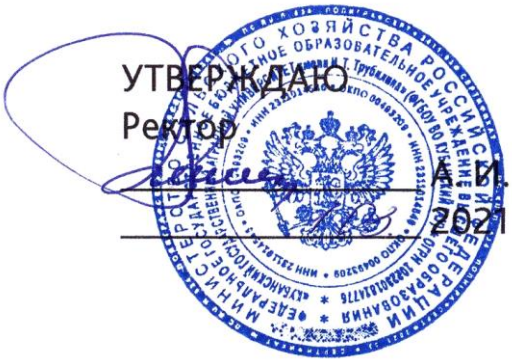
Quality Management System

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
ИМЕНИ И. Т. Трубилина»



СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Организация и обеспечение безопасности персональных данных

Положение университета

Пл КубГАУ 3.2.5 — 2021

версия 1.1

Краснодар

2021

Лист согласования

РАЗРАБОТАНО

Начальник управления кадрового обеспечения и делопроизводства — А. А. Коровин

ЭКСПЕРТИЗА ПРОВЕДЕНА

Начальник центра менеджмента качества — В. М. Смоленцев

СОГЛАСОВАНО

Первый проректор — С. М. Резниченко

Проректор по учебной работе — А. В. Петух

Проректор по научной работе — А. Г. Кощаев

Начальник центра информационных технологий — А. С. Креймер

Начальник отдела кадров — М. И. Удовицкая

Начальник юридического отдела — С. В. Новикова

Содержание

1 Назначение и область применения

Настоящее положение Федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный аграрный университет имени И. Т. Трубилина» (далее – университет) устанавливает основные требования и базовые подходы к обеспечению информационной безопасности в университете.

2 Нормативные ссылки

Настоящее положение разработано в соответствии с:

— Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

— Постановление Правительства РФ от 01.11.2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;

— Постановление Правительства РФ от 15.09.2008 г. № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

— Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

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

— Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных.

3 Термины и определения

Автоматизированная система (АС) – 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 обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

Доступ к информации – возможность получения информации и ее использования.

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

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

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

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

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

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 (КЗ) – 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 (МЭ) – 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) (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 (персональных данных) – государственный орган, муниципальный орган, 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.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

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

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

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

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

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

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

Программное (программно-математическое) воздействие (ПМВ) – 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.

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

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

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

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

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

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

Угрозы безопасности персональных данных (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 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).

4 Общие положения

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

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 технических и организационных мероприятий СЗПДн определяются исходя из уровня защищенности (класса) ИСПДн, установленного в соответствии с требованиями Постановления Правительства № 1119 от 1 ноября 2012 г., приказа ФСТЭК России № 17 от 11 февраля 2013 г., приказа ФСТЭК России № 21 от 18 февраля 2013 г., а также в соответствии с требованиями Постановления Правительства Российской Федерации № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». 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.

Система защиты персональных данных включает организационные меры и технические средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Эти меры 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).

Стадии создания системы защиты персональных данных включают:

— предпроектная стадия, включающая предпроектное обследование информационной системы персональных данных, разработку технического (частного технического) задания на ее создание;

— стадия проектирования (разработки проектов) и реализации мер защиты системы защиты персональных данных;

— стадия ввода в действие системы защиты персональных данных, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия системы защиты персональных данных требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) предусмотренных Политикой информационной безопасности информационной системы персональных данных следующих организационно-распорядительных документов:

— план мероприятий по обеспечению защиты персональных данных при их обработке в информационной системе персональных данных;

— план мероприятий по контролю обеспечения защиты персональных данных;

— порядок резервирования и восстановления работоспособности технических средства и программного обеспечения, баз данных и средств защиты информации;

— должностная инструкция администратора информационной системы персональных данных в части обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных;

— должностная инструкция администратора безопасности информационной системы персональных данных;

— должностная инструкция пользователя информационной системы персональных данных в части обеспечения безопасности персональных данных при их обработке в информационной системе персональных данных;

— инструкция на случай возникновения внештатной ситуации;

— инструкция по размещению, оборудованию и охране помещений, где хранятся персональные данные, по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации.

