УТВЕРЖДЕНО

приказом директора Лицея «Инфотех»

№31.08.1-ОД от 31.08.2022

КОНЦЕПЦИЯ
безопасности персональных данных, обрабатываемых в информационных системах персональных данных Лицея «Инфотех»

г. Йошкар-Ола
2022

Содержание

Определения

В настоящем документе используются следующие термины и их определения.

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

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

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

Доступ к информации – возможность получения информации и её использования.

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

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

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

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

Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

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 распространять их без согласия субъекта персональных данных или наличия иного законного основания.

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

Несанкционированный доступ (несанкционированные действия) – 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 – 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.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

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.

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

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

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

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

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

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

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

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

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

Субъекты персональных данных – работники, обучающиеся; граждане, заключившие договоры с компанией и другие лица.

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 персональных данных (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.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

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

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

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

Введение

Настоящая Концепция безопасности персональных данных, обрабатываемых в информационных системах персональных данных Лицея «Инфотех» (далее – Организация), является официальным документом, в котором определена система взглядов на обеспечение безопасности персональных данных в Организации.

Необходимость разработки Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных Организации (далее – Концепция) обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Организации, при обработке информации в целом и персональных данных в частности, а также необходимостью соответствия требованиям законодательства Российской Федерации в области защиты персональных данных.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных в Организации. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных Организации. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз безопасности персональных данных и разработку системы защиты персональных данных с позиции комплексного применения технических и организационных мер и средств защиты.

Под безопасностью персональных данных понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам персональных данных) или инфраструктуре. Задачи безопасности персональных данных сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению безопасности персональных данных Организации, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

формирования и проведения единой политики в области обеспечения безопасности персональных данных в информационных системах персональных данных Организации;

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

координации деятельности структурных подразделений Организации при проведении работ по развитию и эксплуатации информационных систем персональных данных с соблюдением требований обеспечения безопасности персональных данных;

разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности персональных данных в информационных системах персональных данных Организации.

Область применения Концепции распространяется на все структурные подразделения Организации, эксплуатирующие технические и программные средства информационных систем персональных данных, в которых осуществляется автоматизированная обработка персональных данных, а также на структурные подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования информационных систем персональных данных.

Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных документов по обеспечению безопасности персональных данных.

Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных Организации, в соответствии с Перечнем информационных систем персональных данных. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности персональных данных.

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.

Структура, состав и основные функции системы защиты персональных данных определяются исходя из уровня защищенности персональных данных в информационных системах персональных данных. Система защиты персональных данных 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 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 информационных систем персональных данных, включающая разработку системы защиты персональных данных в составе информационных систем персональных данных;

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

Организационные меры предусматривают создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) локальных нормативных актов в области обработки и защиты персональных данных в информационных системах персональных данных Организации.

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

Цель и 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 защиты персональных данных в информационных системах персональных данных должна обеспечивать эффективное решение следующих задач:

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

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 информационных системах персональных данных;

средствам вычислительной техники информационной системы персональных данных;

аппаратным, программным и криптографическим средствам защиты, используемым в информационных системах персональных данных;

регистрацию действий пользователей при использовании защищаемых ресурсов информационных систем персональных данных в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

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

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

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

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

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

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;

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

Перечень элементов информационных систем персональных данных, подлежащих защите

Обработка персональных данных в Организации производится в информационных системах персональных данных.

Перечень информационных систем персональных данных определяется приказом директора Организации.

Персональные данные, обрабатываемые в информационных системах персональных данных, являются сведениями конфиденциального характера и подлежат защите. Перечень персональных данных, подлежащих защите, определен в Положении об обработке персональных данных в Лицее «Инфотех».

Кроме того, в информационных системах персональных данных защите подлежат:

технологическая информация;

программно-технические средства обработки;

средства защиты персональных данных;

каналы информационного обмена и телекоммуникации;

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

Классификация пользователей информационных систем 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 работник Организации, имеющий доступ к информационной системе персональных данных и ее ресурсам в соответствии с установленным порядком доступа и служебными обязанностями.

