Приложение 1
к Приказу «О проведении работ по защите
персональных данных» от 01.12.2011 г. №75/4

УТВЕРЖДАЮ

Директор ФБУ «Мордовский ЦСМ»

_____ С.И. Мунтантилов
«01»_____12_____2011г.

ПОЛОЖЕНИЕ
по защите персональных данных
Федерального бюджетного учреждения «Государственный региональный центр стандартизации, метрологии и испытаний в Республике Мордовия»

2011 г.

СОДЕРЖАНИЕ

	Термины и определения…….	3
	Перечень сокращений……	7
1.	Общие положения……...	8
2.	Объекты защиты……..	9
3.	Основные принципы построения системы защиты……	10
4.	Способы обеспечения безопасности…….	13

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

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.

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

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

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

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и

технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов,

сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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.

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

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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 – 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 – 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.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АВПО – антивирусное программное обеспечение

АРМ – автоматизированное рабочее место

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

УБПДн – угрозы безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Федерального бюджетного учреждения «Государственный региональный центр стандартизации, метрологии и испытаний в Республике Мордовия». Положение определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

СЗПДн представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, 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 СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Эти 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).

2. ОБЪЕКТЫ ЗАЩИТЫ

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

Федеральное бюджетное учреждение «Государственный региональный центр стандартизации, метрологии и испытаний в Республике Мордовия» является оператором персональных данных сотрудников и клиентов.

Объектами защиты являются:

- обрабатываемые персональные данные сотрудников;
- обрабатываемые персональные данные клиентов;
- технологическая информация;
- схема технологических процессов обработки;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

3. Основные способы построения системы защиты

Построение системы обеспечения безопасности ПДн ИСПДн Федерального бюджетного учреждения «Государственный региональный центр стандартизации, метрологии и испытаний в Республике Мордовия» и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

Законность:

Предполагает осуществление защитных мероприятий и разработку СЗПДн в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ПДн ИСПДн должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

Системность:

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

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей.

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.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

Непрерывность защиты ПДн:

Защита ПДн – 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 ИСПДн.

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

Своевременность:

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

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.

Персональная ответственность:

Предполагает возложение ответственности за обеспечение безопасности ПДн 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.

Принцип минимизации полномочий:

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

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

Взаимодействие и сотрудничество:

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

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности по защите информации.

Гибкость системы защиты ПДн:

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

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 ИСПДн.

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 и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

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

Специализация и профессионализм:

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

Обязательность контроля:

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации.

4. Способы обеспечения безопасности

Система защиты персональных данных должна обеспечивать всестороннюю комплексную защиту.

Законодательные (правовые) меры защиты:

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, 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 ПДн 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.

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, чувство коллективизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний (например, в форме стандартов корпоративной этики).

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.

Организационные (административные) меры защиты:

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

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 ПДн;

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

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

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.

Аппаратно-программные средства защиты ПДн

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 ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства межсетевого экранирования для защиты ИСПДн от нарушителей из внешних сетей;

– антивирусные средства;

– криптографические средства защиты ПДн.