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

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности информационной системы персональных данных университета.

5 Задачи системы защиты персональных данных

Основной целью системы защиты персональных данных является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Для достижения основной цели система безопасности персональных данных должна обеспечивать эффективное решение следующих задач:

5.1 защиту от вмешательства в процесс функционирования информационной системы персональных данных посторонних лиц (возможность использования информационной системы персональных данных и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

5.2 разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационной системы персональных данных (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационной системы персональных данных для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

— к информации, циркулирующей в информационной системе персональных данных;

— средствам вычислительной техники информационной системы персональных данных;

— аппаратным, программным средствам защиты, используемым в информационной системе персональных данных;

— аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

5.3 регистрацию действий пользователей при использовании защищаемых ресурсов информационной системы персональных данных в системных

журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

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

5.5 защиту от несанкционированной модификации и контроль целостности используемых в информационной системе персональных данных программных средств, а также защиту системы от внедрения несанкционированных программ;

5.6 защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

5.7 защиту персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

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

5.9 своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

5.10 создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных;

5.11 оборудование и охрана помещений, где хранятся персональные данные;

5.12 соблюдение порядка хранения персональных данных на бумажных носителях;

5.13 соблюдение порядка хранения ключей от помещений, где хранятся персональные данные на бумажных носителях;

5.14 соблюдение порядка работы исполнителей с персональными данными на бумажных носителях информации.

6 Объекты защиты

В университете производится обработка персональных данных в информационной системе обработки персональных данных.

Перечень информационных систем персональных данных определяется в процессе работы комиссии, по итогам работ которой составляется акт классификации информационной системы персональных данных.

Объектами защиты являются – информация, обрабатываемая в информационной системе персональных данных, и технические средства ее обработки и защиты. Список персональных данных, подлежащих защите, определен в Перечне персональных данных, подлежащих защите в информационной системе персональных данных.

Объекты защиты включают:

— обрабатываемую информацию;

— технологическую информацию;

— программно-технические средства обработки;

— средства защиты персональных данных;

— каналы информационного обмена и телекоммуникации;

— объекты и помещения, в которых размещены компоненты информационной системы персональных данных.

7 Классификация пользователей информационной системы персональных данных

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

Пользователи информационной системы персональных данных делятся на три основные категории:

7.1 Администратор информационной безопасности.

Сотрудники университета, которые занимаются настройкой, внедрением и сопровождением систем безопасности. Администратор информационной безопасности обладает следующим уровнем доступа:

— обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;

— обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных;

— имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;

— не обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

7.2 Администратор информационной системы персональных данных.

Сотрудники университета, которые занимаются сопровождением программного обеспечения.

Администратор информационной системы персональных данных обладает следующим уровнем доступа:

— обладает информацией об алгоритмах и программах обработки информации на информационных системах персональных данных;

— обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационных систем персональных данных на стадии ее разработки, внедрения и сопровождения;

— может располагать любыми фрагментами информации о топологии информационной системы персональных данных и технических средствах обработки и защиты персональных данных, обрабатываемых в информационной системе персональных данных;

— обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

7.3 Оператор информационной системы персональных данных.

Сотрудники подразделений университета участвующие в процессе эксплуатации информационной системы персональных данных.

Оператор информационной системы персональных данных обладает следующим уровнем доступа:

— обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;

— располагает конфиденциальными данными, к которым имеет доступ.

8 Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности персональных данных университета и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

8.1 *Законность*. Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных университета в соответствии с действующим законодательством в области защиты персональных

данных и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал персональных данных информационной системы персональных данных университета должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение порядка защиты персональных данных.

