Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «ИРНИТУ»

ОРИГИНАЛ

Содержание

УТВЕРЖДЕН
приказом И.о. ректора
(чем) (должность)
от «22» апреля 2015г. №424-П

П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «ИРНИТУ»	Взамен положения об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВПО «ИрГТУ» от 26.02.2015

1 Область применения

1.1 Настоящее положение устанавливает порядок организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования Иркутского национального исследовательского технического университета.

1.2 Настоящее положение распространяется на структурные подразделения и сотрудников ИРНИТУ, участвующих в предоставлении и обработке информации, содержащей персональные данные.

2 Нормативные ссылки

В настоящем положении использованы ссылки на следующие нормативные документы:

МС ИСО 9000:2005 Системы менеджмента качества. Основные положения и словарь.

МС ИСО 9001:2008 Системы менеджмента качества. Требования.

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

Постановление Правительства Российской Федерации от 1.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

СТО 002-2015 Система менеджмента качества. Порядок управления документацией СМК.

3 Термины, определения и сокращения

3.1 В настоящем положении применены следующие термины с соответствующими определениями, согласно МС ИСО 9000:2005:

Система менеджмента качества (СМК) – система менеджмента для руководства и управления организацией применительно к качеству.

Стандарт организации (СТО) – нормативный документ по стандартизации, разработанный, как правило, на основе согласия, характеризующегося отсутствием возражений по существенным вопросам у большинства заинтересованных сторон, устанавливающий комплекс норм, правил, требований к различным видам деятельности университета или их результатам и утвержденный руководством университета.

3.2 В настоящем положении используются следующие сокращения:

АРМ - автоматизированное рабочее место;

ИРНИТУ - федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет», далее по тексту Организация;

НСД - несанкционированный доступ;

ИСПДн - информационные системы персональных данных;

ПДн - персональные данные;

ПО - программное обеспечение;

ПЭВМ - персональная электронно-вычислительная техника;

СТО - стандарт организации;

ФСБ - Федеральная служба безопасности;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю.

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений, хранение (как на бумажном, так и на электронном носителе) данного положения организации возложена на директора центра информационной безопасности ИРНИТУ.

4.2 Разработчик настоящего положения осуществляет периодическую проверку (пересмотр) данного положения в установленном порядке согласно СТО 002-2015 «Порядок управления документацией СМК», разработанному по разделу 4.2.3 «Управление документами» МС ИСО 9001:2008.

4.3 Ответственность за организацию работ по защите персональных данных, при их обработке в ИСПДн возлагается на руководителей структурных подразделений ИРНИТУ, в которых осуществляется данная обработка.

5 Общие положения

5.1 Обработка персональных данных

5.1.1 Безопасность персональных данных, обрабатываемых в ИСПДн, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

5.1.2 Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и применение технических средств защиты информации (в том числе шифровальных (криптографических) средств, средств предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, средств межсетевого экранирования и обнаружения вторжений), а также используемые в информационной системе информационные технологии.

5.2 Обеспечение безопасности персональных данных

5.2.1 В ИРНИТУ мероприятия по обеспечению безопасности персональных данных в ИСПДн осуществляются:

a) администраторами ИСПДн (в соответствии с прилагаемой инструкцией (Приложение 1);

b) администраторами безопасности ИСПДн (в соответствии с прилагаемой инструкцией (Приложение 2);

c) пользователями ИСПДн (в соответствии с прилагаемой инструкцией (Приложение 3).

5.2.2 Для обеспечения безопасности персональных данных при их обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

5.2.3 Организация обеспечения безопасности персональных данных при их обработке в ИСПДн формируется в совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности персональных данных в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности персональных данных при их обработке в ИСПДн проводится путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы защиты персональных данных, развертываемой в процессе создания или модернизации ИСПДн.

5.2.4 Организация обеспечения безопасности персональных данных в ИСПДн предусматривает:

a) определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

b) применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

c) применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

d) оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

e) учет машинных носителей персональных данных;

f) обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;

g) восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

h) установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных;

i) обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

j) контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.2.5 Решение следующих вопросов управления обеспечением безопасности персональных данных в динамике изменения обстановки и контроля эффективности защиты является важным аспектом поддержания требуемого уровня безопасности персональных данных:

a) определение порядка действий должностных лиц, допущенных к обработке персональных данных в ИСПДн, в случае возникновения нештатных ситуаций;

b) определение порядка проведения контрольных мероприятий и действий по их результатам.

