дата
	замененных	новых	аннулиро-ванных			

Реестр рассылки стандарта СТО НИРФИ 07-2019

№ экземпляра	Подразделение/ Должность	Фамилия И.О. получателя	Подпись получателя	Дата получения

Разработчик 09.12.2019 Рашутов И.В.

(Подпись, дата) (Инициалы и фамилия)