Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

П О Л И Т И К А О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Политика информационной безопасности автоматизированных информационных систем

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНА
Приказом ректора
(чем) (должность)

от «20» июля 2021 г. № 393-О
(дата)

П О Л И Т И К А О Р Г А Н И З А Ц И И
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Политика информационной безопасности автоматизированных информационных систем

Введена впервые

1 Область применения

1.1 Настоящая политика информационной безопасности АИС ФГБОУ ВО «ИРНИТУ», разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности автоматизированных информационных систем ФГБОУ ВО «ИРНИТУ».

1.2 Настоящая политика определяет требования к персоналу АИС, степень ответственности персонала, структуру и необходимый уровень защищенности АИС, статус и обязанности работников, ответственных за обеспечение безопасности ПДн в АИС ФГБОУ ВО «ИРНИТУ».

1.3 Требования данной политики распространяются на работников ФГБОУ ВО «ИРНИТУ», эксплуатирующих технические и программные средства АИС, в которых осуществляется обработка ПДн, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования АИС ФГБОУ ВО «ИРНИТУ».

2 Нормативные ссылки

Настоящая политика разработана в соответствии и содержит ссылки на следующие нормативные документы:

Конституция Российской Федерации;

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

Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Указ Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;

Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства Российской Федерации от 21.03.2012 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 Российской Федерации от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой

без использования средств автоматизации»;

Постановление Российской Федерации от 06.07.2008 г. №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

Приказ ФСТЭК России от 11.02.2013 г. №17 «Об б утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСБ России от 10.07.2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Устав Иркутского национального исследовательского технического университета;

СТО 002-2018 Порядок управления документированной информацией (документами) СМК.

Положение о персональных данных абитуриентов и обучающихся ФГБОУ ВО «ИРНИТУ».

Положение о персональных данных работников ФГБОУ ВО «ИРНИТУ».

Положение о персональных данных читателей библиотеки ФГБОУ ВО «ИРНИТУ».

3 Термины, определения и сокращения

3.1 В настоящей политике применены следующие термины с соответствующими определениями:

Автоматизированная информационная система – информационная система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности ФГБОУ ВО «ИРНИТУ».

Аутентификация – процедура проверки подлинности пользователя.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в автоматизированных информационных системах.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Конфиденциальность персональных данных – обязательное для лица, получившего

доступ к персональным данным, требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых АИС.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь АИС – лицо, участвующее в функционировании АИС или использующее результаты ее функционирования.

Распространение персональных данных – действия, направленные 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.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Система менеджмента качества – часть системы менеджмента применительно к качеству.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Стандарт организации – 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 приказом руководства университета.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технические средства АИС – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в АИС.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в АИС или в результате которых уничтожаются материальные носители персональных данных.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Электронно-вычислительная машина – комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач.

3.2 В настоящем положении используются следующие сокращения:

АИС – автоматизированная информационная система;

АРМ – автоматизированное рабочее место;

НСД – несанкционированный доступ;

ПДн – персональные данные;

СЗПДн – система защиты персональных данных;

СМК – система менеджмента качества;

СТО – стандарт организации;

СУБД – средство управления базами данных;

ФГБОУ ВО «ИРНИТУ» – Федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет»;

ФСБ – Федеральная служба безопасности Российской Федерации;

ФСТЭК – Федеральная служба по техническому и экспортному контролю Российской Федерации;

ЭВМ – электронно-вычислительная машина.

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данную политику возложена на начальника отдела информационной безопасности и документооборота ФГБОУ ВО «ИРНИТУ».

4.2 Разработчик настоящей политики осуществляет периодическую проверку (пересмотр) данного документа в установленном порядке согласно СТО 002-2018 Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований данной политики возлагается на все должностные лица и подразделения ФГБОУ ВО «ИРНИТУ» участвующие в обработке персональных данных, а также осуществляющие сопровождение, обслуживание и обеспечение функционирования АИС ФГБОУ ВО «ИРНИТУ.

5 Общие положения

5.1 Целью настоящей Политики является обеспечение безопасности объектов защиты ФГБОУ ВО «ИРНИТУ» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также минимизация ущерба от возможной реализации угроз безопасности ПДн.

5.2 Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также путем исключения иных несанкционированных действий.

5.3 Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей.

5.4 Должно осуществляться своевременное обнаружение угроз безопасности ПДн.

5.5 Должно осуществляться предотвращение уничтожения данных или их несанкционированных модификаций.