5.2.6 Контрольные мероприятия заключаются в проверке выполнения требований нормативно-правовых актов по вопросам защиты информации, а также в оценке обоснованности и эффективности принятых организационных и технических мер по защите ИСПДн. Контрольные мероприятия проводятся сотрудниками Центра информационной безопасности ИРНИТУ. Кроме того, контрольные мероприятия могут проводиться на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

5.2.7 Решение основных вопросов обеспечения защиты персональных данных предусматривает соответствующую подготовку должностных лиц, допущенных к обработке персональных данных в ИСПДн, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения.

5.2.8 Работы по обеспечению безопасности персональных данных при их обработке в ИСПДн являются неотъемлемой частью работ по созданию информационных систем.

5.3 Обмен и размещение персональных данных

5.3.1 Обмен персональными данными при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер, а также применения соответствующих технических средств.

5.3.2 Размещение ИСПДн, средств защиты информации, а также охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных, средств вычислительной техники и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.3.3 Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются в соответствии с рекомендациями ФСТЭК России и ФСБ России в пределах их полномочий.

5.4 Обработка персональных данных

5.4.1 При обработке персональных данных в ИСПДн должно быть обеспечено:

a) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

b) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

c) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

d) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

e) постоянный контроль за обеспечением уровня защищенности персональных данных.

5.4.2 Разработка организационно-технических мероприятий по обеспечению безопасности персональных данных при их обработке в ИСПДн осуществляется Центром информационной безопасности ИРНИТУ.

5.4.3 Лица, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных обязанностей, допускаются к соответствующим персональным данным на основании Перечня лиц, допущенных к обработке персональных данных в ИСПДн.

5.4.4 Исполнение предписанных организационно-технических мероприятий возлагается на должностных лиц, допущенных к обработке персональных данных в ИСПДн (пользователей ИСПДн).

5.4.5 Перечни лиц, допущенных к обработке персональных данных в ИСПДн, направляются в Центр информационной безопасности ИРНИТУ, руководителями структурных подразделений ИРНИТУ, ответственными за эксплуатацию ИСПДн. Сводный перечень лиц, допущенных к обработке персональных данных в ИСПДн в ИРНИТУ, разрабатывается Центром информационной безопасности ИРНИТУ и утверждается ректором ИРНИТУ.

5.4.6 Перечни помещений, в которых осуществляется обработка персональных данных в ИСПДн, направляются в Центр информационной безопасности руководителями структурных подразделений ИРНИТУ, ответственными за эксплуатацию ИСПДн. Сводный перечень помещений, в которых осуществляется обработка персональных данных в ИСПДн, разрабатывается Центром информационной безопасности ИРНИТУ и утверждаются ректором ИРНИТУ.

5.4.7 Необходимость использования съемных носителей информации в ИСПДн и список должностных лиц, их использующих, определяется руководителем структурного подразделения ИРНИТУ.

5.4.8 Сведения об использовании съемных носителей информации направляются в Центр информационной безопасности ИРНИТУ для их учета и внесения в соответствующую техническую документацию.

5.4.9 Постоянный контроль за выполнением должностными лицами, допущенными к обработке персональных данных в ИСПДн, требований по защите персональных данных при их обработке в ИСПДн, возлагается на их непосредственных руководителей.

5.4.10 О фактах обработки ПДн в ИСПДн, не входящих в перечень ИСПДн ИРНИТУ, руководители структурных подразделений ИРНИТУ должны сообщить в Центр информационной безопасности в течение 10 рабочих дней.

5.4.11 При планировании использования ИСПДн в деятельности структурных подразделений ИРНИТУ, процессы разработки, внедрения и ввода данных в эксплуатацию данных систем должны быть согласованы с Центром информационной безопасности.

5.4.12 В целях контроля исполнения требований настоящего Положения ИРНИТУ, используя свои, а также привлекаемые силы и средства, оставляет за собой право проверять любой или все аспекты деятельности пользователей в ИСПДн, автоматизированные рабочие места и ИСПДн, собственником которых он является.