Пользователи информационной системы персональных данных делятся на следующие категории:

1. Администратор информационной системы персональных данных – работник Организации, ответственный за настройку, внедрение и сопровождение информационной системы персональных данных. Обеспечивает функционирование подсистемы управления доступом информационной системы персональных данных и уполномочен осуществлять предоставление и разграничение доступа конечным пользователям (Операторам информационной системы персональных данных) к элементам системы, хранящим персональные данные.

Администратор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

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 к техническим средствам обработки информации и средствам защиты;

обладает возможностями внесения изменений в программное обеспечение информационной системы персональных данных на стадии ее разработки, внедрения и сопровождения;

обладает правами конфигурирования и административной настройки технических средств информационных систем персональных данных.

2. Оператор информационной системы персональных данных – работник Организации, осуществляющий обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных в информационную систему персональных данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных. Оператор информационной системы персональных данных не имеет полномочий для управления подсистемами обработки данных и системы защиты персональных данных.

Оператор информационной системы персональных данных обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству персональных данных;
- располагает конфиденциальными данными, к которым имеет доступ.

Основные принципы построения системы комплексной защиты информации

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

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

7.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных Организации 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 информационной системы персональных данных Организации должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение требований данного порядка.

7.2. Системность

Системный подход к построению системы защиты персональных данных Организации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных в информационных системах персональных данных Организации.

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, пути проникновения в распределенные системы и несанкционированного доступа 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.

7.3. Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств для построения 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.

7.4. 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 информационных систем 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.

7.5. 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.

7.6. 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 требованиях по защите, достигнутом отечественном и зарубежном опыте в этой области.

7.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко определен или сведен к минимуму.

7.8. Принцип минимизации полномочий

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

Доступ к персональным данным должен предоставляться только в тех целях и объемах, которые необходимы работнику для выполнения его должностных обязанностей.

7.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Организации, обеспечивающем деятельность информационных системах, персональных данных Организации, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие лицам, ответственным за защиту информации.

7.10. 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.

7.11. 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 её преодоления (даже разработчикам системы). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

7.12. 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 операторов и администраторов информационных системах персональных данных.

7.13. 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 персональных данных 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.

7.14. 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 Организации.

7.15. 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.

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 информационных систем персональных данных подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

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

8.1. Законодательные (правовые) меры защиты

К правовым мерам защиты относятся правила обращения с персональными данными, установленные действующими в стране нормативно-правовыми актами, которые, закрепляют права и обязанности участников информационных отношений, а также устанавливают ответственность за нарушения этих правил. Правовая база создает препятствия неправомерному использованию персональных данных и является сдерживающим фактором для потенциальных нарушителей.

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

8.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения вычислительной техники в стране. 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 коллективе Организации. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

8.3. 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, а также порядок взаимодействия пользователей с информационными системами 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, предпринимаемых на высшем управленческом уровне – сформировать Политику безопасности персональных данных, отражающую подходы к защите персональных данных, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики безопасности персональных данных в информационных системах персональных данных состоит из мер административного уровня и организационных (процедурных) мер защиты персональных данных.

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

- назначение Администратора информационной безопасности;
- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности персональных данных, назначение лиц, 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 Организации 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 ресурсы, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью информационных систем персональных данных.

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

- какова область применения политики безопасности персональных данных;
- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности персональных данных, а так же 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 порядок 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 (аппаратными) средствами защиты и криптозащиты и другими защитными механизмами;

– организовать меры противодействия несанкционированным действиям пользователей на этапах аутентификации, идентификации, обеспечивающие гарантии реализации прав и ответственности субъектов информационных отношений.

– Организационные меры должны состоять из:

– регламентации доступа в помещения, где расположены элементы информационных систем персональных данных;

– порядка допуска работников к использованию ресурсов информационных систем, персональных данных Организации;

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

– регламентации процессов обслуживания и осуществления модификации аппаратных и программных ресурсов информационных систем персональных данных;

– принятия инструкции Администратора информационной безопасности.

