УТВЕРЖДАЮ

Президент Тульской областной нотариальной палаты

_____п/п_____ В.В. Дудкин

«_16_» _____05_____ 2019 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
в информационных системах персональных данных Тульской областной нотариальной палаты

Содержание

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения:

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

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.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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

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

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

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

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение,

конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

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

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

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

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

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

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.

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 становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

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

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.

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.

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

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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

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

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МН ПДн – машинные носители персональных данных

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СиЗИ ИСПДн – система (подсистема) защиты информации в информационной системе персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

В настоящей Политике информационной безопасности (далее – Политика) определены требования к пользователям информационных систем персональных данных (далее – ИСПДн), степень ответственности пользователей ИСПДн, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в ИСПДн Тульской областной нотариальной палаты (далее – Палата).

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн Палаты от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите. Состав ИСПДн, подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки.

2. Область действия

Субъектами настоящей Политики информационной безопасности являются все лица, вовлеченные в организационные и технологические (бизнес) процессы сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), обезличивания, блокирования, удаления уничтожения персональных данных, обрабатываемых в ИСПДн Палаты.

3. Система защиты персональных данных

Система защиты персональных данных (СиЗИ ИСПДн) строится на основании:

- Отчета о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- Частных моделей угроз безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным;

- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн нотариальной палаты. На основании анализа актуальных угроз безопасности ПДн, описанных в Модели угроз и Отчете о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн на всех элементах ИСПДн. В зависимости от уровня защищенности ИСПДн программно-технические средства СиЗИ ПДн должны обеспечивать реализацию следующих мер:

- ✓ идентификацию и аутентификацию субъектов доступа и объектов доступа;
- ✓ управление доступом субъектов доступа к объектам доступа;
- ✓ ограничение программной среды;
- ✓ защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- ✓ регистрацию событий безопасности;
- ✓ антивирусную защиту;
- ✓ обнаружение (предотвращение) вторжений;
- ✓ контроль (анализ) защищенности персональных данных;
- ✓ обеспечение целостности информационной системы и персональных данных;
- ✓ обеспечение доступности персональных данных;
- ✓ защиту среды виртуализации;
- ✓ защиту технических средств;
- ✓ защиту информационной системы, ее средств, систем связи и передачи данных;
- ✓ выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- ✓ управление конфигурацией информационной системы и системы защиты ПДн.

Перечень используемых программно-технических средств защиты ПДн отражается в технических паспортах на ИСПДн. Перечень используемых программно-технических средств защиты ПДн должен поддерживаться в актуальном состоянии.

4. Требования к подсистемам СиЗИ ИСПДн

СиЗИ ИСПДн может включать в себя следующие подсистемы:

1. Подсистема управления доступом;
2. Подсистема регистрации и учета;
3. Подсистема обеспечения целостности;
4. Подсистема антивирусной защиты;
5. Подсистема межсетевого экранирования;
6. Подсистема аудита безопасности;
7. Подсистема обнаружения вторжений;
8. Подсистема криптографической защиты;
9. Подсистема управления процессами обеспечения безопасности;
10. Подсистема обеспечения доступности ПДн.

4.1. Подсистема управления доступом

Назначение:

Подсистема управления доступом предназначена для реализации следующих мер по обеспечению безопасности ПДн:

- ✓ идентификация и аутентификация субъектов доступа и объектов доступа;
- ✓ управление доступом субъектов доступа к объектам доступа;
- ✓ ограничение программной среды;
- ✓ защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее – МН ПДн);
- ✓ защита технических средств.

