Министерство здравоохранения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
дополнительного профессионального образования
РОССИЙСКАЯ МЕДИЦИНСКАЯ АКАДЕМИЯ НЕПРЕРЫВНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

ПРИКАЗ

«3» мая 2023 г. № 154

г. Москва

Об утверждении Политики информационной безопасности информационных систем персональных данных

Руководствуясь Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлениями Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 12.04.2018г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями», Приказом ФСТЭК России от 18.02.2013г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10.07.2014г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств

криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности информационных систем персональных данных Федерального государственного бюджетного образовательного учреждения дополнительного профессионального образования «Российская медицинская академия непрерывного профессионального образования» Министерства здравоохранения Российской Федерации (далее – ФГБОУ ДПО РМАНПО Минздрава России) (Приложение к настоящему приказу).

2. Начальнику отдела делопроизводства и контроля настоящий приказ довести до проректоров, руководителей структурных подразделений и директоров филиалов ФГБОУ ДПО РМАНПО Минздрава России

3. Руководителям структурных подразделений и директорам филиалов ФГБОУ ДПО РМАНПО Минздрава России довести цели Политики информационной безопасности информационных систем персональных данных ФГБОУ ДПО РМАНПО Минздрава России до работников.

Ректор Д.А. Сычев

Приложение к приказу ректора
от 3 мая 2023 г. № 154

Политика информационной безопасности информационных систем персональных данных ФГБОУ ДПО РМАНПО Минздрава России

Москва, 2023

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

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 месте 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.

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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.

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 безопасности (информации в организации) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа, а так же мероприятий по предотвращению несанкционированного доступа к персональным данным на столах, стеллажах, принтерах, экранах мониторов.

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.

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

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

Резервное копирование — процесс создания копий рабочей информации на определенный момент времени, направленный на предотвращение нарушения целостности и/или доступности рабочей информации и на ее восстановление после таких нарушений.

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 автоматизации - совокупность программных, технических и программно-технических средств, предназначенных для создания управляющих систем.

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.

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.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (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.

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

ЗСПД - защищенная сеть передачи данных

ИСПДн - информационная система персональных данных

ЛВС - локальная вычислительная сеть

КЗ - контролируемая зона

МИС МО - медицинская информационная система медицинской организации

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО - программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки

СКЗИ - средства криптографической защиты информации

САЗ - система анализа защищенности

СЗИ - средства защиты информации

СЗПДн - система (подсистема) защиты персональных данных

СОВ - система обнаружения вторжений

СУБД - система управления базами данных

ТКУИ - технические каналы утечки информации

УБПДн - угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности учреждения ФГБОУ ДПО «Российская медицинская академия непрерывного профессионального образования» Минздрава России (далее – Академия) является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Концепции информационной безопасности ИСПДн Академии.

Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», и Постановлений Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и от 12.04.2018г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями».

Политика разработана на основании нормативно-правовых документов:

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

– Приказ ФСБ России от 10.07.2014г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению

безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

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

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

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

– Постановление Правительства РФ от 15.09.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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

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

– Нормативно-методические документы Федеральной службы по техническому и экспортному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн.

– Концепция информационной безопасности информационных систем персональных данных ФГБОУ ДПО РМАНПО Минздрава России.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн Академии.

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты Академии от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, направленных на нарушение процессов сбора, обработки, хранения и предоставления информации и минимизации ущерба от возможной реализации УБПДн.

Безопасность персональных данных поддерживается на соблюдении трех основных принципах:

- конфиденциальности, когда обеспечение информации, ее хранение и просмотр доступны только уполномоченным по своим служебным обязанностям лицам. При этом исключается несанкционированный, в том числе случайный, доступ к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий,

- целостности, когда информация защищена от неправомочной модификации. Существуют множество типов информации, которые имеют ценность только тогда, когда гарантировано, что они правильные. Реализация Политики гарантирует, что информация не повреждена, не разрушена или не изменена любым способом,

- доступности, когда информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей и готовы к эксплуатации всегда, как только они потребуются. В этом случае, реализация Политики

гарантирует, что информация всегда доступна и поддерживается в пригодном состоянии. При этом должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Состав объектов защиты представлен в Перечне ПДн, подлежащих защите.

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

2. Область действия

Настоящая Политика распространяется на всех работников Академии (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчиков, аудиторов и т.п.) и обязательна для применения для всех работников Академии, осуществляющим смешанную обработку различных категорий ПДн.

3. Система защиты персональных данных

СЗПДн строится на основании:

- Отчета о результатах проведения внутренней проверки;
- Перечня ПДн, подлежащих защите в ИСПДн;
- Перечня средств вычислительной техники Академии;
- Перечня должностных лиц, имеющих право доступа к ПДн, обрабатываемым в ИСПДн;
- Акта классификации ИСПДн;
- Модели угроз безопасности ПДн;
- Нормативных документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Академии.

На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн составляется список используемых технических средств защиты, а также программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

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

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.

Так же в список включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн ОС, прикладным ПО и специальными комплексами, реализующими средства защиты. В список функций защиты может входить:

- управление и разграничение доступа пользователей;
- регистрация и учет действий с информацией;
- обеспечение целостности хранимых и обрабатываемых данных;
- обнаружение вторжений.

Список используемых технических средств (далее - Список) фиксируется в Плане мероприятий по обеспечению защиты ПДн и поддерживается в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны

быть внесены в Список и утверждены ректором Академии 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;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы должны обеспечивать выполнение следующих функций:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности ПДн;
- обеспечение целостности информационной системы и ПДн;
- обеспечение доступности ПДн;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;

- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности ПДн (далее - инциденты), и реагирование на них;

- управление конфигурацией информационной системы и системы защиты ПДн;

- криптографическая защита информации.