– принятия инструкций пользователей информационных систем персональных данных (Администратора информационной системы персональных данных, Оператора информационной системы персональных данных).

8.4. Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств, 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 системы охраны, включающую посты охраны, технические средства охраны, которая всеми способами, предотвращает или существенно затрудняет проникновение в здания, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, а также исключает нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

8.5. Аппаратно-программные средства защиты персональных данных

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем персональных данных 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 информационных системах 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;

средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности;

криптографические средства защиты персональных данных.

Успешное применение технических средств защиты на основании принципов, изложенных в разделе 5, 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 работник (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 информационных системах персональных данных Организации разработка и отладка программных средств осуществляется за пределами информационных систем персональных данных, на испытательных стендах;

– все изменения конфигурации технических и программных средств информационных систем персональных данных производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Организации;

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

– специалистами Организации осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Контроль эффективности системы защиты персональных данных

Контроль эффективности системы защиты персональных данных Организации должен осуществляться 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 также прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

Контроль может проводиться как Администратором информационной безопасности, Администраторами информационных систем персональных данных (оперативный контроль в процессе информационного взаимодействия в информационных системах 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 информационной безопасности, Администраторами информационных систем персональных данных 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 безопасности.

Сферы ответственности за безопасность персональных данных

Работники Организации, ответственные за обработку персональных данных с использованием средств автоматизации или без использования таких средств назначаются приказом директора Организации.

Сфера ответственности данных работников включает следующие направления обеспечения безопасности персональных данных:

планирование и реализация мер по обеспечению безопасности персональных данных;

анализ угроз безопасности персональных данных;

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

обучение и информирование пользователей информационных систем персональных данных о порядке работы с персональными данными и средствами защиты;

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

Модель нарушителя безопасности

Под нарушителем в Организации понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб элементам информационных систем персональных данных, подлежащим защите.

Нарушители подразделяются по признаку принадлежности к информационным системам персональных данных. Все нарушители делятся на две группы:

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

внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование информационных систем персональных данных.

Модель угроз безопасности

Для информационных систем персональных данных Организации выделяются следующие основные категории угроз безопасности персональных данных:

Угрозы от утечки по техническим каналам;

Угрозы несанкционированного доступа к информации:

Угрозы непосредственного доступа к элементам информационных систем персональных данных;

Угрозы уничтожения, хищения технических средств информационных систем персональных данных, носителей информации путем физического доступа к элементам информационных систем персональных данных;

Угрозы непреднамеренных 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 не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

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

Угрозы несанкционированного доступа по каналам связи;

Угрозы преднамеренных действий внутренних нарушителей.

Описание угроз, вероятность их реализации, опасность и актуальность представлены в Частной модели угроз безопасности персональных данных каждой информационной системы персональных данных.

Механизм реализации Концепции

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

федеральных законов в области обеспечения информационной безопасности и защиты информации;

постановлений Правительства Российской Федерации;

руководящих, организационно-распорядительных и методических документов ФСБ России, ФСТЭК России, Роскомнадзора;

потребностей информационной системы персональных данных в средствах обеспечения безопасности информации.

Ожидаемый эффект от реализации Концепции

Реализация Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных Организации позволит:

оценить состояние безопасности персональных данных, выявить источники внутренних и внешних угроз безопасности персональных данных, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

разработать распорядительные и нормативно-методические документы применительно к информационным системам персональных данных;

провести определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных;

провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в информационных системах персональных данных;

обеспечить необходимый уровень безопасности элементов информационных систем персональных данных, подлежащих защите.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы защиты персональных данных и создаст условия для ее дальнейшего совершенствования.

Список использованных источников

1. Конституция Российской Федерации;
2. Конституция Республики Марий Эл;
3. Трудовой кодекс Российской Федерации;
4. Семейный кодекс Российской Федерации;
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
6. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
8. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.;
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 14 февраля 2008 г.