Требования к подсистеме:

В соответствии с [9] для подсистемы управления доступом установлены следующие требования:

1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности);
2. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил;
3. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения

или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения;

4. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.
5. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Содержание мер по управлению доступом:

В соответствии с [9] и уровнем защищенности ПДн, функции подсистемы управления доступом обеспечиваются реализацией следующих мер:

Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):

- ✓ Идентификация и аутентификация пользователей, являющихся работниками оператора
- ✓ Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- ✓ Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
- ✓ Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
- ✓ Защита обратной связи при вводе аутентификационной информации
- ✓ Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

Управление доступом субъектов доступа к объектам доступа (УПД):

- ✓ Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

- ✓ Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
- ✓ Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
- ✓ Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
- ✓ Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
- ✓ Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
- ✓ Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных
- ✓ Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему
- ✓ Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
- ✓ Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
- ✓ Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
- ✓ Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки
- ✓ Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
- ✓ Регламентация и контроль использования в информационной системе технологий беспроводного доступа

- ✓ Регламентация и контроль использования в информационной системе мобильных технических средств
- ✓ Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
- ✓ Обеспечение доверенной загрузки средств вычислительной техники

Ограничение программной среды (ОПС)

- ✓ Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
- ✓ Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
- ✓ Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов
- ✓ Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов

Защита машинных носителей персональных данных (ЗНИ)

- ✓ Учет машинных носителей персональных данных
- ✓ Управление доступом к машинным носителям персональных данных
- ✓ Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны
- ✓ Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах
- ✓ Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных
- ✓ Контроль ввода (вывода) информации на машинные носители персональных данных
- ✓ Контроль подключения машинных носителей персональных данных
- ✓ Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания

Защита технических средств (ЗТС)

- ✓ Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам
- ✓ Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
- ✓ Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в

которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены

- ✓ Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
- ✓ Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)

Реализация:

Подсистема управления доступом реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за:
   - ✓ Разработку, внедрение и эксплуатацию подсистемы управления доступом к ПДн;
   - ✓ Обработку ПДн.
2. Разработка и утверждение ответственным лицом внутренних нормативных документов:
   - ✓ Положение о разграничении прав доступа к ПДн;
   - ✓ Инструкция пользователя ИСПДн;
   - ✓ Инструкция администратора ИСПДн.
3. Установление ответственности за нарушение правил разграничения прав доступа к ПДн.

4. Ознакомление работников с внутренними нормативными документами, регламентирующими вопросы организации и разграничения прав доступа к ПДн.

5. Учет машинных носителей ПДн.

6. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

7. Контроль и управление физическим доступом к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены,

исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.

8. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

9. Внедрение систем пожаротушения, кондиционирования, ИБП.

Программно-технические меры:

1. Штатными (встроенными) средствами разграничения доступа (ОС, приложений и СУБД).
2. Специальными программно-техническими средствами и/или комплексами, осуществляющими дополнительные меры по управлению доступом (электронные замки, биометрические идентификаторы и т.д.).

Размещение:

Модули подсистемы управления доступом могут размещаться:
на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;
на уровне серверов ЛВС: файловых серверах; серверах баз данных; и т.д.

4.2. Подсистема регистрации и учета

Назначение:

Подсистема регистрации и учета предназначена для сбора и накопления сведений о событиях безопасности, происходящих в ИСПДн.

Данная подсистема не используется непосредственно для предотвращения нарушений безопасности, она необходима для обнаружения, записи и анализа событий, связанных с обеспечением безопасности информации.

Требования к подсистеме:

В соответствии с [9] для подсистемы регистрации и учета установлены следующие требования:

1. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Содержание мер по регистрации событий безопасности:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы регистрации и учета обеспечиваются реализацией следующих мер:

- ✓ Определение событий безопасности, подлежащих регистрации, и сроков их хранения
- ✓ Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
- ✓ Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
- ✓ Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
- ✓ Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
- ✓ Генерирование временных меток и (или) синхронизация системного времени в информационной системе
- ✓ Защита информации о событиях безопасности

Реализация:

Подсистема регистрации и учета реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы регистрации и учета.

2. Разработка и утверждение ответственным лицом документа «План восстановления работоспособности ИСПДн».

3. Планом восстановления работоспособности ИСПДн должны быть определены:

- ✓ события безопасности, подлежащие регистрации, и сроки их хранения
- ✓ состав и содержание информации о событиях безопасности, подлежащих регистрации
- ✓ период просмотра отчетов о событиях безопасности

- ✓ порядок реагирования на сбои при регистрации событий безопасности

4. Ознакомление ответственных работников с «Планом восстановления работоспособности ИСПДн».

