МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное
учреждение высшего профессионального образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ПРИКАЗ

19.04.2012 № 68-ОД

г. Ростов-на-Дону

Об утверждении Положения об информационной безопасности персональных данных в ЮФУ

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в Южном федеральном университете п р и к а з ы в а ю:

1. Утвердить прилагаемое Положение об информационной безопасности персональных данных федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет».

2. Руководителям структурных подразделений, осуществляющих действия по обработке персональных данных всех категорий работников и обучающихся, в своей деятельности руководствоваться прилагаемым Положением и «Положением об обработке и защите персональных данных работников и обучающихся Южного федерального университета», утвержденным приказом ЮФУ от 20.11.2009 № 150-ОД.

3. Разместить прилагаемое Положение на сайте Южного федерального университета.

4. Контроль за исполнением настоящего приказа возложить на проректора по управлению персоналом и безопасности В.П. Перетокина.

И.о. ректора В.Г. Захаревич

Приложение

УТВЕРЖДЕНО
приказом Южного федерального университета
от 19.04. 2012 г. № 68-ОД

ПОЛОЖЕНИЕ
об информационной безопасности персональных данных федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (далее – Положение) Южного федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» (далее – Университет, ЮФУ) разработано в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности информационных систем персональных данных Университета и определяет политику информационной безопасности персональных данных в ЮФУ.

1.2. Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

«Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного директором ФСТЭК от 5 февраля 2010 г. № 58;

«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», утвержденных руководством 8 Центра ФСБ России от 21 февраля 2008 г. № 149/6/6-662.

1.3. В Положении определены требования к персоналу ИСПДн, степень его ответственности, структура и необходимый уровень защищенности ИСПДн ЮФУ.

1.4. Целью настоящего Положения является обеспечение безопасности объектов защиты ЮФУ от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

1.5. 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.

1.6. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

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

1.8. Состав ИСПДн подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки.

II. ОСНОВНЫЕ ПОНЯТИЯ

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

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

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.

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.

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 (персональным данным) – возможность получения информации и ее использования.

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

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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

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.

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.

Несанкционированный доступ (несанкционированные действия) (НСД) – 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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Исходя из определения, оператором является Южный федеральный университет.

Операционная система (ОС) – комплекс управляющих и обрабатывающих программ, которые, с одной стороны, выступают как интерфейс между устройствами вычислительной системы и прикладными программами, а с другой стороны — предназначены для управления устройствами, управления вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений.

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

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

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

Программное обеспечение (ПО) – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

Система защиты персональных данных (СЗПДн) – комплекс организационных мер и средств защиты информации (в том числе шифровальных (криптографических) средств, средств предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемых в информационной системе информационных технологий.

Система управления базами данных (СУБД) – совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

Средства антивирусной защиты (антивирусные программы) - любые программы для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

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.

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.

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

Угрозы безопасности персональных данных (УБПДн) – 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.

Федеральная служба по техническому и экспортному контролю России (ФСТЭК) – федеральным органом исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам: обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в

информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям; противодействия иностранным техническим разведкам на территории Российской Федерации; обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения её утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации; защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств; осуществления экспортного контроля.

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

III. ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящего Положения распространяются на всех пользователей ИСПДн Университета.

IV. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. СЗПДн строится на основании:

отчета о результатах проведения внутренней проверки;

перечня персональных данных, подлежащих защите;

акта классификации информационной системы персональных данных;

модели угроз безопасности персональных данных;

Положения о разграничении прав доступа к обрабатываемым персональным данным;

руководящих документов ФСТЭК и ФСБ России.

4.2. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Университета. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных

мероприятий для обеспечения безопасности ПДн. Необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

4.3. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

АРМ пользователей;

сервера приложений;

СУБД;

граница ЛВС;

каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

4.4. В зависимости от уровня защищенности ИСПДн 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.

4.5. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн: 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.

4.6. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть согласованы с подразделением (специалистом) по защите информации, внесены в Список и утверждены ректором (руководителем обособленного структурного подразделения) Университета.

V. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

5.1. СЗПДн включает в себя следующие подсистемы:

управления доступом, регистрации и учета;

обеспечения целостности и доступности;

антивирусной защиты;

межсетевого экранирования;

анализа защищенности;

обнаружения вторжений;

криптографической защиты.

5.2. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определяемого Актом классификации ИСПДн в соответствии с требованиями «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК, ФСБ, Мининформсвязи РФ от 13.02.2008 г. № 55/86/20. Соответствие функций подсистем СЗПДн классу защищенности представлен в Приложении № 1.

5.1. Подсистема управления доступом, регистрации и учета

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

идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

идентификации терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;

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

контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;

регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;

регистрация выдачи печатных (графических) материалов на бумажный носитель;

регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

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

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

5.1.2. 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.

5.2. Подсистема обеспечения целостности и доступности

5.2.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ЮФУ, а так же средств защиты, при случайной или намеренной модификации.

5.2.2. Подсистема обеспечения целостности и доступности предназначена для реализации следующих функций:

резервное копирование обрабатываемых данных;

обеспечение целостности программных средств защиты персональных данных, обрабатываемой информации, а так же неизменность программной среды;

периодическое тестирование функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа;

наличие средств восстановления системы защиты персональных данных.

5.2.3. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, проверкой при загрузке системы контрольных сумм компонентов средств защиты информации, ведением двух копий программных компонент средств защиты информации и их периодическим обновлением и контролем работоспособности, а так же резервированием ключевых элементов ИСПДн.

5.3. Подсистема антивирусной защиты

5.3.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Университета.