5.6 Состав объектов защиты представлен в Перечне персональных данных и иных объектов, подлежащих защите разработанном для каждой АИС ФГБОУ ВО «ИРНИТУ».

5.7 Состав АИС подлежащих защите, представлен в Перечне АИС ФГБОУ ВО «ИРНИТУ».

6 Система защиты персональных данных

6.1 Система защиты персональных данных (СЗПДн), для каждой АИС ФГБОУ ВО «ИРНИТУ», строится на основании:

a) перечня персональных данных и иных объектов, подлежащих защите;
b) акта определения уровня защищенности персональных данных;
c) модели угроз безопасности персональных данных;
d) перечня сотрудников, допущенных к обработке персональных данных в АИС;
e) руководящих документов ФСТЭК и ФСБ России.

6.2 На основании данных документов определяется необходимый уровень защищенности ПДн каждой АИС ФГБОУ ВО «ИРНИТУ». На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению безопасности персональных данных.

6.3 Для каждой АИС должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах АИС:

a) АРМ пользователей;
b) серверы приложений;
c) СУБД;
d) граница локальной вычислительной сети;
e) каналы передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

6.4 В зависимости от уровня защищенности АИС и актуальных угроз, СЗПДн может включать следующие технические средства:

a) антивирусные средства для рабочих станций пользователей и серверов;
b) средства межсетевого экранирования;
c) средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

6.5 Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн – операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

a) управление и разграничение доступа пользователей;
b) регистрацию и учет действий с информацией;
c) обеспечение целостности данных;
d) возможность обнаружения вторжений.

6.6 Список используемых технических средств отражается в Перечне технических средств и программного обеспечения, разрабатываемого для каждой АИС ФГБОУ ВО «ИРНИТУ». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов АИС, соответствующие изменения должны быть внесены

в Список и утверждены ректором ФГБОУ ВО «ИРНИТУ» или лицом, ответственным за обеспечение защиты ПДн в ФГБОУ ВО «ИРНИТУ».

7 Требования к подсистемам СЗПДн

7.1 СЗПДн включает в себя следующие подсистемы:

7.1.1 Подсистемы управления доступом, регистрации и учета

7.1.1.1 Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

a) идентификации и проверка подлинности субъектов доступа при входе в АИС;

b) идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

c) идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

d) регистрации входа (выхода) субъектов доступа в систему (из системы);

e) регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

f) регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

7.1.1.2 Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Также может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю.

7.1.2 Подсистема обеспечения целостности и доступности

7.1.2.1 Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств АИС ФГБОУ ВО «ИРНИТУ», а также средств защиты, при случайной или намеренной модификации.

7.1.2.2 Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов АИС.

7.1.3 Подсистема антивирусной защиты

7.1.3.1 Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей АИС ФГБОУ ВО «ИРНИТУ».

7.1.3.2 Средства антивирусной защиты предназначены для реализации следующих функций:

a) резидентный антивирусный мониторинг;

b) антивирусное сканирование;

c) скрипт-блокирование;

d) централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

e) автоматизированное обновление антивирусных баз;

f) ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;

g) автоматический запуск сразу после загрузки операционной системы.

7.1.3.3 Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы АИС.

7.1.4 Подсистема анализа защищенности

7.1.4.1 Подсистема анализа защищенности предназначена для реализации функции контроля установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

7.1.4.2 Подсистема реализуется путем разработки документов, регламентирующих порядок

обновления программного обеспечения, в том числе средств защиты информации.

7.1.5 Подсистема криптографической защиты

7.1.5.1 Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в АИС ФГБОУ ВО «ИРНИТУ», при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

7.1.5.2 Подсистема реализуется при условии передачи защищаемой информации по каналам связи путем внедрения криптографических программных/программно-аппаратных комплексов.

7.2 Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности, установленного в Акте определения уровня защищенности персональных данных.

8 Классификация пользователей АИС

8.1 В Положениях о защите персональных данных определены основные категории работников ФГБОУ ВО «ИРНИТУ», имеющие доступ к персональным данным каждой АИС. На основании данных категории должна быть произведена типизация пользователей АИС, определен их уровень доступа и возможности.

8.2 В АИС ФГБОУ ВО «ИРНИТУ» можно выделить следующие основные группы ролей пользователей, участвующих в обработке и хранении ПДн:

8.2.1 Роль «Системный администратор»

8.2.1.1 Системный администратор – работник ФГБОУ ВО «ИРНИТУ», ответственный за настройку, внедрение и сопровождение системного и прикладного программного обеспечения АИС.

8.2.1.2 Системный администратор обеспечивает функционирование:

a) подсистемы управления доступом АИС. Уполномочен осуществлять предоставление и разграничение доступа пользователя АРМ к системному программному обеспечению;

b) подсистемы обеспечения целостности и доступности. Уполномочен осуществлять резервное копирование обрабатываемых персональных данных;

c) подсистемы антивирусной защиты.

8.2.1.3 Системный администратор обладает следующим уровнем доступа и знаний:

a) обладает полной информацией о системном и прикладном программном обеспечении АИС;

b) обладает полной информацией о технических средствах и конфигурации АИС;

c) имеет доступ ко всем техническим средствам обработки информации и всем персональным данным обрабатывающимся в АИС;

d) обладает правами конфигурирования и административной настройки технических средств АИС;

e) не имеет доступ к средствам защиты информации АИС.

8.2.2 Роль «Администратор информационной безопасности»

8.2.2.1 Администратор информационной безопасности – работник ФГБОУ ВО «ИРНИТУ», ответственный за функционирование СЗПДн.

8.2.2.2 Администратор информационной безопасности обеспечивает функционирование:

a) подсистемы управления доступом АИС. Уполномочен вести контроль за предоставлением и разграничением доступа пользователей АРМ к системному программному обеспечению и элементам хранящим персональные данные;

b) подсистемы обеспечения целостности и доступности. Уполномочен осуществлять резервное копирование СЗПДн и вести контроль за резервным копированием обрабатываемых персональных данных;

c) подсистемы антивирусной защиты. Уполномочен осуществлять анализ состояния подсистемы;

d) подсистемы анализа защищенности;

e) подсистемы криптографической защиты.

8.2.2.3 Администратор информационной безопасности обладает следующим уровнем доступа и знаний:

a) обладает полной информацией об АИС;

b) имеет доступ ко всем персональным данным обрабатывающимся в АИС;

c) имеет доступ к средствам защиты информации и протоколирования АИС;

d) не имеет доступ к конфигурированию технических средств АИС, за исключением контрольных (инспекционных) средств и средств, предназначенных для защиты информации.

8.2.3 Роль «Разработчик»

8.2.3.1 Разработчик – работник ФГБОУ ВО «ИРНИТУ», ответственный за настройку, внедрение и сопровождение разработанного/доработанного в ФГБОУ ВО «ИРНИТУ» прикладного программного обеспечения АИС.

8.2.3.2 Разработчик обеспечивает функционирование:

a) подсистемы управления доступом АИС. Уполномочен осуществлять предоставление и разграничение доступа пользователя АРМ к элементам, хранящим персональные данные;

b) подсистемы обеспечения целостности и доступности. Уполномочен осуществлять резервное копирование обрабатываемых персональных данных.

8.2.3.3 Разработчик обладает следующим уровнем доступа и знаний:

a) обладает полной информацией о разработанном/доработанном в ФГБОУ ВО «ИРНИТУ» прикладном программном обеспечении АИС;

b) имеет доступ ко всем персональным данным обрабатывающимся в АИС;

c) не имеет доступ к средствам защиты информации АИС;

d) не имеет доступ к конфигурированию технических средств АИС.

8.2.4 Роль «Технический специалист»

8.2.4.1 Технический специалист – работник ФГБОУ ВО «ИРНИТУ», ответственный за обеспечение работоспособности вычислительной техники АИС.

8.2.4.2 Технический специалист обеспечивает функционирование:

a) подсистемы управления доступом АИС. Уполномочен осуществлять очистку носителей персональных данных, в случае их плановой или внеплановой замены;

b) подсистемы обеспечения целостности и доступности. Уполномочен обеспечивать работоспособность вычислительной техники, а также осуществлять процедуру восстановления информации на носителях персональных данных, если это является возможным и необходимым.

8.2.4.3 Технический специалист обладает следующим уровнем доступа и знаний:

a) обладает полной информацией о системном и прикладном программном обеспечении АИС;

b) обладает полной информацией о технических средствах и конфигурации АИС;

c) имеет доступ ко всем техническим средствам обработки информации и всем персональным данным обрабатывающимся в АИС;

d) обладает правами конфигурирования и административной настройки технических средств АИС.

8.2.5 Роль «Пользователь АРМ»

8.2.5.1 Пользователь АРМ – работник ФГБОУ ВО «ИРНИТУ», осуществляющий обработку ПДн.

8.2.5.2 Пользователь АРМ не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

8.2.5.3 Пользователь АРМ обладает следующим уровнем доступа и знаний:

a) обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

b) располагает персональными данными, к которым имеет доступ.

8.3 Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Матрице разграничения доступа к ресурсам информационных систем.

8.4 Обязанности работников ФГБОУ ВО «ИРНИТУ», на которых распространяются роли пользователей АИС описаны в следующих документах, разработанных, при необходимости, для каждой АИС:

8.4.1 Инструкция системного администратора АИС;

8.4.2 Инструкция администратора информационной безопасности АИС;

8.4.3 Инструкция разработчика АИС;

8.4.4 Инструкция технического специалиста АИС;

8.4.5 Инструкция пользователя АРМ в АИС.

9 Требования к персоналу по обеспечению защиты ПДн

9.1 Все работники ФГБОУ ВО «ИРНИТУ», являющиеся пользователями АИС, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

9.2 При вступлении в должность нового работника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования АИС.

9.3 Работник должен быть ознакомлен со сведениями настоящей Политики, и принятыми процедурами работы с элементами АИС и СЗПДн.

9.4 Работники ФГБОУ ВО «ИРНИТУ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

9.5 Работники ФГБОУ ВО «ИРНИТУ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей.

9.6 Работники ФГБОУ ВО «ИРНИТУ» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

9.7 Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации к оборудованию АИС.

9.8 Работникам запрещено использовать личные технические средства (ноутбуки, смартфоны, планшеты, фотокамеры, флеш-носители, съемные жесткие диски и пр.), электронную почту, облачные хранилища и любые другие способы для копирования, фотографирования, распространения и передачи защищаемой информации.

9.9 Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ФГБОУ ВО «ИРНИТУ», третьим лицам.

9.10 При работе с ПДн в АИС работники ФГБОУ ВО «ИРНИТУ» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами, например, с мониторов АРМ.

9.11 При завершении работы с АИС работники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю.

9.12 Работники ФГБОУ ВО «ИРНИТУ» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

9.13 Работники обязаны без промедления сообщать обо всех подозрительных случаях работы АИС, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных

ими событиях, затрагивающих безопасность ПДн, руководству подразделения и администратору информационной безопасности.

10 Ответственность работников АИС ФГБОУ ВО «ИРНИТУ»

10.1 В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

10.2 Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если данные действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ).

10.3 Системный администратор и администратор информационной безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

10.4 Разработчик и пользователь АРМ несут ответственность за все действия, совершенные от имени их учетных записей, если не доказан факт несанкционированного использования учетных записей.

10.5 При нарушениях работниками ФГБОУ ВО «ИРНИТУ» правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

10.6 Сведения об ответственности работников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки должны быть отражены в Положениях о подразделениях ФГБОУ ВО «ИРНИТУ», осуществляющих обработку ПДн в АИС и должностных инструкциях работников ФГБОУ ВО «ИРНИТУ».

Приложение 1 Лист согласования Политики информационной безопасности автоматизированных информационных систем

(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по молодежной политике и работе с выпускниками	С.С. Аносов	10.06.21	
Проректор по административно-хозяйственной деятельности	И.А. Горбунов	08.06.2021	
Проректор по научной работе	А.М. Кононов	15.06.2021	
Советник ректора	Е.Г. Можаева	15.06.2021	
Проректор по международной деятельности	Д.А. Савкин	15.06.2021	
Проректор по инновационной деятельности	Е.Ю. Семёнов	08.06.21	
Проректор по учебной работе	В.В. Смирнов	28.06.21	
Советник ректора по безопасности и международным связям	С.К. Филиппов	25.06.2021 г.	
Начальник управления по работе с персоналом и обучающимися	Т.Ю. Гуруленко	18.06.2021	
Начальник управления планирования, бухгалтерского учета и аудита	Н.Б. Максимова	17.06.21 г.	
Начальник управления по дополнительному образованию и социальной работе	Б.Б. Пономарев	28.06.21 г.	
Начальник управления информатизации	В.В. Шмелев	02.6-21	
Руководитель юридической службы	О.Л. Пенизева	17.06.2021	
Заместитель начальника отдела мониторинга и качества образовательных услуг	О.С. Артемова	17.06.21	

РАЗРАБОТАНО:

Начальник отдела информационной безопасности и документооборота	Л.В. Бархатова	02.06.21	

Приложение 2 Лист регистрации изменений Политики информационной безопасности автоматизированных информационных систем

(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 3 Лист ознакомления с Политикой информационной безопасности автоматизированных информационных систем
(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись