УТВЕРЖДАЮ

Директор государственного автономного

учреждения Саратовской области «Центр адаптации и реабилитации инвалидов»

_____ Е.С.Пяткина

Термины и определения.

В настоящем документе используются следующие термины и их определения:

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

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

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

строения тела и другую подобную информацию.

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

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

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

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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

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

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

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не

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

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

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

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

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

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

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик

физических величин.

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

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

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

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (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 – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

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 – 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 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.

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

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

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

Обозначения и сокращения

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИБ – информационная безопасность

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПД – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СЗПД – система (подсистема) защиты персональных данных

СКЗИ – система криптографической защиты информации

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПД – угрозы безопасности персональных данных

Введение

Настоящая Политика информационной безопасности персональных данных (далее – Политика) государственного автономного учреждения Саратовской области «Центр адаптации и реабилитации инвалидов» (далее Учреждения) является официальным документом, в котором определена система обеспечения информационной безопасности.

Настоящая Политика определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПД) в Учреждении. Политика

определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации. Также определены требования к сотрудникам, являющимися пользователями информационных систем персональных данных (ИСПД), степень их ответственности, должностные обязанности сотрудников, ответственных за организацию обработки персональных данных (ПД) в ИСПД.

Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПД, с позиции комплексного применения технических и организационных мер и средств защиты.

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

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности ИСПД, а также организационных и распорядительных документов, обеспечивающих ее реализацию.

Политика является основой для:

- · принятия управленческих решений и разработки практических мер по реализации политики и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПД;
- · координации деятельности органов исполнительной власти при проведении работ по развитию и эксплуатации ИСПД с соблюдением требований обеспечения безопасности ПД;
- · разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПД в ИСПД.

Основными нормативными правовыми и методическими документами, на которых базируется настоящая Политика являются:

- · Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
- · Требования к защите персональных данных при их обработке в информационных системах персональных данных (утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119);
- · Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17;
- · «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

Общие положения

Целью настоящей Политики является обеспечение безопасности ИСПД Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПД (УБПД).

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 иные несанкционированные действия.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение, реагирование на УБПД, предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Область действия

Требования и выполнение положений настоящей Политики распространяются на всех сотрудников Учреждения, являющихся пользователями ИСПД.

Основные принципы обеспечения информационной безопасности

Определенность целей. Функциональные цели и цели информационной безопасности ИСПД должны быть явно определены во внутренних документах Учреждения. Неопределенность приводит к “расплывчатости” невозможности оценки адекватности принятых защитных мер.

Своевременность обнаружения проблем. Необходимо своевременно обнаруживать проблемы, потенциально способные повлиять на функциональные цели и цели информационной безопасности ИСПД.

Прогнозируемость развития проблем. Необходимо выявлять причинно-следственную связь возможных проблем и строить на этой основе точный прогноз их развития.

Оценка влияния проблем на функциональные цели. Необходимо адекватно оценивать степень влияния выявленных проблем на функциональные цели ИСПД.

Адекватность защитных мер. Необходимо выбирать защитные меры, адекватные моделям угроз и нарушителей, с учетом затрат на реализацию таких мер и объема возможных потерь от выполнения угроз.

Эффективность защитных мер. Необходимо эффективно реализовывать принятые защитные меры.

Использование опыта при принятии и реализации решений. Необходимо накапливать, обобщать и использовать как свой опыт, так и опыт других организаций на всех уровнях принятия решений и их исполнения.

Контролируемость защитных мер. Необходимо применять только те защитные меры, правильность работы которых может быть проверена, при этом необходимо регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на функциональные цели и цели информационной безопасности ИСПД.

Система защиты персональных данных

Система защиты персональных данных (СЗПД), строится на основании:

- Актов классификации информационных систем персональных данных;
- Моделей угроз безопасности персональных данных;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПД в ИСПД. На основании анализа актуальных угроз безопасности ПД описанного в Моделях угроз безопасности персональных данных делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПД.

Для ИСПД должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПД на всех элементах ИСПД:

- АРМ пользователей;

- Серверах межведомственного взаимодействия;

- Границе ЛВС;

- Каналах передачи в сети общего пользования и (или) международного обмена по которым передаются ПД.

Требования к подсистемам СЗПД

СЗПД включает в себя следующие подсистемы:

- подсистема межсетевого взаимодействия;
- подсистема антивирусной защиты;
- подсистема обнаружения вторжений;
- подсистема анализа защищенности;
- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема криптографической защиты;
- подсистема резервного копирования;
- организационные меры.

Подсистема межсетевого взаимодействия

Подсистема межведомственного взаимодействия предназначена для реализации следующих функций:

- регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения

межсетевого экрана);

- идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- контроль целостности программной и информационной части межсетевого экрана;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления;
- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
- регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
- регистрация запуска программ и процессов (заданий, задач);
- межсетевое экранирование должно обеспечивать регламентное тестирование процесса регистрации;
- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
- фильтрация с учетом любых значимых полей сетевых пакетов.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПД.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную (удаленную) установку (деинсталляцию)
- антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;

- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы.

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

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление

сетевых атак на элементы ИСПД подключенные к сетям общего пользования и (или) международного обмена.

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

Подсистема анализа защищенности

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

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

Подсистема управления доступом

Подсистема управления доступом, предназначена для реализации следующих функций:

- идентификация и проверка подлинности пользователя при входе в систему ИСПД по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- при идентификации и проверке подлинности пользователя при входе в систему должен дополнительно использоваться идентификатор (код).

Подсистема регистрации и учета

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

- регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается результат попытки входа (успешная или неуспешная);
- при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);
- **при регистрации входа (выхода) пользователя в систему (из системы) либо регистрации загрузки и инициализации операционной системы и ее программного останова в параметрах регистрации дополнительно указывается результат попытки входа (успешная или неуспешная).**

Подсистема обеспечения целостности

Подсистема обеспечения целостности предназначена для реализации следующих функций:

- периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности;
- обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации.

Подсистема криптографической защиты

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

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

Подсистема резервного копирования

В ИСПД должно быть предусмотрено средство резервного копирования персональных данных, для последующего их восстановления в случае модификации или уничтожения

в результате несанкционированного доступа.

Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПД можно подразделяются на:

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

Законодательные (правовые) меры защиты

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

Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПД, использование ресурсов ИСПД, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПД 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 основные подходы к защите информации и обеспечить их выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация подходов к защите ПД в ИСПД состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

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

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ПД, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПД;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются Учреждением;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

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

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

- какова область применения политики безопасности ПД;
- каковы роли, обязанности и ответственность должностных лиц, отвечающих за проведение политики безопасности ПД;
- кто имеет права доступа к ПД;
- какие меры и средства защиты использовать;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры

- учит лиц, допущенных к работе с персональными данными в ИСПД; лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.
- для выбора и реализации методов и способов защиты информации в ИСПД требуется назначить в Учреждении структурные подразделения или должностные лица (работника), ответственные за обеспечение безопасности персональных данных
- обучение лиц, использующих средства защиты информации, применяемые в ИСПД, правилам работы с ними
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации,

которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений

- размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные

- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПД;
- регламента доступа в помещения с компонентами ИСПД;
- инструкций пользователей ИСПД (администратора информационной безопасности)

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.

Аппаратно-программные средства защиты ПД

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

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

- обеспечена физическая целостность всех компонент ИСПД;
- каждый сотрудник (пользователь ИСПД) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств ИСПД производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Управления делами Правительства Саратовской области;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).
- администратором информационной безопасности совместно с ответственным за обеспечение безопасности персональных данных осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Контроль эффективности системы защиты ИСПД

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

Контроль может проводиться как администратором информационной безопасности (оперативный контроль в процессе информационного взаимодействия в ИСПД), 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 как с помощью штатных средств системы защиты ПД, так и с помощью специальных программных средств контроля.

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

Пользователи ИСПД

В ИСПД можно выделить следующие группы пользователей, участвующих в обработке ПД:

- Администратора информационной безопасности (ИБ);

- Оператора АРМ;

Администратор ИБ - сотрудник, ответственный за настройку, внедрение и сопровождение ИСПД, функционирование СЗПД. Обеспечивает функционирование подсистемы управления доступом ИСПД и уполномочен осуществлять предоставление конечного пользователя (Оператора АРМ) к элементам хранящим персональные данные.

Администратор ИБ обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПД;
- обладает полной информацией о технических средствах и конфигурации ИСПД;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПД;
- обладает правами конфигурирования и административной настройки технических средств ИСПД;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПД;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных);
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- Администратор безопасности уполномочен:
- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПД;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других учреждений.

Оператор АРМ - пользователь, осуществляющий обработку ПД в ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПД.

Оператор СМЭВ обладает следующим уровнем доступа и знаний:

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

Требования к персоналу по обеспечению защиты ПД

Все пользователи ИСПД, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемому объекту и соблюдению принятого

режима безопасности ПД.

При вступлении в должность нового сотрудника, являющегося пользователем ИСПД, непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПД, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПД.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПД и СЗПД.

Пользователи ИСПД, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Пользователи ИСПД должны следовать установленным процедурам поддержания режима безопасности ПД при выборе и использовании паролей (если не используются технические средства аутентификации).

Пользователи ИСПД должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПД и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Пользователям запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Пользователям запрещается разглашать защищаемую информацию, которая стала им известна при работе с ИСПД, третьим лицам.

При работе с ПД в ИСПД пользователи обязаны обеспечить отсутствие возможности просмотра ПД третьими лицами с мониторов АРМ.

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

Сотрудники, использующие ИСПД, должны быть проинформированы об угрозах нарушения режима безопасности ПД и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПД.

Пользователи ИСПД обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы системы, могущих повлечь за собой угрозы безопасности ПД, а также о выявленных ими событиях, затрагивающих безопасность ПД, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПД.

Должностные обязанности пользователей ИСПД

Должностные обязанности пользователей ИСПД описаны в следующих документах:

- Инструкция администратора информационной безопасности;

- Инструкция пользователя региональной системы межведомственного электронного взаимодействия;

- Инструкция по действиям персонала в нештатных ситуациях.

Ответственность пользователей ИСПД

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

1. Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных настоящим Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с настоящим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор информационной безопасности несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Учреждения – пользователей ИСПД правил, связанных с безопасностью ПД, они несут ответственность, установленную действующим законодательством Российской Федерации.