5.3.2. Средства антивирусной защиты предназначены для реализации следующих функций:

резидентный антивирусный мониторинг;

антивирусное сканирование;

блокирование автозапуска программ (приложений);

настройка, администрирование антивирусного продукта, просмотр отчетов и статистической информации по работе продукта;

автоматизированное обновление антивирусных баз;

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

автоматический запуск сразу после загрузки операционной системы.

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

5.4. Подсистема межсетевого экранирования

5.4.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

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

фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

фильтрацию с учетом любых значимых полей сетевых пакетов;

фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

фильтрацию с учетом даты и времени;

аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;

регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

регистрацию и учет запросов на установление виртуальных соединений;

локальную сигнализацию попыток нарушения правил фильтрации;

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

регистрацию запуска программ и процессов (заданий, задач);

регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;

возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;

контроль целостности своей программной и информационной части;

контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и (или) аутентификации запросов, процесса идентификации и (или) аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

5.4.2. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

5.5. Подсистема анализа защищенности

5.5.1. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн,

которые могут быть использованы нарушителем для реализации атаки на систему.

5.5.2. Функционал подсистемы может быть реализован программными и (или) программно-аппаратными средствами анализа защищенности.

5.6. Подсистема обнаружения вторжений

5.6.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

5.6.2. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами обнаружения вторжений.

5.7. Подсистема криптографической защиты

5.7.1. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Университета, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

5.7.2. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

VI. ПОЛЬЗОВАТЕЛИ ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн Университета можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

администраторы ИСПДн;

администраторы безопасности;

пользователи АРМ ИСПДн;

администраторы сети;

технические специалисты по обслуживанию периферийного оборудования;

программисты-разработчики ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.

6.1. Администратор ИСПДн

6.1.1. Администратор ИСПДн, работник Университета, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя АРМ ИСПДн к элементам, хранящим персональные данные.

6.1.2. Администратор ИСПДн обладает следующим уровнем доступа и знаний:

обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

обладает полной информацией о технических средствах и конфигурации ИСПДн;

имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

обладает правами конфигурирования и административной настройки технических средств ИСПДн.

6.2. Администратор безопасности

6.2.1. Администратор безопасности – работник Университета, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

6.2.2. Администратор безопасности обладает следующим уровнем доступа и знаний:

обладает правами Администратора ИСПДн;

обладает полной информацией об ИСПДн;

имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

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

6.2.3. Администратор безопасности уполномочен:

реализовывать политики безопасности в части настройки программно-аппаратных средств защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь АРМ ИСПДн получает возможность работать с элементами ИСПДн;

осуществлять аудит средств защиты;

устанавливать взаимоотношения своей защищенной сети с сетями других структурных подразделений Университета (при наличии таких подключений).

6.3. Пользователь АРМ ИСПДн

6.3.1. Пользователь АРМ ИСПДн – работник Университета, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Пользователь АРМ ИСПДн не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

6.3.2. Пользователь АРМ ИСПДн обладает следующим уровнем доступа и знаний:

обладает всеми необходимыми атрибутами (например, идентификатор, ключевые элементы, пароль), обеспечивающими доступ к ПДн, обрабатываемых информационной системой, к которой подключен АРМ;

располагает конфиденциальными данными, к которым имеет доступ.

6.4. Администратор сети

6.4.1. Администратор сети, работник Университета, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

6.4.2. Администратор сети обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн;

имеет физический доступ к техническим средствам обработки информации и средствам защиты;

знает, по меньшей мере, одно легальное имя доступа.

6.5. Технический специалист по обслуживанию периферийного оборудования

6.5.1. Технический специалист по обслуживанию, работник Университета, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

6.5.2. Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

обладает частью информации о технических средствах и конфигурации ИСПДн;

знает, по меньшей мере, одно легальное имя доступа.

6.6. Программист-разработчик ИСПДн

6.6.1. Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как работники Университета, так и работники сторонних организаций.

6.6.2. Лицо этой категории:

обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

VII. ТРЕБОВАНИЯ К РАБОТНИКАМ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

7.1. Все работники Университета, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению установленных требований безопасности ПДн.

7.2. При вступлении в должность нового работника непосредственный 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 ИСПДн.

7.3. Работник должен быть ознакомлен с требованиями настоящего Положения, принятых процедур (регламентов) работы с элементами ИСПДн и СЗПДн.

7.4. Работники Университета, 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.

7.5. Работники Университета должны следовать установленным процедурам обеспечения безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

7.6. Работники Университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи ИСПДн должны знать требования по обеспечению безопасности ПДн. Пользователям ИСПДн запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них конфиденциальную информацию.

7.7. Работникам запрещается разглашать конфиденциальную информацию, которая стала им известна в ходе выполнения должностных обязанностей.

7.8. При работе с ПДн в информационных системах работники Университета обязаны обеспечить отсутствие возможности визуального просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

7.9. При завершении работы с ИСПДн пользователи обязаны блокировать доступ к защищаемым ресурсам.

7.10. Работники обязаны немедленно сообщать обо всех подозрительных случаях работы ИСПДн, а также о выявленных ими событиях, угрожающих безопасности ПДн, руководителю (ответственному за безопасность ПДн) подразделения.

VIII. Инструкции пользователей ИСПДн

Типовые инструкции пользователей ИСПДн приведены в приложениях:

типовая инструкция администратора ИСПДн - Приложение № 2;

типовая инструкция администратора безопасности ИСПДн - Приложение № 3;

типовая инструкция пользователя АРМ ИСПДн - Приложение № 4.

IX. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ УНИВЕРСИТЕТА, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПДн

9.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований законодательства РФ о персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

9.2. Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положении о подразделениях, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях работников. Для чего в Положении о подразделениях Университета, осуществляющих обработку ПДн в ИСПДн, вносятся сведения об ответственности их руководителей и работников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.