Приложение

УТВЕРЖДЕНА
приказом Южного федерального
университета
от 17.04. 2012 г. № 65-ОД

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

I. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Концепция информационной безопасности информационных систем персональных данных Южного федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» (далее – Южный федеральный университет, ЮФУ) является локальным актом, определяющим систему взглядов на обеспечение информационной безопасности ИСПДн Южного федерального университета.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Южном федеральном университете, а так же в соответствии с требованиями законодательства о персональных данных.

Настоящая Концепция определяет основные цели и задачи общей стратегии построения системы защиты персональных данных в Южном федеральном университете, а также в соответствии с требованиями законодательства о персональных данных. Концепция определяет ряд основных требований и базовый подход к их реализации, с целью достижения необходимого уровня безопасности информации.

Концепция основывается на системном подходе к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн с позиции комплексного применения технических и организационных мер и средств защиты.

Основной задачей информационной безопасности является минимизация ущерба от возможной реализации угроз безопасности ПДн, прогнозирование и предотвращение таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Южного федерального университета, а также нормативных и методических документов, сопровождающих ее реализацию. Концепция не предполагает подмены функций государственных органов власти Российской Федерации, ответственных за обеспечение безопасности информационных технологий и защиту информации.

Принципы Концепции являются основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Южного федерального университета;

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

– координации деятельности структурных подразделений Южного федерального университета при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Южного федерального университета.

Настоящая Концепция основывается на правовой базе действующих в РФ законодательных и нормативных документов по обеспечению безопасности ПДн.

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.

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

Эти организационные меры и технические средства защиты информации призваны обеспечить:

– конфиденциальность информации (защита от несанкционированного ознакомления);

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

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

Создание СЗПДн проходит стадии:

– предпроектная, включающая предпроектное обследование ИСПДн, разработку технического (частного технического) задания;

– проектирования (разработка проектов) и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн;

– ввода в действие СЗПДн, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание, поддержание в актуальном состоянии правовой базы о ПДн и разработку (введение в действие) следующих организационно-распорядительных документов:

– план мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

– план мероприятий по контролю обеспечения защиты ПДн;

– порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных и СЗПДн;

– инструкция администратора ИСПДн;

– инструкция администратора безопасности ИСПДн;

– инструкция пользователя АРМ;

– инструкция на случай возникновения внештатной ситуации;

– рекомендации по использованию программных и аппаратных средств защиты информации.

Технические меры защиты реализуются соответствующими программно-техническими средствами и методами защиты.

Перечень необходимых мер защиты информации составляется на основании результатов внутренней проверки информационных систем ПДн Южного федерального университета.

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.

Виртуальная частная сеть (VPN) - обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (Virtual Private Network).

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.

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.

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.

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 – 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.

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.

Программное обеспечение – 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.

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 – 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. ЗАДАЧИ СЗПДН

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

3.2. Для достижения основной цели системы безопасности ПДн необходимо эффективное решение следующих задач:

– защита от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования АС и доступ к ее ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

– защита от несанкционированного доступа, разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей;

– регистрация действий пользователей защищаемых ресурсов ИСПДн в системных журналах, периодический контроль корректности действий пользователей системы и анализ информации, содержащейся в этих журналах;

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

– защита от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защита системы от внедрения несанкционированных программ;

– защита ПДн от утечки по техническим каналам при их обработке;

– защиту ПДн от несанкционированного разглашения или искажения при их обработке;

– обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

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

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

IV. ОБЪЕКТЫ ЗАЩИТЫ

4.1. Перечень информационных систем

4.1.1. В Южном федеральном университете производится обработка персональных данных в информационных системах обработки персональных данных (ИСПДн).

4.1.2. Перечень информационных систем ПДн определяется на основании Отчета по результатам внутренней проверки информационных систем ПДн Южного федерального университета.

4.2 Перечень объектов защиты

4.2.1. Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты:

- обрабатываемая информация;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

4.2.2. Данные, подлежащие защите, определяет Перечень персональных данных, подлежащих защите в ИСПДн.

V. КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИСПДН

5.1. Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является сотрудник Южного федерального университета, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком и его функциональными обязанностями.

5.2. Основные категории пользователей:

- администратор ИСПДн - категория сотрудников Южного федерального университета, которые занимаются настройкой, внедрением и сопровождением информационной системы;

- программист-разработчик ИСПДн – категория сотрудников Южного федерального университета или сторонних организаций, которые занимаются разработкой программного обеспечения;

- пользователь АРМ – категория сотрудников подразделений Южного федерального университета, участвующих в процессе эксплуатации ИСПДн. Пользователь ИСПДн обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству ПДн и (или) располагает конфиденциальными данными, к которым имеет доступ.

