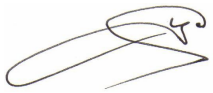
УТВЕРЖДАЮ
Председатель комитета по
делам записи актов гражданского
состояния и архивов Правительства
Хабаровского края

 О.В. Завьялова

« 22 » апреля 2015 г.

Политика информационной безопасности информационных систем персональных данных комитета по делам ЗАГС и архивов Правительства Хабаровского края

Содержание

1. 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.

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) – 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 ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

ПЕРСОНАЛЬНЫЕ ДАННЫЕ – 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.

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

ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

ПРАВИЛА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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

ПРОГРАММНОЕ (ПРОГРАММНО-МАТЕМАТИЧЕСКОЕ) ВОЗДЕЙСТВИЕ – 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).

2. 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;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ОС – операционная система;

КОМИТЕТ – комитет по делам ЗАГС и архивов Правительства Хабаровского края;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

ПО – программное обеспечение;

ПЭМИН – побочные электромагнитные излучения и наводки;

САЗ – система анализа защищенности;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

СОВ – система обнаружения вторжений;

ТКУИ – технические каналы утечки информации;

УБПДн – угрозы безопасности персональных данных.

3. Введение

3.1. Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных", на основании:

- Постановления Правительства РФ от 01 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- 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 №149/6/6-662.

3.2. В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Комитета.

4. Общие положения

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

4.2. 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.

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

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

4.5. Состав объектов защиты представлен в Перечнях защищаемых информационных ресурсов ИСПДн Комитета.

4.6. Состав ИСПДн подлежащих защите, представлен в Технических паспортах ИСПДн Комитета.

5. Область действия

5.1. Требования настоящей Политики распространяются на всех сотрудников Комитета (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

6. Система защиты персональных данных

6.1. Система защиты персональных данных (СЗПДн), строится на основании:

- Перечня сведений конфиденциального характера (персональных данных) Комитета;
- Актов определения уровней защищенности информационных систем персональных данных;
- Частных моделей угроз безопасности персональных данных;
- Положения о порядке обращения с конфиденциальной информацией и мерах по обеспечению ее защиты и сохранности в Комитете;
- Руководящих документов ФСТЭК и ФСБ России.

6.2. На основании вышеперечисленных документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Комитета.

6.3. На основании анализа актуальных угроз безопасности ПДн описанного в Моделях угроз и Актах определения уровней защищенности ИСПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Системах нейтрализации предполагаемых угроз безопасности персональных данных соответствующих ИСПДн.

6.4. Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- серверах приложений;
- СУБД;
- ЛВС;
- каналах передачи в сети общего пользования и (или) международного информационного обмена, если по ним передаются ПДн.
- В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:
- средства защиты информации от несанкционированного доступа;
- антивирусные средства;
- средства межсетевого экранирования;
- средства криптографической защиты информации (при передаче защищаемой информации по каналам связи за пределы контролируемой зоны);
- средства защиты информации от утечки по каналам ПЭМИН.

6.5. В список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты.

6.6. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

Список используемых технических средств отражается в Перечне применяемых средств защиты информации Комитета. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены начальником Комитета или лицом, ответственным за обеспечение защиты ПДн.

7. Требования к подсистемам СЗПДн

7.1. СЗПДн в зависимости от возможных угроз безопасности и уровня защищенности ИСПДн может включать в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты;
- защиты от утечки по каналам ПЭМИН.

7.2. Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ИСПДн, определенного в Акте определения уровня защищенности информационной системы персональных данных.

7.3. Подсистемы управления доступом, регистрации и учета

7.3.1. Подсистема управления доступом, регистрации и учета в общем случае предназначена для реализации следующих функций:

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

7.3.2. Подсистема управления доступом реализуется с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД) и внедренных специальных технических средств, осуществляющих дополнительные меры по аутентификации и контролю.

7.4. Подсистема обеспечения целостности и доступности

7.4.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а так же средств защиты, при случайной или намеренной модификации.
7.4.2. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

7.5. Подсистема антивирусной защиты

7.5.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн.
7.5.2. Средства антивирусной защиты, в общем случае, 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.