8.2 *Системность*. Системный подход к построению системы защиты персональных данных предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных информационной системы персональных данных университета.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированный доступ к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

8.3 *Комплексность*. 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.

Защита должна строиться эшелонировано. 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.

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.

8.4 *Непрерывность защиты персональных данных*. Защита персональных данных – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем персональных данных.

Информационные системы персональных данных должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационной системы персональных данных в незащищенное состояние.

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.

8.5 Своевременность. Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационной системы персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационной системы персональных данных в целом и ее системы защиты информации, в частности.

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

8.6 *Преемственность и совершенствование*. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы персональных данных 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.

8.7 *Персональная ответственность*. Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии

с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

8.8 *Принцип минимизации полномочий* означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

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

8.9 *Взаимодействие и сотрудничество* предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность информационной системы персональных данных ФГБОУ ВО Кубанский ГАУ, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

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

8.10 *Гибкость системы защиты персональных данных*. 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.

8.11 *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.

8.12 *Простота применения средств защиты*. 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.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов информационной системы персональных данных.

8.13 *Научная обоснованность и техническая реализуемость*. 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 персональных данных.

Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

8.14 *Специализация и профессионализм*. Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, 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 университета.

8.15 *Обязательность контроля*. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

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.

9 Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности информационной системы персональных данных подразделяются на:

9.1 Законодательные (правовые) меры защиты.

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

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

9.2 Морально-этические меры защиты

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

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

9.3 Организационные (административные) меры защиты.

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

Главная цель административных мер – сформировать Политику информационной безопасности персональных данных (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности персональных данных в информационной системе персональных данных состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

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

— принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, определение ответственных за ее реализацию;

— формулирование целей, постановка задач, определение направлений деятельности в области безопасности персональных данных;

— принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне университета в целом;

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

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

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

— какова область применения политики безопасности персональных данных;

— каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности персональных данных, а так же установить их ответственность;

— кто имеет права доступа к персональным данным;

— какими мерами и средствами обеспечивается защита персональных данных;

— какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

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

— определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным;

— определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

— организовать меры противодействия несанкционированному доступу пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:

— регламента доступа в помещения информационной системы персональных данных;

— порядок допуска сотрудников к использованию ресурсов информационной системы персональных данных университета;

— регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

— регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационной системы персональных данных;

— инструкций пользователей информационной системой персональных данных (администратора информационной системы персональных данных, администратора безопасности, оператора информационной системы персональных данных);

— инструкция пользователя при возникновении внештатных ситуаций;

— инструкция по размещению, оборудованию и охране помещений, где хранятся персональные данные, по хранению персональных данных на бумажных носителях и порядку работы исполнителей с персональными данными на бумажных носителях информации.

9.4 Физические меры защиты.

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

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

способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

9.5 Аппаратно-программные средства защиты персональных данных.

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.).

С учетом всех требований и принципов обеспечения безопасности персональных данных в информационной системе персональных данных по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

— средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационной системы персональных данных;

— средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационной системы персональных данных университета;

— средства обеспечения и контроля целостности программных и информационных ресурсов;

— средства оперативного контроля и регистрации событий безопасности;

— криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов (раздел 8) предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

— обеспечена физическая целостность всех компонент информационной системы персональных данных;

— каждый сотрудник (пользователь информационной системы персональных данных) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

— в информационной системе персональных данных университета разработка и отладка программ осуществляется за пределами информационной системы персональных данных, на испытательных стендах;

— все изменения конфигурации технических и программных средств информационной системы персональных данных производятся строго установленным порядком (регистрируются и контролируются) только на основании приказов ректора университета;

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

— специалистами университета осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10 Контроль эффективности системы защиты персональных данных

Контроль эффективности системы защиты персональных данных должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты персональных данных (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

Контроль может проводиться как администраторами безопасности информационной системы персональных данных (оперативный контроль в процессе информационного взаимодействия в информационной системе персональных данных), 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.

