УТВЕРЖДАЮ

Ректор ФГБОУ ВО «ИГУ»

_____ Аргучинцев А.В.

«01» марта 2016 г.

ПОЛИТИКА
информационной безопасности информационных систем персональных данных ФГБОУ ВО «ИГУ»

СОГЛАСОВАНО

Проректор по административно-хозяйственной деятельности и капитальному строительству _____ Гагаров А.А.

Директор ЦНИТ _____ Абдрахимов И.С

г. Иркутск, 2016

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Автоматизированная информационная система (АИС) –информационная система персональных данных,предназначенная для автоматизации деятельности, связанной с хранением, передачей и обработкой информации.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

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 информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом, затрагивающих права и свободы субъекта персональных данных или других лиц.

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 соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов, персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – 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.

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

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место

рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или 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.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

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

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

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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 информационной системе персональных данных.

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

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

ФГБОУ ВО «ИГУ» – федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский государственный университет».

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АРМ –автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

АИС – автоматизированная информационная система

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

НастоящаяПолитика информационной безопасности (далее – Политика) федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский государственный университет»(далее - ФГБОУ ВО «ИГУ»), разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенными в Положении о защите персональных данных ФГБОУ ВО «ИГУ».

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»,Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа 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»; на основании:

- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»(утв. ФСБ России 21.02.2008 г. № 149/6/6-662).

В Политике определены требования к персоналу информационной системы персональных данных (далее – автоматизированная информационная система (АИС)), степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в АИСФГБОУ ВО «ИГУ».

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение безопасности объектов защиты ФГБОУ ВО «ИГУ» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (далее – УБПДн).

Безопасность персональных данных 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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

Состав АИС подлежащих защите, представлен в приказах об организации информационныхсистем персональных данныхФГБОУ ВО «ИГУ».

Настоящая Политика информационной безопасности утверждается и вводится в действие приказом ректора.

2. ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех сотрудников ФГБОУ ВО «ИГУ» (штатных, временных, работающих по гражданско-правовому договоруи т.п.), посетителей официального сайта ФГБОУ ВО «ИГУ»,а также всех иныхлиц (подрядчики, аудиторы и т.п.).

3. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (СЗПДн), строится на основании:

- Отчета о проведении проверки;
- Перечня персональных данных, подлежащих защите;
- Акта установления уровня защищенности информационной системы персональных данных;
- Списка лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных обязанностей;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимыйуровень защищенности ПДнкаждойАИСФГБОУ ВО «ИГУ».На основании анализа актуальных угроз безопасности ПДн и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использованиятехнических средств и выполнения организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению безопасности персональных данных.

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

- АРМ пользователей;
- Сервера приложений;
- СУБД;
- Граница ЛВС;
- Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

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

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

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

Список используемых технических средств отражается в «Перечне технических средств и программного обеспечения в АИС. 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 ректоромФГБОУ ВО «ИГУ» или лицом, ответственным за обеспечение защиты ПДн.

4. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- контроль (анализ) защищенности персональных данных;
- межсетевого экранирования;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности АИС, определенного в Акте установления защищенности информационной системы персональных данных.

4.1 Подсистемы управления доступом, регистрации и учета

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

- идентификации и проверка подлинности субъектов доступа при входе в АИС;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам и (или) IP-адресам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

4.2 Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных

средствАИСФГБОУ ВО «ИГУ», а также средств защиты, при случайной или намеренной модификации.

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

4.3 Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей АИСФГБОУ ВО «ИГУ».

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.
- администрирование, просмотр отчетов и статистической информации по работе антивирусного продукта;

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

4.4 Подсистема анализа защищенности

Подсистема анализа защищенности предназначена для реализации следующих функций:

- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.

Подсистема реализуется путем разработки документов, регламентирующих порядок обновления программного обеспечения, в том числе средств защиты информации.

4.5 Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- идентификации и аутентификации администратора межсетевого экрана при его локальных запросах на доступ;

- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

- регистрации и учета запрашиваемых сервисов прикладного уровня;

- блокирования доступа не идентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных или программных комплексов межсетевого экранирования на границе ЛСВ и (или) на рабочих станциях.

4.6 Подсистема криптографической защиты

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

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

5. ПОЛЬЗОВАТЕЛИ АИС

В Положении о защите персональных данных определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей АИС, определен их уровень доступа и возможности.

В АИСФГБОУ ВО «ИГУ» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- АдминистраторыАИС;
- Администраторы информационной безопасности;
- Операторы.

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

5.1 Администратор АИС

Администратор АИС –работникФГБОУ ВО «ИГУ», ответственный за настройку, внедрение и сопровождение АИС. Обеспечивает функционирование подсистемы управления доступом АИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор АИС обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении АИС;
- обладает полной информацией о технических средствах и конфигурации АИС;
- имеет доступ ко всем техническим средствам обработки информации и данным АИС;
- обладает правами конфигурирования и административной настройки технических средств АИС.

5.2 Администратор безопасности

Администратор безопасности – работникФГБОУ ВО «ИГУ», ответственный за функционированиеСЗПДн, включая обслуживание и настройку административной, серверной части и контроль за обслуживанием и настройкойклиентских компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора АИС;
- обладает полной информацией об АИС;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов АИС;

- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементамиАИС;

- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с другими сетями.

5.3 Оператор АРМ

Оператор АРМ – работникФГБОУ ВО «ИГУ», осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему АИС, формирование справок и отчетов по информации, полученной из АИС. Оператор не имеет полномочий для управления подсистемами обработки данных иСЗПДн.

Оператор АИС обладает следующим уровнем доступа и знаний:

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

- располагает конфиденциальными данными, к которым имеет доступ.

6. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

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

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

Работникдолжен быть ознакомлен со сведениями настоящейПолитики, принятых процедур работы с элементамиАИС и СЗПДн.

РаботникиФГБОУ ВО «ИГУ», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а такжевозможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

РаботникиФГБОУ ВО «ИГУ» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

РаботникиФГБОУ ВО «ИГУ»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.

Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

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

При работе с ПДн в АИСработникиФГБОУ ВО «ИГУ» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с АИСработникиобязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

РаботникиФГБОУ ВО «ИГУ» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, которые нарушили принятые политику и процедуры безопасности ПДн.

Работникиобязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы АИС, способныхповлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ АИС

Должностные обязанности пользователей АИС описаны в следующих документах:

- Инструкция администратора АИС;
- Инструкция администратора безопасности АИС;
- Инструкция пользователя АИС.

8. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВФГБОУ ВО «ИГУ»

В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданско-правовую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации 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 эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

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

При нарушениях работникамиФГБОУ ВО «ИГУ» – пользователей АИС правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях ФГБОУ ВО «ИГУ», осуществляющих обработку ПДн в АИС и должностных инструкциях сотрудников ФГБОУ ВО «ИГУ».

ВПоложения о подразделениях ФГБОУ ВО «ИГУ», осуществляющих обработку ПДн в АИС, должны быть внесены сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

9. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1 Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

2 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».

3 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»;

4 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства Российской Федерациот 15.09.2008 г. № 687.

5 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в АИС.

6 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 15.02.2008 г. (ДСП).

7 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 15.02.2008 г.)