УТВЕРЖДЕНА

приказом генерального директора
МУП «Водоканал»
№ 171 «О» от 25 марта 2013 г.

Политика информационной безопасности МУП «Водоканал»

2013

Термины и определения

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

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

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

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

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

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

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

Доступ к информации – возможность получения информации и ее использования.

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

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.

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.

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.

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

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

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

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

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

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

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

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).

Перечень сокращений

АВПО – антивирусное программное обеспечение
АРМ – автоматизированное рабочее место
ВДТ – видеодисплейный терминал;
ИСПДн – информационная система персональных данных
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система (подсистема) защиты персональных данных
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных.

Введение

Настоящая Политика информационной безопасности (далее Политика) МУП «Водоканал» (далее Оператор) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных.

Политика разработана в соответствии с требованиями нормативных документов:

– Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановление Правительства РФ от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденных Приказом ФСТЭК России от 05.02.2011г. № 58;

– «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу, обслуживающему и эксплуатирующему ИСПДн, степень ответственности сотрудников, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных Оператора.

1 Общие положения

Целью, настоящей Политики, является обеспечение безопасности объектов защиты Оператора от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных с целью минимизации ущерба от возможной реализации 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.

2 Область действия

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

3 Система защиты персональных данных

Система защиты персональных данных (СЗПДн) строится на основании:

- Перечня персональных данных;
- Акта классификации информационных систем персональных данных;
- Частной модели актуальных угроз безопасности и вероятного нарушителя;
- Положения о разграничении прав доступа к персональным данным;
- локальных приказов и распоряжений действиями по обеспечению безопасности персональных данных;
- нормативных документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн, обрабатываемых в каждой ИСПДн Оператора. На основании анализа актуальных угроз безопасности ПДн, описанных в Частной модели актуальных угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по внутреннему контролю соблюдения безопасности персональных данных.

Организационные мероприятия должны включать:

- правовое основание для сбора персональных данных;
- определение мест хранения и режима доступа к персональным данным;

- определение ответственных лиц за соблюдением мер безопасности;
- защиту персональных данных, обрабатываемых без средств автоматизации;
- защиту персональных данных, обрабатываемых с применением средств автоматизации;
- защиту объектов от хищения;
- защиту съемных накопителей, содержащих персональные данные;
- вопросы обезличивания и уничтожения персональных данных.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- защиты от несанкционированного доступа к персональным данным;
- антивирусной защиты для рабочих станций пользователей и серверов;
- межсетевого экранирования;
- криптографической защиты информации, при передаче защищаемой информации по каналам связи;
- защиты от копирования;
- средства защиты от утечки по ТКУИ.

4 Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- управления доступом;
- регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- контроля отсутствия недекларированных возможностей;
- криптографической защиты;
- защиты от утечки по ТКУИ.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

4.1 Подсистема управления доступом должна осуществлять:

– идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по идентификатору и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

– идентификацию терминалов, технических средств информационной системы, каналов связи и внешних устройств ИСПДн по их логическим адресам (номерам);

– идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;

– контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа.

4.2 Подсистема регистрации и учета должна осуществлять:

– регистрацию входа (выхода) пользователя в систему (из системы) либо регистрацию загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или не успешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа, код или пароль, предъявленный при неуспешной попытке.

– учет всех защищаемых носителей информации посредством нанесения на них маркировки и занесения данных в журнал учета с отметкой об их выдаче (приеме);

– регистрацию выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращений к подсистеме вывода), краткое содержание документа (наименование, вид, код), спецификация устройства выдачи (логическое имя (номер) внешнего устройства);

– очистку (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних носителей информации;

– регистрацию запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный);

– регистрацию попыток доступа программных средств (программ, процессов, задач) к защищаемым файлам. В параметрах регистрации указываются

дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла;

– регистрацию попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер)).

4.3 Подсистема обеспечения целостности должна осуществлять:

– обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

– физическую охрану информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

– периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;

– наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

4.4 Подсистема антивирусной защиты

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, обеспечивающей обработку этой информации, рекомендуется применять специальные средства антивирусной защиты (подсистема антивирусной защиты). Такие средства способны обеспечивать:

– обнаружение и блокирование деструктивных вирусных воздействий на общесистемное и прикладное ПО, реализующее обработку ПДн, а также на сами ПДн;

– обнаружение и удаление "неизвестных" вирусов (т.е. вирусов, сигнатуры которых еще не внесены в антивирусные базы данных);

– обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

4.5 Подсистема межсетевого экранирования

Межсетевое экранирование должно обеспечивать:

– фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

– идентификацию и аутентификацию лица, осуществляющего администрирование межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

– регистрацию входа (выхода) лица, осуществляющего администрирование межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

– контроль целостности своей программной и информационной части;

– фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– восстановление свойств межсетевого экрана после сбоев и отказов оборудования;

– регламентированное тестирование реализации правил фильтрации, процесса идентификации и аутентификации лица, осуществляющего администрирование межсетевого экрана, процесса регистрации действий лица, осуществляющего администрирование межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления;

– фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

– фильтрацию с учетом любых значимых полей сетевых пакетов;

– регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);

– регистрация запуска программ и процессов (заданий, задач);

– фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;

– фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;

– фильтрацию с учетом даты и времени;

– аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;

– регистрацию и учет запросов на установление виртуальных соединений;

– локальную сигнализацию попыток нарушения правил фильтрации;

– предотвращение доступа не обладающего данным правом пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;

– идентификацию и аутентификацию лица, осуществляющего администрирование межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;

– регистрацию действий лица, осуществляющего администрирование межсетевого экрана по изменению правил фильтрации;

– возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной формы;

– контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.

4.6 Подсистема анализа защищенности

Подсистема анализа защищенности предназначена для осуществления контроля настроек защиты операционных систем на видеотерминальных дисплеях и сервере и позволяет оценить возможность проведения нарушителями атак на сетевое оборудование, контролирует безопасность программного обеспечения. С помощью таких средств (средства обнаружения уязвимостей) производится сканирование сети с целью исследования ее топологии, осуществления поиска незащищенных или несанкционированных сетевых подключений, проверки настроек межсетевых экранов и т.п. Данный анализ производится на основании детальных описаний уязвимостей настроек средств защиты (например, коммутаторов, маршрутизаторов, межсетевых экранов) или уязвимостей операционных систем или прикладного программного обеспечения. Результатом работы средств анализа защищенности является отчет, в котором обобщаются сведения об обнаруженных уязвимостях.

– Средства обнаружения уязвимостей могут функционировать на сетевом уровне, уровне операционной системы и уровне приложения. Применяя сканирующее ПО, можно составить карту доступных узлов ИСПДн, выявить

используемые на каждом из них сервисы и протоколы, определить их основные настройки и сделать предположения относительно вероятности реализации НСД. По результатам сканирования системы вырабатываются рекомендации и меры, позволяющие устранить выявленные недостатки.

4.7 Подсистема обнаружения вторжений

Выявление угроз НСД при межсетевом взаимодействии производится с помощью систем обнаружения вторжений (подсистема обнаружения вторжений). Такие системы строятся с учетом особенностей реализации атак и этапов их развития. Они основаны на следующих методах обнаружения атак: сигнатурные методы, методы выявления аномалий, комбинированные методы с использованием обоих названных методов.

Для обнаружения вторжений в ИСПДн 3 и 4 классов рекомендуется использовать системы обнаружения сетевых атак, применяющие методы сигнатурного анализа.

4.8 Подсистема контроля отсутствия недекларированных возможностей реализуется в большинстве случаев на базе систем управления базами данных, специальных средств защиты информации, антивирусных средств защиты информации.

4.9 Подсистема криптографической защиты информации

Подсистема объединяет средства криптографической защиты информации. По ряду функций подсистема кооперируется с подсистемой защиты от НСД. Поддержку подсистемы криптографической защиты в части управления ключами осуществляет подсистема управления СЗИ. Структурно подсистема состоит из:

– программных средств симметричного шифрования данных;

– программно-аппаратных средств цифровой подписи электронных документов.

Функции подсистемы предусматривают:

– обеспечение целостности передаваемой по каналам связи и хранимой информации;

– имитозащиту сообщений, передаваемых по каналам связи (имитозащита – защита системы шифрованной связи от навязывания ложных данных);

– скрытие смыслового содержания конфиденциальных сообщений, передаваемых по каналам связи и хранимых на носителях;

– обеспечение аутентификации источника данных.

Функции подсистемы направлены на ликвидацию наиболее распространенных угроз сообщениям в автоматизированных системах:

– угроз, направленных на несанкционированное ознакомление с информацией;

– несанкционированного чтения информации на машинных носителях ЭВМ;

– незаконного подключения к аппаратуре и линиям связи;

– перехвата ЭМИ с линий связи;

– угроз, направленных на несанкционированную модификацию (нарушение целостности) информации;

– изменения служебной или содержательной части сообщения;

– подмены сообщения;

– изъятия (уничтожения) сообщения и т.д.

4.10 Подсистема защиты от утечки по каналам техническим каналам утечки информации (ТКУИ)

С целью предотвращения утечек акустической (речевой), видовой информации, а также утечек информации за счет побочных электромагнитных излучений и наводок применяются специальные технические средства. При этом выделяются пассивные и активные средства защиты.

Пассивные средства защиты, как правило, реализуются на этапе разработки проектных решений при строительстве или реконструкции зданий. Преимущества применения пассивных средств заключаются в том, что они позволяют заранее учесть типы строительных конструкций, способы прокладки коммуникаций, оптимальные места размещения защищаемых помещений.

Защита ПДн при осуществлении пользователями информационных систем голосового ввода данных в ИСПДн или их воспроизведении акустическими средствами ИСПДн обеспечивается путем звукоизоляции помещений, в которых устанавливаются аппаратные средства ИСПДн, систем инженерного обеспечения (вентиляции, отопления и кондиционирования), а также ограждающих конструкций помещений (стены, пол, потолок, окна, двери).

Звукоизоляция обеспечивается с помощью архитектурных и инженерных решений, применением специальных звукопоглощающих строительных и отделочных материалов, виброизолирующих опор, которыми разделяют друг от друга различные ограждающие конструкции. Для обеспечения требований по защите ПДн достаточным является повышение звукоизоляции на 10-15 дБ. Для снижения вероятности перехвата информации такого рода необходимо исключить возможность установки посторонних предметов на внешней стороне ограждающих конструкций помещений и выходящих из них инженерных коммуникаций.

В случае технической невозможности использования пассивных средств защиты помещений, применяют активные меры защиты, заключающиеся в создании маскирующих акустических и вибрационных помех.

Средства акустической маскировки используется для защиты речевой информации от утечки по прямому акустическому каналу путем создания акустических шумов в местах возможного размещения средств подслушивания или нахождения посторонних лиц.

Средства виброакустической маскировки применяются для защиты информации от перехвата с помощью электронных стетоскопов, радиостетоскопов, а также лазерных акустических систем подслушивания.

С целью предотвращения утечки информации по телефонным каналам связи необходимо оконечные устройства телефонной связи, которые имеют прямой выход на городскую автоматическую телефонную станцию, оборудовать специальными средствами защиты информации, которые используют электроакустическое преобразование.

Защита от утечки видовой информации:

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

В информационных системах, имеющих подключение к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования), или при функционировании которых предусмотрено использование съемных носителей информации, используются средства антивирусной защиты.

5 Способы обеспечения безопасности

Система защиты персональных данных должна обеспечивать всестороннюю комплексную защиту.

Законодательные (правовые) меры защиты.

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее

обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

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

Морально-этические меры защиты.

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

Организационные (административные) меры защиты.

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

Организационные меры должны:

– предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

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

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

Организационные меры должны состоять из:

– регламента доступа в помещения ИСПДн;

– порядка допуска работников к использованию ресурсов ИСПДн;

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

– регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

– инструкций пользователей ИСПДн (администратора безопасности, оператора ИСПДн);

– инструкций пользователя при возникновении внештатных ситуаций.

Физические меры защиты.

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

Аппаратно-программные средства защиты ПДн.

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;

– средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн МУП «Водоканал»;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства защиты ПДн.

6 Пользователи ИСПДн

Пользователями ИСПДн являются штатные сотрудники Оператора, осуществляющие 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.

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.

7 Требования к персоналу по обеспечению защиты ПДн

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

При поступлении сотрудника на работу, специалист по кадрам обязан под роспись организовать его ознакомление с должностным регламентом и необходимыми документами, регламентирующими требования по защите ПДн, а также совместно с Администратором безопасности провести обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен с требованиями настоящей Политики, принятыми процедурами работы с элементами ИСПДн и СЗПДн.

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

Сотрудники 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.

Пользователям ИСПДн 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 Оператора, третьим лицам.

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

С целью минимизации риска неавторизованного доступа или повреждения бумажных документов, носителей данных и средств обработки информации, рекомендуется внедрить политику «чистого стола» и «чистого экрана».

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 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 лиц, нарушивших 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, непосредственному руководителю, Ответственному за обеспечение безопасности ПДн для принятия мер и немедленного реагирования на угрозы безопасности ПДн.

8 Ответственность сотрудников

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 гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Уголовный Кодекс РФ (статьи272,273и 274) предусматривает ответственность за совершение следующих действий:

– Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;

– Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

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