Программно-технические меры:

1. Штатными (встроенными) средствами регистрации событий безопасности (ОС, приложений, СЗИ и СУБД).

2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по регистрации событий безопасности (системы обнаружения вторжений).

Размещение:

Модули подсистемы управления доступом могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.3. Подсистема обеспечения целостности

Назначение:

Подсистема обеспечения целостности предназначена для обеспечения целостности информационной системы и персональных данных;

Требования к подсистеме:

В соответствии с [9] для подсистемы обеспечения целостности установлены следующие требования:

1. Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности

информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Содержание мер по обеспечению целостности:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы обеспечения целостности обеспечиваются реализацией следующих мер:

- ✓ Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации;
- ✓ Контроль целостности персональных данных, содержащихся в базах данных информационной системы;
- ✓ Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций;
- ✓ Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);
- ✓ Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы;
- ✓ Ограничение прав пользователей по вводу информации в информационную систему;
- ✓ Контроль точности, полноты и правильности данных, вводимых в информационную систему;
- ✓ Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях.

Реализация:

Подсистема обеспечения целостности реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы обеспечения целостности.

2. Разработка и утверждение ответственным лицом внутренних нормативных документов:

- ✓ Положение о разграничении прав доступа к ПДн;
- ✓ План восстановления работоспособности ИСПДн;
- ✓ Инструкция пользователя ИСПДн;
- ✓ Инструкция администратора ИСПДн.

3. Планом восстановления работоспособности ИСПДн должны быть определены места хранения дистрибутивов ПО и СЗИ.

4. Ознакомление ответственных работников с «Планом восстановления работоспособности ИСПДн».

5. Положение о разграничении прав доступа к ПДн должно базироваться на принципе минимизации полномочий для пользователей ИСПДн в части ограничения их прав по вводу информации в информационную систему.

6. В «Инструкции пользователя ИСПДн» должны быть установлены:

- ✓ запрет на хранение документов, содержащих ПДн, на неподконтрольных внешних информационных ресурсах (файлообменные сети, почта);
- ✓ запрет на запуск файлов-вложений, содержащихся в спам-письмах.

Программно-технические меры:

1. Штатными (встроенными) средствами обеспечения целостности информационной системы и персональных данных и средствами разграничения доступа (ОС, приложений, СЗИ и СУБД, применение спам-фильтров, встроенных в почтовые клиенты, почтовые сервера, МЭ).

2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по обеспечению целостности информационной системы и персональных данных, средствами разграничения доступа, а также средствами противодействия утечкам информации (системы защиты от утечек ПДн (DLP).

Размещение:

Модули подсистемы обеспечения целостности могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.4. Подсистема антивирусной защиты

Назначение:

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

Требования к подсистеме:

В соответствии с [9] для подсистемы обеспечения целостности установлены следующие требования:

1. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Содержание мер по антивирусной защите:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы антивирусной защиты обеспечиваются реализацией следующих мер:

- ✓ Реализация антивирусной защиты;
- ✓ Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

Реализация:

Подсистема антивирусной защиты реализуется специализированными программными средствами и комплексами.

Размещение:

Модули подсистемы обеспечения целостности могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.5. Подсистема межсетевого экранирования

Назначение:

Подсистема межсетевого экранирования предназначена для обеспечения защиты информационной системы, ее средств, систем связи и передачи данных.

Требования к подсистеме:

В соответствии с [9] для подсистемы обеспечения целостности установлены следующие требования:

1. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Содержание мер по межсетевому экранированию:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы межсетевого экранирования обеспечиваются реализацией следующих мер:

- ✓ Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы
- ✓ Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом
- ✓ Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

- ✓ Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)
- ✓ Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств
- ✓ Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами
- ✓ Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
- ✓ Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи
- ✓ Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации
- ✓ Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам
- ✓ Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов
- ✓ Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю
- ✓ Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя
- ✓ Использование устройств терминального доступа для обработки персональных данных
- ✓ Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных
- ✓ Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов
- ✓ Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

- ✓ Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения
- ✓ Изоляция процессов (выполнение программ) в выделенной области памяти
- ✓ Защита беспроводных соединений, применяемых в информационной системе

Реализация:

Подсистема межсетевого экранирования реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы межсетевого экранирования.
2. Определение политики фильтрации входящих и исходящих соединений (необходимость / достаточность).

Программно-технические меры:

1. Штатными (встроенными) средствами обеспечения межсетевого экранирования, разграничения доступа, построения VPN соединений и администрирования ОС, сетевого оборудования (шифрование в беспроводных сетях, фильтрация по MAC-адресам и т.д.).
2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по обеспечению: межсетевого экранирования, разграничения доступа, антивирусной защиты, а также противодействия утечкам информации (средства электронной подписи, антивирусное ПО, средства построения VPN соединений, системы DLP и т.д.).

4.6. Подсистема анализа защищенности

Назначение:

Подсистема анализа защищенности предназначена для обеспечения контроля (анализа) защищенности информационной системы и персональных данных

Требования к подсистеме:

В соответствии с [9] для подсистемы анализа защищенности установлены следующие требования:

1. Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Содержание мер по анализу защищенности:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы анализа защищенности обеспечиваются реализацией следующих мер:

- ✓ Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
- ✓ Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
- ✓ Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
- ✓ Контроль состава технических средств, программного обеспечения и средств защиты информации
- ✓ Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе

Реализация:

Подсистема анализа защищенности реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы анализа защищенности.
2. В «Инструкции администратора ИСПДн» в перечень должностных обязанностей должны быть включены:
   - ✓ контроль и период контроля работоспособности ПО и СЗИ
   - ✓ инвентаризация ПО и СЗИ и период проведения
   - ✓ контроль правил генерации и смены паролей

Программно-технические меры:

1. Штатными (встроенными) средствами анализа защищенности, разграничения доступа, построения VPN соединений и администрирования ОС, сетевого оборудования (просмотр журналов, отчетов о событиях безопасности).

2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по анализу защищенности (сканеры безопасности, средства генерации паролей, средства математического моделирования и оценки рисков нарушения безопасности ПДн).

Размещение:

Модули подсистемы анализа защищенности могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;
на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.7. Подсистема обнаружения вторжений

Назначение:

Подсистема обнаружения вторжений реализуется модулем обнаружения вторжений в ИСПДн, подключенных к сетям международного информационного обмена.

Требования к подсистеме:

В соответствии с [9] для подсистемы обнаружения вторжений установлены следующие требования:

1. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия

Содержание мер по обнаружению вторжений:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы обеспечиваются реализацией следующих мер:

- ✓ Обнаружение вторжений
- ✓ Обновление базы решающих правил

Реализация:

Подсистема обнаружения вторжений реализуется специализированными программными средствами и комплексами.

Размещение:

Модули подсистемы обнаружения вторжений могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;
на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.8. Подсистема криптографической защиты

Назначение:

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

Требования к подсистеме:

В соответствии с нормативными документами ФСБ России для подсистемы криптографической защиты установлены следующие требования:

1. Меры по криптографической защите персональных данных должны обеспечивать генерацию и распределение ключевой информации между элементами ИСПДн, управление ключевой информацией, шифрование/дешифрование конфиденциальной информации, взаимодействие с подсистемами управления процессами обеспечения безопасности информации, контроля доступа к ресурсам и аудита.

Содержание мер по криптографической защите:

В соответствии с нормативными документами ФСБ России и установленным уровнем защищенности ПДн функции подсистемы криптографической защиты обеспечиваются реализацией следующих мер:

- ✓ Шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные портативные носители данных (дискеты, usb -носители и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа;
- ✓ Создание каналов связи, обеспечивающих защиту передаваемой информации;
- ✓ Принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию.
- ✓ Аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
- ✓ Обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;
- ✓ Обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

Реализация:

Подсистема криптографической защиты реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы криптографической защиты.

2. Лицами, ответственными за внедрение и эксплуатацию подсистемы криптографической защиты, должны быть определены места хранения ключевых носителей, а также дистрибутивов средств криптографической защиты информации, исключающие несанкционированный доступ.

3. Лицами, ответственными за внедрение и эксплуатацию подсистемы криптографической защиты должен быть организован учет средств криптографической защиты информации.

4. В «Инструкции пользователя ИСПДн» должны быть приведены правила эксплуатации и хранения ключевых носителей

5. Ознакомление работников с внутренними нормативными документами, регламентирующими вопросы криптографической защиты ПДн.

Программно-технические меры:

1. Штатными (встроенными) средствами криптографической защиты ОС, СУБД, сетевого оборудования.

2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по криптографической защите ПДн (специализированное ПО, ЭП и т.д.).

Размещение:

Модули подсистемы обнаружения вторжений могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.9. Подсистема управления процессами обеспечения безопасности

Назначение:

Подсистема управления процессами обеспечения безопасности ПДн предназначена для реализации следующих мер по обеспечению безопасности ПДн:

- ✓ выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- ✓ управление конфигурацией информационной системы и системы защиты персональных данных.

Требования к подсистеме:

В соответствии с [9] для подсистемы управления процессами обеспечения безопасности ПДн установлены следующие требования:

1. Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

2. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Содержание мер по управлению процессами обеспечения безопасности ПДн:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы управления процессами обеспечения безопасности ПДн обеспечиваются реализацией следующих мер:

- ✓ Определение лиц, ответственных за выявление инцидентов и реагирование на них
- ✓ Обнаружение, идентификация и регистрация инцидентов
- ✓ Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами
- ✓ Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий
- ✓ Принятие мер по устранению последствий инцидентов
- ✓ Планирование и принятие мер по предотвращению повторного возникновения инцидентов
- ✓ Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных
- ✓ Управление изменениями конфигурации информационной системы и системы защиты персональных данных
- ✓ Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных
- ✓ Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных

Реализация:

Подсистема реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы управления процессами обеспечения безопасности ПДн.

2. В «Инструкции администратора ИСПДн» в перечень должностных обязанностей должны быть включены:

- ✓ настройка и управление средствами защиты;
- ✓ анализ инцидентов безопасности ИСПДн, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- ✓ принятие мер по устранению последствий инцидентов;
- ✓ планирование и принятие мер по предотвращению повторного возникновения инцидентов;
- ✓ анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных;
- ✓ определение порядка поставки, закрепления, ввода в эксплуатацию копирования, тиражирования, доработки, восстановления программного обеспечения;
- ✓ обучение (подготовка) пользователей порядку и правилам работы с программно-аппаратными средствами объекта, порядку использования средств защиты информации;
- ✓ документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных
- ✓ организация контроля за состоянием защиты информации и работой пользователей ИСПДн в части соблюдения требований по защите информации;
- ✓ определение периодичности и порядка смены средств опознавания и разграничения доступа (паролей, личных идентификаторов);
- ✓ организация учета, хранения, уничтожения, ремонта машинных носителей информации и порядка обращения с ними.

3. В «Инструкции пользователя ИСПДн» в перечень должностных обязанностей должны быть включено требование о своевременном информировании пользователем ответственных лиц о возникновении инцидентов в информационной системе и системе защиты ПДн

4. В «Инструкции пользователя ИСПДн» должен быть установлен запрет для пользователей на внесение изменений в конфигурацию информационной системы и системы защиты персональных данных

Программно-технические меры:

Выявление инцидентов

1. Штатными (встроенными) средствами регистрации событий и аудита безопасности информации (ОС, приложений и СУБД).

2. Специальными программно-техническими средствами и/или комплексами, реализующими дополнительные меры по анализу защищенности информации (ПО анализа рисков, сканеры безопасности и т.д.), а также средствами противодействия утечкам информации (системы защиты от утечек ПДн (DLP).

Управление конфигурацией:

1. Штатными (встроенными) средствами разграничения доступа (ОС, приложений и СУБД).

2. Специальными программно-техническими средствами и/или комплексами, осуществляющими дополнительные меры по управлению доступом (электронные замки, биометрические идентификаторы и т.д.).

Размещение:

Модули подсистемы управления процессами обеспечения безопасности могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

4.10. Подсистема обеспечения доступности ПДн

Назначение:

Подсистема обеспечения доступности ПДн предназначена для доступа пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе

Требования к подсистеме:

В соответствии с [9] для подсистемы обеспечения доступности ПДн установлены следующие требования:

1. Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Содержание мер по обеспечению доступности ПДн:

В соответствии с [9] и установленным уровнем защищенности ПДн, функции подсистемы обеспечения доступности ПДн обеспечиваются реализацией следующих мер:

- ✓ Использование отказоустойчивых технических средств
- ✓ Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы
- ✓ Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование
- ✓ Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных
- ✓ Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала

Реализация:

Подсистема реализуется организационными и программно-техническими мерами:

Организационные меры:

1. Назначение лиц ответственных за разработку, внедрение и эксплуатацию подсистемы обеспечения доступности ПДн.
2. В «Инструкции администратора ИСПДн» в перечень должностных обязанностей должны быть включен контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

3. Лицами, ответственными за внедрение и эксплуатацию подсистемы обеспечения доступности ПДн, должен быть разработан документ «План восстановления работоспособности ИСПДн», в котором должно быть указано время восстановления ПДн с МН.

Программно-технические меры:

1. Штатными средствами ОС Windows реализовать копирование, архивирование данных и состояний ОС.
2. Специальными программно-техническими средствами и/или комплексами, осуществляющими меры по резервному копированию данных, создания образов ОС.
3. Создать резервный канал связи с сетью Интернет путем подключения ИСПДн к альтернативному провайдеру.

Размещение:

Модули подсистемы обеспечения доступности ПДн могут размещаться:

на уровне АРМ: АРМы пользователей ИСПДн; АРМы системных администраторов ИСПДн;

на уровне серверов ЛВС: файловых серверах; серверах баз данных; серверах приложений; серверах электронной почты; серверах каталогов; серверах безопасности и т.д.

5. Пользователи ИСПДн

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности. В ИСПДн Палаты можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор ИСПДн;
- Пользователь ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5.1. Администратор ИСПДн

Администратор ИСПДн (сотрудник Палаты) - обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (пользователя ИСПДн) к элементам, хранящим персональные

данные. Администратор ИСПДн является ответственным за функционирование СиЗИ ПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;
- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн.

Администратор ИСПДн уполномочен:

- реализовывать политики безопасности в части настройки СЗИ, СКЗИ, в соответствии с которыми пользователь ИСПДн получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- осуществлять контроль и обучение пользователей в части использования ресурсов ИСПДн.

5.2. Пользователь ИСПДн

Пользователь ИСПДн - сотрудник Палаты, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Пользователь ИСПДн не имеет полномочий для управления подсистемами обработки данных и СиЗИ ИСПДн.

Пользователь ИСПДн обладает следующим уровнем доступа и знаний:

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

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники Палаты, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника Администратор ИСПДн обязан организовать его ознакомление с должностной инструкцией и необходимыми документами,

регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятыми процедурами работы с элементами ИСПДн и СиЗИ ИСПДн.

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

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

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

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

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

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

При завершении работы с ИСПДн 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 Палаты должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, Администратору ИСПДн и/или лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция пользователя ИСПДн.

8. Ответственность пользователей ИСПДн

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность.

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

9. Список использованных источников

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

1. Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
2. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
5. 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»
6. Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

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

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;
8. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;
9. Приказ ФСТЭК России 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».

Нормативно-методические документы Федеральной службы безопасности России:

10. Приказ Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".