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

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

11 Сферы ответственности за безопасность персональных данных

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является ректор университета. Ректор может

делегировать часть полномочий по обеспечению безопасности персональных данных руководителям структурным подразделений.

Сфера ответственности руководителей структурных подразделений включает следующие направления обеспечения безопасности персональных данных:

— планирование и реализация мер по обеспечению безопасности персональных данных;

— анализ угроз безопасности персональных данных;

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

— обучение и информирование пользователей информационной системы персональных данных, о порядке работы с персональными данными и средствами защиты;

— предотвращение, выявление, реагирование и расследование нарушений безопасности персональных данных.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты (раздел 6), с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности персональных данных при выполнении работ в информационной системе персональных данных». Подготовка типовых вариантов этих соглашений осуществляется юридическим отделом университета.

12 Модель нарушителя безопасности

Под нарушителем в университете понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Все нарушители делятся на две группы:

— внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование информационной системы персональных данных, а так же хранятся персональные данные на бумажных носителях;

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

оборудование информационной системы персональных данных, а так же хранятся персональные данные на бумажных носителях.

Классификация нарушителей представлена в Модели угроз безопасности персональных данных.

13 Модель угроз безопасности

Для информационной системы персональных данных университета выделяются следующие основные категории угроз безопасности персональных данных:

— угрозы от утечки по техническим каналам.

— угрозы несанкционированного доступа к информации.

— угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных носителей информации путем физического доступа к элементам информационной системы персональных данных.

— 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 информационной системы персональных данных и системы защиты персональных данных 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.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в «Модели угроз безопасности персональных данных в информационной системе персональных данных».

14 Механизм реализации Положения

Реализация Положения 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;

— постановлений Правительства Российской Федерации;

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

— потребностей информационной системы персональных данных в средствах обеспечения безопасности информации.

15 Порядок работы с персональными данными сотрудников

15.1 Обязанности работодателя.

В целях исполнения требований законодательства РФ при обработке персональных данных, все работники учреждения должны исполнять установленный порядок работы:

Работа с персональными данными работников должна не нарушать требований законодательства РФ и локальных нормативных актов организации, и должна быть непосредственно связана с осуществлением ими своих трудовых функций.

При сборе и обработке персональных данных работника работодатель Должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

Персональные данные работников должны быть получены только непосредственно у него. Если для обработки его данных или их получения привлекается третьи лица, то работник должен дать предварительное письменное согласие на это. Одновременно работник должен быть уведомлен о целях сбора информации, источниках ее получения, а также о последствиях отказа от предоставления письменного согласия на сбор информации.

Персональные данные работника о его политических, религиозных и иных убеждениях, частной жизни, а также членстве в общественных и профсоюзных организациях не подлежат сбору организацией, если иное не предусмотрено законодательством.

Защита персональных данных работника должна обеспечиваться полностью за счет работодателя.

Учреждение при приеме на работу, а также при любых изменениях правил работы с персональными данными обязано письменно знакомить с ними всех работников.

Учреждение не имеет право принуждать работников к отказу от своих прав на защиту персональных данных.

15.2 Обязанности работника.

Работник обязан:

— передать работодателю все персональные данные, указанные в соответствующих документах.

— сообщать работодателю в установленный правилами срок об изменении своих персональных данных.

15.3 Передача персональных данных

При осуществлении передачи персональных данных работников третьим лицам работодатель обязан:

— не сообщать персональные данные без полученного письменного согласия работника, кроме случаев, когда такие обязанности установлены законодательством;

— не передавать персональные данные работника для использования в коммерческих целях;

— требовать от третьих лиц соблюдения правил работы с персональными данными, а также предоставления письменного подтверждения использования персональных данных в порядке, предусмотренных настоящим положением о защите персональных данных;

— давать доступ к персональным данным только лицам, имеющим соответствующий допуск и использующих их только для выполнения конкретных полномочий;

— не истребовать информацию о состоянии здоровья работника, за исключением данных, которые могут повлиять на исполнение работником своих трудовых обязанностей.