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

7.6. Подсистема межсетевого экранирования

7.6.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по различным параметрам;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;
- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

7.6.2. Подсистема реализуется внедрением сертифицированных комплексов межсетевого экранирования на границе ИСПДн.

7.7. Подсистема анализа защищенности

7.7.1. Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.
7.7.2. Функционал подсистемы может быть реализован программными или программно-аппаратными средствами.

7.8. Подсистема обнаружения вторжений

7.8.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.
7.8.2. Функционал подсистемы может быть реализован программными или программно-аппаратными средствами.

7.9. Подсистема криптографической защиты

7.9.1. Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.
7.9.2. Подсистема реализуется внедрением криптографических программных или программно-аппаратных комплексов.

7.10. Подсистема защиты от утечки по каналам ПЭМИН

7.10.1. Подсистема защиты информации от утечки по каналам ПЭМИН предназначена для исключения съема информативного сигнала техническими средствами за счет побочных электромагнитных излучений и наводок, возникающих при функционировании средств вычислительной техники и периферийного оборудования ИСПДн.
7.10.2. Защита от утечки по каналам ПЭМИН может быть реализована организационными мерами (увеличение границ контролируемой зоны), пассивными методами или средствами активной защиты, предназначенными для маскировки побочных электромагнитных излучений путем излучения в окружающее пространство электромагнитного поля шума.

8. Пользователи ИСПДн

8.1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

8.2. В ИСПДн Комитета можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор баз данных;
- администратор безопасности;
- пользователь АРМ;
- специалист по техническому обслуживанию оборудования;
- программист-разработчик ИСПДн.

8.3. Данные о группах пользователях, уровне их доступа и информированности должны быть отражены в Матрицах разграничения доступа к информационным ресурсам в информационных системах персональных данных Комитета.

8.4. Администратор баз данных

8.4.1. Администратор баз данных, сотрудник Комитета, ответственный за настройку, внедрение и сопровождение серверов баз данных, АРМов. Обеспечивает функционирование серверов баз данных, АРМов, выполняет резервное копирование баз данных ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя АРМ к элементам баз данных, хранящим персональные данные.
8.4.2. Администратор баз данных 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.

8.5. Администратор безопасности

8.5.1. Администратор безопасности, сотрудник Комитета, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.
8.5.2. Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора баз данных;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь АРМ получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других организаций.

8.6. Пользователь АРМ ИСПДн

8.6.1. Пользователь АРМ ИСПДн, сотрудник Комитета, 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 не имеет полномочий для управления подсистемами обработки данных и СЗПДн.
8.6.2. Пользователь АРМ 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.

8.7. Специалист по техническому обслуживанию оборудования

8.7.1. Специалист по техническому обслуживанию, сотрудник Комитета (организации сервисного подрядчика) осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Специалист по техническому обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.
8.7.2. Специалист по техническому обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

8.8. Программист-разработчик ИСПДн

8.8.1. Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Комитета, так и сотрудники сторонних организаций (организации сервисного подрядчика).

8.8.2. Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

9. Требования к персоналу по обеспечению защиты ПДн

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

9.2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией, а специалист Комитета, ответственный за организацию обработки персональных данных, - с положениями законодательства Российской Федерации о персональных данных, локальными актами по вопросам обработки персональных данных, требованиями к защите персональных данных.

9.3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

9.4. Сотрудники Комитета, 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.

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

9.6. Сотрудники Комитета 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.

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

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

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

9.10. 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.

9.11. Сотрудники Комитета 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.

9.12. Сотрудники Комитета 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, руководителю

структурного подразделения и ответственному за обеспечение безопасности персональных данных (администратору безопасности) ИСПДн.

10. Ответственность сотрудников ИСПДн

10.1. В соответствии со ст. 24 Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ "О персональных данных" лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

10.2. Действующее законодательство Российской Федерации 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).

10.3. Администратор баз данных 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.

10.4. При нарушениях сотрудниками Комитета – пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

11. Список использованных источников

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

- Федеральный Закон от 27.07.2006 №152-ФЗ "О персональных данных";
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 21 марта 2012 г. №211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21.02.2008 №149/5-144;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21.02.2008 №149/6/6-622.