Подсистемы СЗПДн имеют различный функционал в зависимости от типа ИСПДн, определенного в Акте классификации ИСПДн.

4.1. Подсистема управления доступом, регистрации и учета

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

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;

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

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

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

- 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.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (ОС, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс,

осуществляющий дополнительные меры по аутентификации и контролю, предназначенный для обеспечения присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности). Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Подсистема управления доступом, регистрации и учета обеспечивает установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения и исключает возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

4.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности должна обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней ПДн, а также возможность восстановления ИСПДн и содержащихся в ней ПДн и предоставлять авторизованный доступ пользователей, имеющих права по доступу, к ПДн, содержащимся в информационной системе, в штатном режиме функционирования ИСПДн.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн и предоставления доступа пользователей после различных методов авторизации.

4.3. Подсистема антивирусной защиты

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

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, 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.

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

4.4. Подсистема межсетевого экранирования

Подсистема межсетевого экранирования позволяет регламентировать потоки сетевого трафика в рамках как внутреннего, так и внешнего информационно обмена Академии, блокируя, тем самым, действия потенциального злоумышленника, направленные на получение несанкционированного доступа к информационным ресурсам Академии, блокирование работоспособности систем или на реализацию атак на различные сетевые приложения. Подсистема межсетевого экранирования обеспечивает защиту корпоративной сети передачи данных от внешних сетевых атак, а также защиту критичных внутренних сегментов сети.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика;

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

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

- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- идентификации и аутентификацию 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;

- регистрации и учета запрашиваемых сервисов прикладного уровня;

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

- регистрации действия администратора межсетевого экрана по изменению правил фильтрации;

- 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;

- контроль за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС.

4.6. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

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

4.7. Подсистема обнаружения вторжения

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

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

4.8. Подсистема криптографической защиты

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

Подсистема реализуется путем внедрения криптографических программно-аппаратных комплексов. Нормативные требования по защите машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн, используемым в учреждении СКЗИ, а также правилам формирования ЭП, для любой формы документа, созданного электронным образом в Академии, регламентируются Приказом ФСБ России от 10.07.2014г. №378.

5. Пользователи ИСПДн

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

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

- Оператор АРМ;
- Администратор ИСПДн;
- Администратор безопасности ИСПДн;

- Администратор сети;

- Технический специалист по обслуживанию периферийного оборудования;

- Программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности отражаются в Положении о разграничении прав доступа к обрабатываемым ПДн в ИСПДн.

5.1. Администраторы ИСПДн

Администратор ИСПДн – работник Академии, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим ПДн.

Администратор ИСПДн должен обладать следующим уровнем доступа и знаний:

- полной информацией о системном и прикладном программном обеспечении ИСПДн;

- полной информацией о технических средствах и конфигурации ИСПДн;

- иметь доступ ко всем техническим средствам обработки информации и данным ИСПДн;

- обладать правами конфигурирования и административной настройки технических средств ИСПДн.

5.2. Администратор безопасности ИСПДн

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

Администратор безопасности ИСПДн должен обладать следующим уровнем доступа и знаний:

- правами Администратора ИСПДн;

- полной информацией об ИСПДн;

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

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

Администратор безопасности ИСПДн уполномочен:

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

- осуществлять аудит средств защиты.

5.3. Оператор АРМ

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

Оператор ИСПДн 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.

5.4. Администратор сети

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

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.

5.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию периферийного оборудования (далее – Технический специалист по обслуживанию) 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. К данной группе могут относиться как работники Академии, так и сотрудники сторонних организаций.

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.

5.6. Программист-разработчик ИСПДн

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

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

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

6. Требования к персоналу по обеспечению защиты ПДн

Все работники Академии, являющиеся пользователями ИСПДн, 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 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.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Работники Академии, 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.

Работники Академии должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

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

Работникам Академии запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Академии, третьим лицам.

При работе с ПДн в ИСПДн работники Академии обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

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

Работники Академии 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.

Работники Академии обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях,

затрагивающих безопасность ПДн, руководителю подразделения и администратору безопасности ИСПДн.

7. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

8. Ответственность пользователей ИСПДн Академии

При нарушениях работниками Академии - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

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

В соответствии со ст. 24 Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность, как дисциплинарную, так и административную, и уголовную:

- «Трудовой кодекс Российской Федерации» от 30.12.2001г. № 197-ФЗ - Статья 81. Расторжение трудового договора по инициативе работодателя: Трудовой договор может быть расторгнут работодателем в случаях:

в) разглашения охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения

персональных данных другого работника (в ред. Федерального закона от 30.06.2006 № 90-ФЗ);

- «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001г. № 195-ФЗ - Глава 13. Административные правонарушения в области связи и информации:

а) Статья 13.11. Нарушение законодательства Российской Федерации в области персональных данных;

6) Статья 13.12. Нарушение правил защиты информации;

в) Статья 13.14. Разглашение информации с ограниченным доступом - влечет на должностных лиц, а также и на юридических лиц наложение штрафов;

- «Уголовный кодекс Российской Федерации» от 13.06.1996г. № 63-ФЗ:

а) Статья 137. Нарушение неприкосновенности частной жизни;

6) Статья 140. Отказ в предоставлении гражданину информации;

в) Статья 272. Неправомерный доступ к компьютерной информации: наказывается штрафом, либо исправительными работами или лишением свободы в зависимости от степени тяжести нанесения данными деяниями нарушений.

В Положения о подразделениях Академии, осуществляющих обработку ПДн в ИСПДн, должны быть внесены сведения об ответственности их руководителей и работников за разглашение и несанкционированную модификацию(искажение, фальсификацию, уничтожение) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.