5.3. Категории пользователей определяются для каждой ИСПДн. Следует уточнять разделение сотрудников внутри категорий по типам пользователей в соответствии с Положением об информационной безопасности персональных данных Южного федерального университета. Все определённые группы пользователей отражаются в Отчете по результатам внутренней проверки информационных систем ПДн Южного федерального университета. На основании анализа данных Отчета определяются права доступа к элементам ИСПДн каждой группой пользователей и отражаются в Разрешительной системе доступа к информационным ресурсам ИСПДн.

VI. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Построение системы обеспечения безопасности ПДн ИСПДн Южного федерального университета и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;

– системность;

– комплексность;

– непрерывность;

– своевременность;

– преемственность и непрерывность совершенствования;

– персональная ответственность;

– минимизация полномочий;

– взаимодействие и сотрудничество;

– гибкость системы защиты;

– открытость алгоритмов и механизмов защиты;

– простота применения средств защиты;

– научная обоснованность и техническая реализуемость;

– специализация и профессионализм;

– обязательность контроля.

6.1. Законность

6.1.1. Предполагает осуществление защитных мероприятий и разработку СЗПДн Южного федерального университета в соответствии с действующим законодательством в области защиты ПДн и другими нормативными правовыми актами по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

6.1.2. Пользователи и обслуживающий персонал ИСПДн Южного федерального университета должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение требований защиты ПДн.

6.2. Системность

6.2.1. Системный подход к построению СЗПДн Южного федерального университета предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн в каждой ИСПДн.

6.2.2. 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

(особенно высококвалифицированных злоумышленников), 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.

6.3. Комплексность

6.3.1. 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.

6.3.2. Защита должна быть многоуровневой. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

6.3.3. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

6.4. Непрерывность защиты

6.4.1. Защита ПДн является не разовым мероприятием и не простой совокупностью проведенных мероприятий и установленных средств защиты, а непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

6.4.2. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по предотвращению перехода ИСПДн в незащищенное состояние.

6.4.3. 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.

6.5. Своевременность

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

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

6.6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн 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.

6.7. Персональная ответственность

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

6.8. Принцип минимизации полномочий

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

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

6.9. Взаимодействие и сотрудничество

6.9.1. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Южного федерального университета, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

6.9.2. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

6.10. Гибкость системы защиты ПДн

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем 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.

6.11. Открытость алгоритмов и механизмов защиты

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 (даже авторам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

6.12. Простота применения средств защиты

6.12.1. 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, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

6.12.2. Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

6.13. Научная обоснованность и техническая реализуемость

6.13.1. 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.

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

6.14. Специализация и профессионализм

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 Южного федерального университета.

6.15. Обязательность контроля

6.15.1. 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.

6.15.2. 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.

VII. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЕННОСТИ

Обеспечение требуемого уровня защищенности должно достигаться комплексным применением мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

– правовые;

– морально-этические;

– организационные (административные);

– физические;

– технические (аппаратные и программные).

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

7.1. Правовые меры защиты

7.1.1. К правовым мерам защиты относятся законы и иные нормативные правовые акты о персональных данных, устанавливающие ответственность за нарушение законодательства о персональных данных, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

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

7.2. Морально-этические меры защиты

7.2.1. К морально-этическим мерам защиты относятся нормы поведения пользователей, традиционно сложившиеся в процессе распространения ЭВМ в стране или мировом сообществе. 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 – это свод неписаных законов, правил и предписаний таких, как честность, патриотизм и др.

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

7.3. Организационные (административные) меры защиты

7.3.1. Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

7.3.2. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – разработать документы, определяющие политику информационной безопасности ПДн Южного федерального университета (настоящая Концепция, Положение об информационной безопасности), отражающие подходы к обеспечению безопасности ПДн, и обеспечить выполнение требований этих документов, выделяя необходимые ресурсы и контролируя состояние дел.

7.3.3. Реализация требований документов, определяющих политику информационной безопасности, состоит из мер административного уровня и организационных мер обеспечения безопасности ПДн.

7.3.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Примером таких решений могут быть:

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

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

– принятие решений по вопросам реализации программы информационной безопасности, которые рассматриваются на уровне Южного федерального университета в целом;

– обеспечение нормативно - правовой базы вопросов безопасности и т.п.

7.3.5. Положение должно четко определить сферу влияния и ограничения в целях безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн.

7.3.6. На организационном уровне определяются процедуры и правила достижения целей и решения задач Положения. Эти правила определяют:

– область применения Положения;

– роль и обязанности должностных лиц, ответственных за реализацию требований Положения, а так же устанавливают их права:

– доступа к ПДн;

– выбора средств и мер обеспечения защиты ПДн;

– обеспечения контроля соблюдения требований безопасности ПДн.

7.3.7. Организационные меры должны предусматривать:

– регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определение принципов и методов разграничения доступа к ПДн;

– порядок работы с программно-математическими, техническими (аппаратные) средствами защиты, средствами криптозащиты и др.;

– организацию мер противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

7.3.8. Организационные меры должны включать:

– регламент (инструкцию) доступа в помещения ИСПДн;

– порядок допуска сотрудников к использованию ресурсов ИСПДн Южного федерального университета;

– регламент процессов ведения баз данных и осуществления модификации информационных ресурсов;

– регламент процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

– инструкции пользователей ИСПДн (администратора ИСПДн, администратора безопасности, оператора АРМ);

– инструкцию пользователя при возникновении внештатных ситуаций.

7.4. Физические меры защиты

7.4.1. Физические меры защиты основаны на применении механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий при возможных проникновениях либо доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7.4.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться установлением соответствующих постов охраны, с помощью технических средств охраны либо иными способами, предотвращающими, существенно затрудняющими проникновение в здание (помещение) посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки (видеокамер, подслушивающих устройств).

7.5. Аппаратно-программные средства защиты ПДн

7.5.1. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн 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.).

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

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

– средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Южного федерального университета;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства защиты ПДн;

– лицензированные и сертифицированные средства антивирусной защиты в составе программного обеспечения.

7.5.3. Успешное применение технических средств защиты на основании принципов построения системы комплексной защиты информации предполагает выполнение перечисленных ниже требований, обеспеченных организационными (административными) мерами и используемыми физическими средствами защиты:

– обеспечение физической целостности всех компонент ИСПДн;

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

– разработка и отладка программ для ИСПДн осуществляется на испытательных стендах, средствах вычислительной техники, не входящих в состав ИСПДн;

– все изменения конфигурации технических и программных средств ИСПДн производятся в строго установленном порядке, регистрируются и контролируются администраторами ИСПДн только на основании распоряжений руководителей Южного федерального университета и обособленных структурных подразделений Южного федерального университета;

– размещение сетевого оборудования в местах, недоступных для посторонних лиц;

– осуществление специалистами Южного федерального университета непрерывного управления и административной поддержки функционирования средств защиты.

VIII. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИСПДН ЮЖНОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА

8.1. Контроль эффективности СЗПДн должен осуществляется на основе периодических проверок. Целью контроля эффективности системы является своевременное выявление ненадлежащих режимов работы СЗПДн

(отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

8.2. Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), 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.

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

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

IX. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПДН

9.1. Ответственным за разработку мер и контроля обеспечения безопасности ПДн является проректор по управлению персоналом и безопасности Южного федерального университета, а в обособленных структурных подразделениях – их руководители. Часть полномочий по обеспечению безопасности ПДн может делегироваться специальным подразделениям (назначенным в подразделениях специалистам).

9.2. Сфера ответственности за обеспечение безопасности ПДн включает следующие направления:

– планирование и реализация мер по обеспечению безопасности ПДн;

– анализ угроз безопасности ПДн;

– разработка, внедрение, контроль, исполнение и поддержание в актуальном состоянии организационных документов (политика, руководство, концепция, процедура, регламент, инструкция и др.);

– обучение, информирование пользователей ИСПДн о порядке работы с ПДн и их средствами защиты;

– предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

9.3. В случае необходимости предоставления доступа к защищаемым объектам лицам сторонних организаций, заключается «Соглашение о конфиденциальности» либо «Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн».

X. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ

10.1. Понятие «Нарушитель» трактуется Концепцией, как лицо, в результате умышленных действий которого может быть нанесен ущерб объектам защиты.

10.2. Нарушители делятся на две группы:

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

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

10.3. Классификация типов нарушителей представляется в Модели угроз безопасности персональных данных ИСПДн каждого класса.

XI. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

11.1. Для ИСПДн Южного федерального университета выделяются следующие основные категории угроз безопасности персональных данных:

- угрозы утечки информации по техническим каналам;

- угрозы несанкционированного доступа к информации;

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

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

- угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

- угрозы преднамеренных действий внутренних нарушителей;

- угрозы несанкционированного доступа по каналам связи.

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

XII. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

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

– федеральных законов в области обеспечения информационной безопасности и защиты информации;

– нормативно-правовых актов Правительства Российской Федерации;

– руководящих, организационно-распорядительных и методических документов ФСТЭК России;

– потребностей ИСПДн в средствах обеспечения безопасности информации;

– внутренних локальных актов.

XIII. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ КОНЦЕПЦИИ

13.1. Реализация Концепции безопасности ПДн в ИСПДн позволит:

– оценить текущее состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления деятельности в сфере предотвращения, отражения и нейтрализации этих угроз;

– разработать распорядительные и нормативно-методические документы по применению ИСПДн;

– провести классификацию и сертификацию каждой ИСПДн;

– провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

– обеспечить необходимый уровень безопасности объектов защиты.

13.2. Осуществление мероприятий по защите информации обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.