Приложение 1 Инструкция администратора информационных систем персональных данных Иркутского национального исследовательского технического университета
(обязательное)

ИНСТРУКЦИЯ

администратора информационных систем персональных данных Иркутского национального исследовательского технического университета

1 Общие положения

1.1 Администратор информационных систем персональных данных (далее – ИСПДн) Иркутского национального исследовательского технического университета (далее – Администратор) назначается приказом ректора Иркутского национального исследовательского технического университета (далее – ИРНИТУ), в соответствии с Положением об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных ИРНИТУ из числа наиболее квалифицированных в области информационных технологий сотрудников ИРНИТУ.

1.2 Администратор в своей работе руководствуется настоящей инструкцией, Положением об организационных и технических мерах по защите персональных данных при их обработке в ИСПДн ИРНИТУ, руководящими и нормативными документами ФСТЭК России в области защиты информации, иными эксплуатационными документами ИСПДн.

1.3 Администратор отвечает за обеспечение устойчивой работоспособности элементов ИСПДн при обработке персональных данных.

2 Обязанности

Администратор обязан:

2.1 Знать и выполнять требования действующих нормативно-правовых актов по вопросам защиты информации, а также внутренних инструкций, Положения об организационных и технических мерах по защите персональных данных при их обработке в ИСПДн ИРНИТУ, руководящих и нормативных документов ФСТЭК России и ФСБ России.

2.2 Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн, в том числе аппаратного и программного обеспечения автоматизированных рабочих мест и серверов (операционные системы, прикладное и специальное программное обеспечение).

2.3 Разрабатывать и установленным порядком утверждать регламент резервного копирования баз данных ИСПДн, иную эксплуатационную документацию.

2.4 Обеспечивать работоспособность элементов ИСПДн.

2.5 Осуществлять резервное копирование баз данных ИСПДн в соответствии с утвержденным регламентом резервного копирования.

2.6 Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов информации.

2.7 Обеспечивать функционирование и поддерживать работоспособность средств защиты информации, в рамках возложенных на него функций.

2.8 В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты персональных данных, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.9 Проводить периодический контроль принятых мер по защите, в рамках возложенных на него функций.

2.10 Хранить, осуществлять прием и выдачу персональных паролей пользователей ИСПДн, осуществлять контроль за правильностью использования персонального пароля пользователем ИСПДн.

2.11 Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности персональных данных.

2.12 Информировать администратора безопасности ИСПДн о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

2.13 Требовать прекращения обработки персональных данных, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты информации.

2.14 Обеспечивать выполнение требований по обеспечению безопасности персональных данных при организации обслуживания технических средств и организации ремонтных работ. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации.

2.15 Присутствовать при выполнении технического обслуживания элементов ИСПДн сторонними физическими лицами и организациями.

2.16 Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий.

2.17 Не отключать или модифицировать средства защиты информации.

2.18 Согласовывать с администратором безопасности приобретение и установку новых или модификацию старых аппаратных и программных средств ИСПДн.

2.19 Не разглашать информацию, ставшую известной администратору ИСПДн в связи с исполнением должностных обязанностей.

Приложение 2 Инструкция администратора безопасности информационных систем персональных данных Иркутского национального исследовательского технического университета

(Обязательное)

ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных Иркутского национального исследовательского технического университета

1 Общие положения

1.1 Администратор безопасности информационных систем персональных данных (далее – ИСПДн) Иркутского национального исследовательского технического университета (далее – Администратор безопасности) назначается приказом ректора Иркутского национального исследовательского технического университета (далее – ИРНИТУ), в соответствии с Положением об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ИРНИТУ из числа наиболее квалифицированных в области информационной безопасности сотрудников ИРНИТУ.

1.2 Администратор безопасности в своей работе руководствуется настоящей инструкцией, Положением об организационных и технических мерах по защите персональных данных при их обработке в ИСПДн в ИРНИТУ, руководящими и нормативными документами ФСТЭК России и ФСБ России в области защиты персональных данных.

1.3 Администратор безопасности отвечает за поддержание необходимого уровня защищенности персональных данных при их обработке в ИСПДн ИРНИТУ.

1.4 Администратор безопасности является ответственным должностным лицом ИРНИТУ, уполномоченным на проведение работ по технической защите персональных данных и поддержание достигнутого уровня защищенности ИСПДн и ее ресурсов на этапах текущей эксплуатации и периодической модернизации.

1.5 Администратор безопасности должен иметь специальное рабочее место, расположенное так, что бы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.