15.4 Защита персональных данных работника.

В рамках реализации пунктов настоящего Положения о защите персональных данных работников, руководитель учреждения издает приказ о назначении лица, ответственного за соблюдение порядка работы с персональными данными работников, на котором лежат все обязанности по обеспечению конфиденциальности полученных данных, а также организации работы с ними.

Передача информации происходит только в письменном виде. Запрос должен быть сделан в письменном виде с указанием всех реквизитов лица, запрашивающего информацию. Ответ должен быть сделан на фирменном бланке учреждения и отправлен либо курьерской службой, либо заказным письмом.

Все полученные персональные данные должны храниться в месте, исключающем несанкционированных доступ третьих лиц.

15.5 Ответственность за разглашение информации, связанной с персональными данными работника.

Лица, признанные виновными в нарушении требований настоящего Положения о защите персональных данных работником привлекаются к дисциплинарной, административной, гражданско-правовой и уголовной ответственности, в порядке, предусмотренном законодательством РФ и локальными нормативными актами.

16 Порядок работы с персональными данными учащихся

16.1 Порядок получения и обработки персональных данных учащихся.

Под обработкой персональных данных понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных учащихся.

Работа с персональными данными учащихся должна не нарушать требований законодательства РФ и локальных нормативных актов организации.

Использование персональных данных возможно только в соответствии с целями, определившими их получение. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской федерации.

Обработка персональных данных в автоматизированных информационных системах осуществляется на основании ряда утвержденных руководителем инструкций, регламентирующих обработку персональных данных в информационной системе персональных данных.

16.2Доступ к персональным данным.

Внутренний доступ (доступ внутри организации) определяется перечнем лиц, имеющих доступ к персональным данным учащихся, определяется приказом руководителя.

Внешний доступ: к числу массовых потребителей персональных данных вне организации можно отнести государственные функциональные структуры: налоговые инспекции, правоохранительные органы, органы статистики, военкоматы, органы социального страхования, пенсионные фонды, подразделения муниципальных органов управления.

Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

16.3 Права обязанности и ответственность субъекта персональных данных.

Закрепление прав субъектов персональных данных, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

В целях защиты персональных данных контрагенты (законные представители) имеют право:

— требовать исключения или исправления неверных или неполных персональных данных, на свободный бесплатный доступ к своим персональным данным, включая право на получение копии новой записи, содержащей персональные данные;

— определять своих представителей для защиты своих персональных данных на сохранение и защиту своей личной тайны.

16.4 Права обязанности и ответственность оператора персональных данных.

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Юридические и физические лица, в соответствии со своими полномочиями владеющие о гражданах получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Руководитель, разрешающий доступ сотрудника к документу, содержащему персональные сведения учащихся, несет персональную ответственность за данное разрешение.

Каждый сотрудник организации, получающий для работы документ, содержащий персональные данные несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Допуск к персональным данным учащихся других сотрудников работодателя, не имеющих надлежащим образом оформленного доступа, запрещается.

Передача (обмен и т.д.) персональных данных между подразделениями осуществляется только между сотрудниками, имеющими доступ к персональным данным учащихся.

За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель

вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

17 Особенности обработки персональных данных без использования средств автоматизации

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

— не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;

— персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

— документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

— дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

Документы (носители информации), содержащие персональные данные, должны храниться в служебных помещениях в надежно запираем опечатываемых шкафах (сейфах).

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

— при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование пер-

сональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

— при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях должно быть раздельным.

Лист регистрации изменений

Содержание изменения	Дата и номер приказа	Дата введения изменения
Введение в действие, версия 1.0	26.09.2016 г. № 330а	26.09.2016 г.
Актуализация положения, версия 1.1	01.03.2021 г. № 88	01.03.2021 г.