Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

К О Н Ц Е П Ц И Я О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Концепция информационной безопасности автоматизированных информационных систем

ОРИГИНАЛ

Содержание

УТВЕРЖДЕНА
Приказом ректора
(чем) (должность)
от «20» июля 2021 г. № 393-О
(дата)

К О Н Ц Е П Ц И Я О Р Г А Н И З А Ц И И
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Концепция информационной безопасности автоматизированных информационных систем — Введена впервые

1 Область применения

1.1 Настоящая концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных АИС ФГБОУ ВО «ИРНИТУ». Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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

2 Нормативные ссылки

Настоящая концепция 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 Федеральной службы по техническому и экспортному контролю Российской Федерации от 11.02.2013 г. №17 «Об б утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ Федеральной службы по техническому и экспортному контролю Российской Федерации 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 Федеральной службы безопасности Российской Федерации 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.

3 Термины, определения и сокращения

3.1 В настоящей концепции 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.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

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.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в АИС.

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.

Перехват информации – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение АИС и (или) блокировать аппаратные средства.

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 защиты персональных данных – представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ними.

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.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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).

3.2 В настоящей концепции 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;

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

4 Ответственность

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

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

4.3 Ответственность за выполнение требований данной концепции 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 Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку СЗПДн, с позиции комплексного применения технических и организационных мер и средств защиты информации.

5.2 Под информационной безопасностью ПДн понимается защищенность ПДн и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи обеспечения информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

5.3 Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ПДн в ФГБОУ ВО «ИРНИТУ», а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

5.4 Концепция является методологической основой для:

a) формирования и проведения единой политики в области обеспечения безопасности ПДн во всех АИС ФГБОУ ВО «ИРНИТУ»;

b) принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности ПДн;

c) разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в АИС.

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

5.6 Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн в АИС. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения НСД, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

5.7 Меры защиты призваны обеспечить:

a) конфиденциальность информации (защита от несанкционированного ознакомления);

b) целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

c) доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

5.8 Стадии создания СЗПДн включают:

a) предпроектная стадия, включающая предпроектное обследование АИС;

b) стадия проектирования (разработки проектов) и реализации АИС, включающая разработку СЗПДн в составе АИС;

c) стадия ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия АИС требованиям безопасности информации.

5.9 Организационные меры предусматривают создание и поддержание правовой базы

безопасности ПДн и разработку (введение в действие) следующих организационно-распорядительных документов:

а) план мероприятий по обеспечению безопасности ПДн в АИС;

б) порядок резервирования и восстановления работоспособности технических средств и программного обеспечения защищаемой информации и средств защиты в АИС;

в) должностные инструкции для каждой категории пользователей АИС, в части обеспечения безопасности ПДн при их обработке в АИС.

5.10Технические меры защиты реализуются при помощи программно-технических средств и методов защиты.

6 Задачи системы защиты персональных данных

6.1 Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

6.2 Для достижения основной цели СЗПДн АИС должна обеспечивать эффективное решение следующих задач:

а) защиту от вмешательства в процесс функционирования АИС посторонних лиц (возможность использования АИС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

b) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АИС для выполнения своих служебных обязанностей), то есть защиту от НСД к:

- информации, циркулирующей в АИС;
- средствам вычислительной техники АИС;
- аппаратным, программным и криптографическим средствам защиты, используемым в АИС;

c) регистрацию действий пользователей при использовании защищаемых ресурсов АИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

d) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

e) защиту от несанкционированной модификации и контроль целостности используемых в АИС программных средств, а также защиту системы от внедрения несанкционированных программ;

f) защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

g) защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

h) обеспечение устойчивости криптографических средств защиты информации при компрометации части ключевой системы;

i) своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

j) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

7 Объекты защиты

7.1 Перечень информационных систем

7.1.1 В ФГБОУ ВО «ИРНИТУ» производится обработка персональных данных в автоматизированных информационных системах (АИС).

7.1.2 Перечень АИС утверждается приказом ректора ФГБОУ ВО «ИРНИТУ».

7.2 Перечень объектов защиты

7.2.1 Объектами защиты являются – информация, обрабатываемая в АИС, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных и иных объектов, подлежащих защите в АИС, утвержденном для каждой АИС ФГБОУ ВО «ИРНИТУ».

7.2.2 Объекты защиты включают:

a) обрабатываемую информацию;
b) технологическую информацию;
c) программно-технические средства обработки;
d) средства защиты ПДн;
e) каналы информационного обмена и телекоммуникации;
f) объекты и помещения, в которых размещены компоненты АИС.

8 Классификация пользователей АИС

8.1 Пользователем АИС является лицо, участвующее в функционировании АИС или использующее результаты ее функционирования. Пользователями АИС являются работники ФГБОУ ВО «ИРНИТУ», имеющими доступ к АИС и ее ресурсам в соответствии с установленным порядком и его функциональными обязанностями.

8.2 Пользователи АИС делятся на две категории:

8.2.1 Администраторы, ответственные за настройку, внедрение и сопровождение программного обеспечения, функционирование СЗПДн, обеспечение работоспособности вычислительной техники АИС.

8.2.1.1 Администраторы обладают следующим уровнем доступа и знаний:

a) обладают полной информацией об АИС;

b) имеют доступ ко всем техническим средствам обработки информации и всем персональным данным обрабатывающимся в АИС;

c) обладают правами конфигурирования и административной настройки технических средств АИС;

d) имеют доступ к средствам защиты информации и протоколирования АИС.

8.2.2 Пользователи АРМ осуществляющие обработку ПДн.

8.2.2.1 Пользователи АРМ обладают следующим уровнем доступа и знаний:

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

b) располагают конфиденциальными данными, к которым имеет доступ.

8.3 Категории пользователей должны быть определены для каждой АИС. Должно быть уточнено разделение работников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

9 Основные принципы построения системы комплексной защиты информации

9.1 Построение системы обеспечения безопасности ПДн АИС и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

9.1.1 Законность

9.1.1.1 Предполагает осуществление защитных мероприятий и разработку СЗПДн АИС в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

9.1.1.2 Пользователи и администраторы ПДн АИС должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

9.1.2 Системность

9.1.2.1 Системный подход к построению СЗПДн АИС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн АИС.

9.1.2.2 При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

9.1.3 Комплексность

9.1.3.1 Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

9.1.4 Непрерывность защиты ПДн

9.1.4.1 Защита ПДн – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АИС.

9.1.4.2 АИС должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода АИС в незащищенное состояние.

9.1.4.3 Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

9.1.5 Своевременность

9.1.5.1 Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите АИС и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки АИС в целом и ее системы защиты информации, в частности.

9.1.5.2 Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

9.1.6 Преемственность и совершенствование

9.1.6.1 Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АИС и ее системы защиты с учетом изменений в методах

и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

9.1.7 Персональная ответственность

9.1.7.1 Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

9.1.8 Принцип минимизации полномочий

9.1.8.1 Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

9.1.8.2 Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

9.1.9 Взаимодействие и сотрудничество

9.1.9.1 Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность АИС, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

9.1.9.2 В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений информационной безопасности.

9.1.10 Гибкость системы защиты ПДн

9.1.10.1 Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности изменения уровня защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

9.1.11 Открытость алгоритмов и механизмов защиты

9.1.11.1 Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления. Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

9.1.12 Простота применения средств защиты

9.1.12.1 Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей.

9.1.12.2 Должна достигаться автоматизация максимального числа действий пользователей и администраторов АИС.

9.1.13 Научная обоснованность и техническая реализуемость

9.1.13.1 Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

9.1.13.2 СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

9.1.14 Специализация и профессионализм

9.1.14.1 Предполагает привлечение к разработке средств и реализации мер защиты

информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами ФГБОУ ВО «ИРНИТУ».

9.1.15 Обязательность контроля

9.1.15.1 Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

9.1.15.2 Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

10 Меры, методы и средства обеспечения требуемого уровня защищенности

10.1 Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности АИС подразделяются на:

10.1.1 Законодательные (правовые) меры защиты

10.1.1.1 К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

10.1.1.2 Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

10.1.2 Морально-этические меры защиты

10.1.2.1 К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения электронно-вычислительных машин в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

10.1.2.2 Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

10.1.3 Организационные меры защиты

10.1.3.1 Организационные меры защиты – это меры организационного характера, регламентирующие процессы функционирования АИС, использование ресурсов АИС, деятельность пользователей и администраторов АИС, а также порядок взаимодействия пользователей с АИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

10.1.3.2 Главная цель организационных мер, предпринимаемых на высшем

управленческом уровне – сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

10.1.3.3 Реализация Политики информационной безопасности ПДн в АИС состоят из мер административного уровня и организационных (процедурных) мер защиты информации.

10.1.3.4 К административному уровню относятся решения руководства, затрагивающие деятельность АИС в целом. Эти решения закрепляются в Политике информационной безопасности. Примером таких решений могут быть:

a) принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПДн, определение ответственных за ее реализацию;

b) формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

c) принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне ФГБОУ ВО «ИРНИТУ» в целом;

d) обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

10.1.3.5 Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью АИС.

10.1.3.6 На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн. Эти правила определяют:

a) область применения Политики безопасности ПДн;

b) роли и обязанности должностных лиц, отвечающих за проведение Политики безопасности ПДн, а также ответственность данных лиц;

c) права доступа должностных лиц к ПДн;

d) меры и средства обеспечения защиты ПДн;

e) меры и средства обеспечения контроля за соблюдением введенного режима безопасности.

10.1.3.7 Организационные меры должны:

a) предусматривать регламент информационных отношений, исключающий возможность несанкционированных действий в отношении объектов защиты;

b) определять принципы и методы разграничения доступа к ПДн;

c) определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты;

d) организовать меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающие гарантии реализации прав и ответственности субъектов информационных отношений.

10.1.3.8 Организационные меры должны состоять из:

a) порядка доступа в помещения АИС;

b) инструкций для каждой категории пользователей АИС.

10.1.4 Физические меры защиты

10.1.4.1 Физические меры защиты основаны на применении разного рода механических, электро-/электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

10.1.4.2 Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или

существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой зоны технических средств разведки.

10.1.5 Технические (аппаратно-программные) меры защиты ПДн

10.1.5.1 Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав АИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

10.1.5.2 С учетом всех требований и принципов обеспечения безопасности ПДн в АИС по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

a) средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей АИС;

b) средства разграничения доступа зарегистрированных пользователей системы к ресурсам АИС;

c) средства обеспечения и контроля целостности программных и информационных ресурсов;

d) средства оперативного контроля и регистрации событий безопасности;

e) криптографические средства защиты ПДн.

10.1.5.3 Успешное применение технических средств защиты на основании принципов, перечисленных в разделе 9 данной Концепции, предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

a) обеспечена физическая целостность всех компонент АИС;

b) каждый работник (пользователь АИС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

c) все изменения конфигурации технических и программных средств АИС производятся строго установленным порядком (регистрируются и контролируются) только на основании приказов и распоряжений руководства ФГБОУ ВО «ИРНИТУ»;

d) сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

10.1.5.4 В ФГБОУ ВО «ИРНИТУ» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10.2 Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

11 Контроль эффективности системы защиты АИС

11.1 Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и реагирование на новые угрозы безопасности ПДн.

11.2 Контроль может проводиться как администраторами АИС (оперативный контроль в процессе информационного взаимодействия в АИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

11.3 Контроль может осуществляться администратором как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

11.4 Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

12 Сферы ответственности за безопасность персональных данных

12.1 Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является должностное лицо ФГБОУ ВО «ИРНИТУ» назначенное приказом ректора. Ответственный может делегировать часть полномочий по обеспечению безопасности персональных данных.

12.2 Ответственный контролирует следующие направления обеспечения безопасности ПДн:

a) планирование и реализация мер по обеспечению безопасности ПДн;

b) анализ угроз безопасности ПДн;

c) разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

d) защищенность информационной инфраструктуры ФГБОУ ВО «ИРНИТУ» от угроз информационной безопасности;

e) обучение и информирование пользователей АИС о порядке работы с ПДн и средствами защиты;

f) предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

12.3 При взаимодействии со сторонними организациями в случаях, когда работникам этих организаций предоставляется доступ к объектам защиты (раздел 7 данной Концепции), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в АИС», либо в договор заключаемый со сторонней организацией, должен быть внесен соответствующий пункт. Подготовка типовых вариантов этих соглашений осуществляется совместно с Юридической службой ФГБОУ ВО «ИРНИТУ».

13 Модель нарушителя безопасности

13.1 Нарушители подразделяются по признаку принадлежности к АИС. Все нарушители делятся на две группы:

a) внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АИС;

b) внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование АИС.

13.2 Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой АИС.

14 Модель угроз безопасности

14.1 Для АИС выделяются следующие основные категории угроз безопасности персональных данных:

a) угрозы НСД к информации;

b) угрозы уничтожения, хищения аппаратных средств АИС носителей информации

путем физического доступа к элементам АИС;

c) угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

d) угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования АИС 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;

e) угрозы преднамеренных действий внутренних нарушителей;

f) угрозы НСД по каналам связи.

14.2 Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой АИС.

15 Механизм реализации концепции

15.1 Реализация концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

a) федеральных законов в области обеспечения информационной безопасности и защиты информации;

b) постановлений Правительства Российской Федерации;

c) руководящих, организационно-распорядительных и методических документов ФСТЭК России;

d) потребностей АИС в средствах обеспечения безопасности информации.

16 Ожидаемый эффект от реализации концепции

16.1 Реализация концепции безопасности ПДн в АИС позволит:

a) оценить состояние безопасности информации АИС;

b) выявить источники внутренних и внешних угроз информационной безопасности;

c) определить приоритетные направления предотвращения, отражения и нейтрализации угроз информационной безопасности;

d) разработать распорядительные и нормативно-методические документы применительно к АИС;

e) провести классификацию и сертификацию АИС;

f) провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в АИС;

g) обеспечить необходимый уровень безопасности объектов защиты.

16.2 Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности АИС и создаст условия для ее дальнейшего совершенствования.

Приложение 1 Лист согласования концепции 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	08.06.2021г.	
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	29.06.21.	
Советник ректора по безопасности и международным связям	С.К. Филиппов	25.06.2021г.	
Начальник управления по работе с персоналом и обучающимися	Т.Ю. Гуруленко	15.06.2021	
Начальник управления планирования, бухгалтерского учета и аудита	Н.Б. Максимова	17.06.21г.	
Начальник управления по дополнительному образованию и социальной работе	Б.Б. Пономарев	28.06.21г.	
Начальник управления информатизации	В.В. Шмелев	02.06.21	
Руководитель юридической службы	О.Л. Пенизева	2.06.2021	
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 концепции 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 концепцией информационной безопасности автоматизированных информационных систем
(обязательное)

№	И.О. Фамилия	Должность	Дата	Подпись