1.6 Рабочее место Администратора безопасности должно быть оборудовано средствами физической защиты (личный сейф, железный шкаф или другое), подключено к ИСПДн (при необходимости), а так же средствами контроля за техническими средствами защиты информации.

1.7 Администратор безопасности осуществляет методическое руководство работой пользователей и администраторов ИСПДн, в части обеспечения безопасности персональных данных.

1.8 Требования Администратора безопасности, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями и администраторами ИСПДн.

1.9 Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защищенности ИСПДн.

2 Обязанности

Администратор безопасности обязан:

2.1 Знать и выполнять требования действующих нормативно-правовых актов по вопросам защиты информации, а также внутренних инструкций, Положения об организационных и технических мерах по защите персональных данных при их обработке в ИСПДн ИРНИТУ, руководящих и нормативных документов ФСТЭК России и ФСБ России в области защиты персональных данных.

2.2 Осуществлять установку, настройку и сопровождение технических средств защиты информации.

2.3 Участвовать в контрольных и тестовых испытаниях, проверках элементов ИСПДн.

2.4 Согласовывать приобретение и установку новых и модернизацию старых аппаратных и программных средств ИСПДн, участвовать в их приемке.

2.5 Обеспечить доступ к персональным данным пользователей ИСПДн согласно их правам доступа при получении оформленного соответствующим образом разрешения.

2.6 Уточнять в установленном порядке обязанности пользователей ИСПДн по обработке объектов защиты.

2.7 Вести контроль над процессом осуществления резервного копирования объектов защиты.

2.8 Анализировать состояние системы защиты ИСПДн и ее отдельных подсистем.

2.9 Контролировать неизменность состояния средств защиты информации, их параметров и режимов защиты.

2.10 Контролировать физическую сохранность средств и оборудования ИСПДн.

2.11 Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а так же правильность работы с элементами ИСПДн и средствами защиты информации.

2.12 Контролировать исполнение пользователями ИСПДн парольной политики.

2.13 Контролировать работу пользователей ИСПДн в сетях общего пользования и (или) международного обмена.

2.14 Своевременно анализировать журнал учета событий, регистрируемых средствами защиты информации с целью выявления возможных нарушений.

2.15 Не допускать установку, использование, хранение и размножение в ИСПДн программных средств, не связанных с выполнением функциональных задач.

2.16 Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты ИСПДн.

2.17 Оказывать помощь пользователям ИСПДн, в части применения средств защиты информации и консультировать по вопросам введенного режима защиты.

2.18 Периодически представлять непосредственному руководителю отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн, допущенных пользователями ИСПДн нарушениях установленных требований по защите информации.

2.19 В случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.20 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.21 Вести учет используемых в ИСПДн съемных носителей информации.

Приложение 3 Инструкция пользователя информационной системы персональных данных Иркутского национального исследовательского технического университета
(обязательное)

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных
Иркутского национального исследовательского технического университета

1 Общие положения

1.1 Инструкция пользователя информационных систем персональных данных Федерального государственного бюджетного образовательного учреждения высшего профессионального образования Иркутский национальный исследовательский технический университет (далее – Инструкция) определяет общие правила работы сотрудников в информационных системах персональных данных ФГБОУ ВО ИРНИТУ.

1.2 Персональные данные (ПДн) относятся к категории информации ограниченного доступа.

1.3 Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон).

1.4 Руководители структурных подразделений, ответственных за эксплуатацию ИСПДн, под роспись ознакамливают пользователей ИСПДн с настоящей Инструкцией и Положением об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО ИРНИТУ.

2 Обязанности пользователя ИСПДн

2.1 Знать и выполнять требования законодательных актов Российской Федерации, иных нормативных актов Правительства Российской Федерации, нормативно-методических документов федеральных органов исполнительной власти в области защиты персональных данных, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

2.2 Выполнять на автоматизированном рабочем месте (персональный компьютер или терминал) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3 Знать и соблюдать установленные требования по режиму обработки персональных данных, обеспечению безопасности персональных данных при их автоматизированной обработке.

2.4 Соблюдать требования парольной политики.

2.5 Соблюдать правила работы в сетях общего доступа и (или) международного обмена.

2.6 Не разглашать персональные данные, которые доверены или стали известны пользователю ИСПДн в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

2.7 Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

2.8 Немедленно ставить в известность руководителя подразделения, администратора безопасности ИСПДн:

a) при подозрении на компрометацию личных ключей и паролей;

b) при обнаружении нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа (НСД) к ресурсам ИСПДн ИРНИТУ;

c) при несанкционированных (произведенных с нарушением установленного порядка) изменениях в конфигурации программных или аппаратных средств ИСПДн;

d) при обнаружении фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

2.9 Использовать информационные ресурсы ИРНИТУ и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

2.10 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, в том числе через оконные проемы.

2.11 Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных в ИСПДн необходимо сообщать администратору безопасности ИСПДн ИРНИТУ и непосредственному руководителю.

2.12 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения необходимо обращаться к администратору ИСПДн.

2.13 Ставить в известность Администратора безопасности при:

a) необходимости обновления антивирусных баз;

b) обновлении программного обеспечения;

c) проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;

d) необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;

e) некорректном функционировании установленных средств защиты информации.

2.14 Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

2.15 Вынос средств вычислительной техники, на которых проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п., без разрешения руководителя структурного подразделения и согласования с администратором безопасности ИСПДн запрещен. При принятии решения о выносе средств вычислительной техники, носители информации должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения ИРНИТУ.

2.16 Пользователю ИСПДн запрещается:

a) разглашать защищаемую информацию третьим лицам;

b) использовать персональные данные при подготовке открытых публикаций, докладов, научных работ и т.д.;

c) оставлять не запертыми и не опечатанными после окончания работы помещения и хранилища, в которых находятся ИСПДн;

d) использовать компоненты программного и аппаратного обеспечения ИСПДн структурного подразделения ИРНИТУ в неслужебных целях;

e) самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ и средств защиты информации или устанавливать на АРМ программные и аппаратные средства без согласования с администратором безопасности ИСПДн и администратором ИСПДн;

f) осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;

g) копировать и хранить персональные данные на неучтенных носителях информации;

h) оставлять включенной без присмотра рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

i) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к утечке персональных данных;

j) подключать к автоматизированному рабочему месту личные внешние носители информации и мобильные устройства;

k) отключать (блокировать) средства защиты информации;

l) сообщать (передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

3 Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям администратором безопасности ИСПДн, администратором ИСПДн или создаются самостоятельно.

3.2 Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3 Правила формирования пароля:

a) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

b) пароль должен состоять не менее чем из 6 символов;

c) запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

d) запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

e) запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

f) запрещается выбирать пароли, которые уже использовались ранее.

3.4 Правила ввода пароля:

a) ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

b) во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5 Правила хранение пароля:

a) запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

b) запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6 Лица, использующие паролирование, обязаны:

a) четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

b) своевременно сообщать администратору безопасности ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4 Правила работы в сетях общего доступа и (или) международного обмена (Интернет)

4.1 Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2 При работе в Сети запрещается:

a) осуществлять работу при отключенных средствах защиты персональных данных (антивирус и других);

b) передавать по Сети защищаемую информацию без использования средств шифрования;

c) запрещается скачивать из Сети программное обеспечение и другие файлы;

d) запрещается посещение сайтов сомнительной репутации (сайты, содержащие нелегально распространяемое ПО и другие);

e) запрещается нецелевое использование подключения к Сети.

5 Ответственность

5.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За нарушение требований настоящей инструкции, порядка работы с документами и машинными носителями, содержащими ПДн, должностные лица могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

Приложение 4 Лист согласования положения об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «ИРНИТУ»
(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Первый проректор	Н.П. Коновалов	07.04.2015г	
Проректор по учебной и социальной работе	Б.Б. Пономарев	19.03.2015г.	
Проректор по экономическим и правовым вопросам	В.Н. Гордеев	02.04.2015	
Проректор по информационным системам и технологиям	С.Ю. Красноштанов	17.03.15	
Начальник правовой службы	А. И. Мишарина	01.04.2015	
Начальник отдела менеджмента качества	В.В. Власова	16.03.2015	

РАЗРАБОТАНО:

Директор центра информационной безопасности ИРНИТУ	П.Ю. Пушкин	16.03.2015	

Приложение 5 Лист регистрации изменений положения об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «ИРНИТУ»
(обязательное)

Порядковый номер изменения	Основание (№ приказа, дата)	Дата введения изменения	Изменения внёс	
			Фамилия, инициалы	Подпись вносившего изменения, дата внесения
1	2	3	4	5

Приложение 6 Лист ознакомления с положением об организационных и технических мерах по защите персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «ИРНИТУ»

(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись